А.В. Бабаш
Е.К. Баранова
Д.А. Ларин

Информационная безопасность

Том 2

История защиты информации в России

Москва 2012

УДК
ББК
Б

Бабаш А.В., Баранова Е.К., Ларин Д.А. **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ:** Учебно-практичес-кое пособие. – М.: Изд. центр ЕАОИ, 2012. – 736 с.

Показана история развития защиты информации в России с древнейших времен: шифрование, дешифрование, в том числе умерших языков. Для студентов высших учебных заведений, обучающихся по направлению информационной безопасности и прикладной информатики.

ISBN

Содержание

Том 2. История защиты информации в России

Памяти Генриха Петровича Шанкина
посвящается

Предисловие авторов

Предлагаемая читателям книга посвящена криптографической защите информации в России. Охватываемый исторический период от IX в. до XX в.

Отдельная глава посвящена Российской криптографии XIV–XVIII вв. от времен царствования Ивана IV Грозного до эпохи Петра I. Замечено, что Петр Великий был первым из российских правителей, кто предельно ясно осознал важность криптографической деятельности для обеспечения безопасности государства. Во время его правления впервые в истории отечественной криптографии к осуществлению криптографической деятельности привлеклось все высшее руководство России, включая царя.

В отдельном разделе рассмотрены вопросы рождения российского криптоанализа. Он посвящен 270-летию создания отечественной дешифровальной службы. Описаны первые шаги отечественного криптоанализа и достижения российских ученых в этой области.

Исторически так сложилось, что с криптографией связаны неординарные и разносторонне одаренные личности, достаточно упомянуть барона Шиллинга фон Канштадта или Александра Сергеевича Грибоедова о деятельности которых, и не только о них, вы прочитаете в главе «Русские криптографические идеи в России XIX века».

Глава «Криптографическая деятельность революционеров в России» знакомит читателя с некоторыми принципами организации конспиративной переписки от 20-х гг. XIX в. до начала века XX. Подробный материал представлен о периоде подпольной работы РСДРП, а точнее об организации конспиративной переписки «Искры» и деятельности виднейших революционеров.

Большое внимание в книге уделено вопросам рождения и развития советской криптографической службы в период с 1917 г. до конца XX в.

Противостояние криптографов и взломщиков шифров всегда являлось двигателем в эволюции методов шифрования, а попытки создания абсолютно стойких шифров сродни попыткам создания вечного двигателя. Затраты на вскрытие зашифрованных данных часто превышают стоимость самой информации и тогда прибегают к специальным методам: кража, подкуп, взлом зачастую оказываются «более рентабельными». Глава 10 «Тайные операции в криптографии» знакомит читателей с агентурно-оперативными методами работы спецслужб и проникновением в криптографические тайны противника.

При написании книги, авторами были использованы многочисленные исторические источники, статьи, мемуары и монографии. Наша цель – популяризация криптографического подхода к защите информации; при этом, читатель должен получить достаточно содержательное представление о конкретных методах и средствах защиты информации, появившихся в рассматриваемый исторический отрезок времени в России.

Книга рекомендуется студентам, обучающимся в высших учебных заведениях, специализирующихся в области информационной безопасности. Материал может быть полезен и всем тем, кто интересуется вопросами становления криптографии в России.

Представляется, что предлагаемая работа может заинтересовать и специалистов по защите информации, интересующихся вопросами возникновения и становления криптографии, как искусства и науки.

Благодарим коллег, принявших участие в обсуждении подготовленных материалов и предоставивших новые данные и сведения по истории криптографии в России.

А. В.Бабаш
Е.К.Баранова
Д.А.Ларин

Введение

С древних времен человечество стремится защищать свои тайны. Наиболее мощным средством защиты информации является криптография. Одними из первых криптографию стали использовать различные государственные структуры для защиты правительственных, военных, дипломатических сообщений. Здесь следует заметить, что при оценке влияния криптографии на те или иные события мировой истории следует использовать более широкое понятие – криптографическая деятельность. Под криптографической деятельностью понимается не только шифрование и дешифрование, но и организация каналов передачи сообщений (системы связи), использование различных методов защиты информации (криптография, стеганография, физическая защита собственно линий связи и др.), организация перехвата шифрованной информации противника. Дешифрование без перехвата невозможно. Разумеется, сюда входят меры по добыванию информации, облегчающей дешифрование (добывание ключей, описания шифрсистем и др.). С другой стороны, при разработке методов и средств защиты информации необходимо учитывать возможные аналогичные действия противника и предпринимать соответствующие меры для их пресечения. Если действия по добыванию информации связаны с разведывательными операциями, то при защите главную роль играют контрразведывательные мероприятия. Поэтому криптографические службы работают в тесном контакте с разведкой и контрразведкой.

Вообще криптографическая деятельность есть составная часть информационного противоборства, которое включает в себя организацию пропаганды и информационного воздействия на потенциального и реального противника и своего населения (поддержка патриотического духа, разъяснение политики государства и др.), ведение контрпропаганды, проведение операций по дезинформации противника. В случае проведения операций по информационному воздействию на против-

ника нередко используется криптография. С одной стороны, узнав о дешифровании своих секретных сообщений, можно не усиливать защиту, а продолжать использовать тот же шифр, передавая дезинформацию, которую другая сторона будет принимать за истинную информацию. Такая ситуация называется дезинформацией «под шифром». В этом случае для передачи настоящей информации следует использовать другие шифры и другие каналы связи. С другой стороны, тайно захватив шифры и ключи противника (или вскрыв их аналитическим путем), можно попытаться от имени истинного отправителя передать противнику дезинформацию [Гольев, 2008].

Фактически, как только где-то на Земле происходило становление того или иного государства так тут же начиналась криптографическая деятельность, с развитием государственных институтов учреждались специальные криптографические службы. Известный американский историк Дэвид Кан считает, что признаками великой державы являются наличие у страны ядерного оружия, успехов в освоении космоса и достижений в области криптографии [Кан, 2004].

Разумеется, не стала исключением и наша страна, где история криптографической деятельности насчитывает не одно столетие. В данной книге рассказывается о событиях, которые привели к возникновению отечественной криптографической службы, которая сегодня одна из лучших в мире. По словам Д. Кана «русские вознесли достижения своей страны в сфере криптологии[1] до высоты полета космических спутников» [Кан, 2004].

[1] На западе часто употребляется этот термин для обозначения науки о криптографических методах защиты информации. Криптология разделяется на криптографию (науку о создании шифров) и криптоанализ, изучающий методы их взлома. У нас в стране для обозначения данной сферы человеческой деятельности принят термин криптография.

Глава 1.

Криптография Древней Руси

В IX в. в результате объединения новгородских и киевских земель образовалось единое русское государство – Киевская Русь. Эффективное управление весьма обширной территорией было невозможно без организации надежной связи между столицей Киевом с подчиненными территориями и войсками, несущими сторожевую службу на границах Руси, а также находящимися в походе. Основным средством связи в то время были специальные княжеские гонцы – «люди пешие и конные» – и «верные головы» (люди из княжеской дружины), которые со скоростью 200 и более верст в сутки передвигались от одного пункта до другого, передавая как устные, так и письменные сообщения» [Астрахан, 1996]. Использовались и другие способы связи: оптическая сигнализация с помощью костров и дымов, почтовые голуби, на поле боя управление осуществлялось с помощью сигнальных труб и свистков [Астрахан, 1996], [История, 1984], [Кудрявцев, 2002].

Для обеспечения конфиденциальности передаваемой информации использовались различные методы. Наиболее важные сообщения заучивались гонцом наизусть. При этом часто использовались намеки, иносказания условные слова. Суть данного метода заключается в том, что смысл передаваемого сообщения мог понять только посвященный человек. В последствии, в криптографии такой способ обеспечения секретности получил название «жаргонного кода» и применяется до сих пор. Так, например, на жаргоне многих разведок слово БОЛЕТЬ означает «арест» или «заключение под стражу»; БОЛЬНИЦА – тюрьма; ДОКТОР – контрразведка. Тогда сообщение «Майкл арестован контрразведкой. Ему грозит заключение в тюрьму», принимает следующий «невинный» вид: «Майкл заболел. Вчера был доктор и посоветовал ему лечиться в больнице» [Гольев, 2008], [Полмар, 1999]. Использовался и так называе-

мый «тарабарский язык»[1] когда в устное сообщение вставлялись частицы-паразиты так фраза «возьми суму» звучала так: «тараВОбараЗЬМИтараСУбараМУ». Причем фраза произносилась как можно быстрее, человеку непривычному к такому способу общения понять смысл сказанного было крайне затруднительно. Подобные способы защиты информации с древних времен были распространены не только у государственных служб, но и среди представителей криминального мира в различных странах, в том числе и в России.

Для защиты письменных сообщений использовалась физическая защита, стеганография и шифрование. В качестве гонцов использовались физически крепкие люди, они были хорошо вооружены, нередко гонец следовал в сопровождении охраны. Сами письма скручивались в свитки, которые опечатывались специальными печатями, содержащими надпись «ДЬНЕСЛОВО», что переводится как «скрытое, тайное слово». Такие печати были у многих русских князей, в том числе и у Александра Невского [Соболева, 2002].

Стеганографический метод заключался в запрятывании сообщений. Депеши зашивались в одежду, помещались в подошвы и каблуки обуви и другие места. Об этом, в частности, говорилось в одной из древних новгородских грамот «…человиком грамотку пришли тайно…» [Бабаш, 2002].

К сожалению, шифрованные документы, содержащие информацию государственного характера, относящиеся к эпохе Древней Руси пока не обнаружены. Однако сохранился ряд памятников русской письменности, в которых имеются зашифрованные фрагменты. В основном это летописи и тексты религиозного содержания. В этих источниках тайнопись применяется не столько для обеспечения секретности, сколько для того, чтобы подчеркнуть важность того или иного фрагмента, а также увековечить имя автора или переписчика. Именно эти документы дают возможность описать древнерусские системы шифрования.

---

[1] Интересно отметить, что шифрованные записи в Древней Руси называли «тарабарской грамотой».

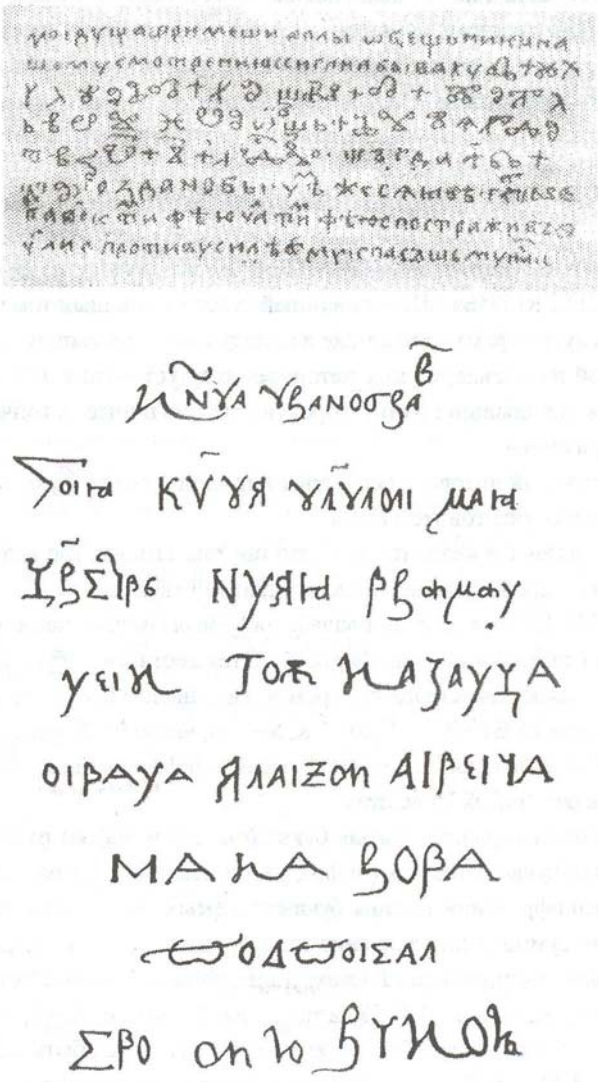
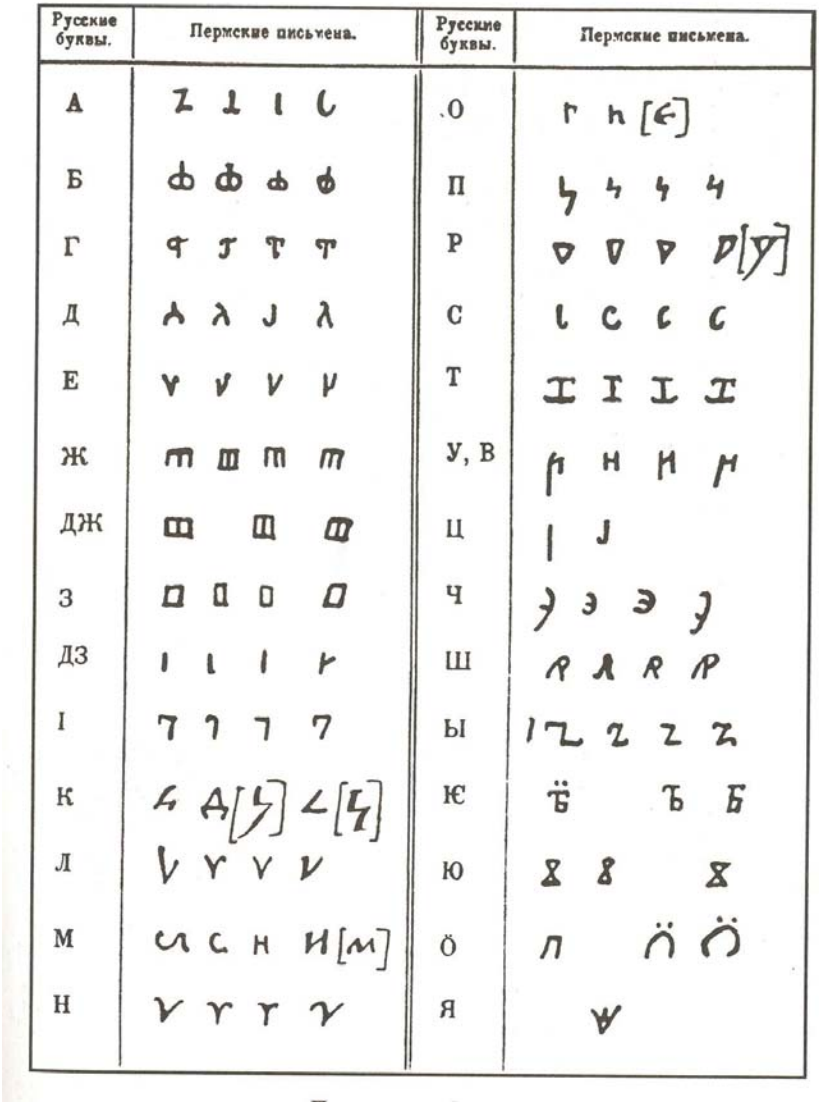


Рис. 1.1. **Текст написанный глаголицей [Бабаш, 2002]**



Русские буквы.	Пермские письмена.	Русские буквы.	Пермские письмена.
А		О	
Б		П	
Г		Р	
Д		С	
Е		Т	
Ж		У, В	
ДЖ		Ц	
З		Ч	
ДЗ		Ш	
І		Ы	
К		Ю	
Л		Ю	
М		Ö	
Н		Я	

Рис. 1.2. **Пермская азбука [Соболева, 2002]**

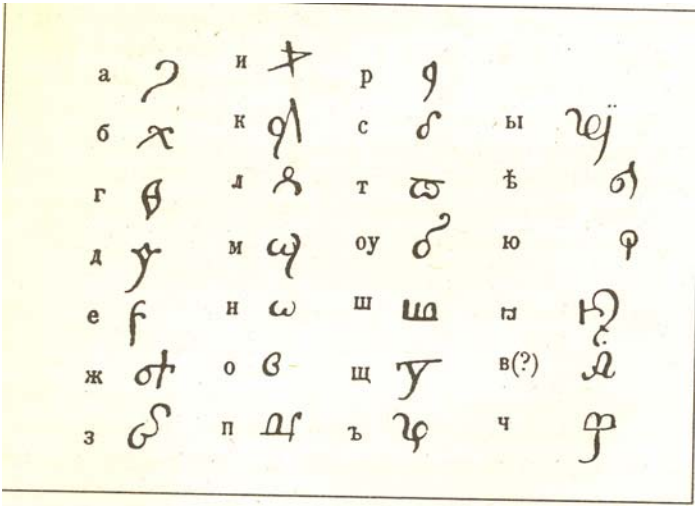


Рис. 1.3. **Ключ к шифру простой замены (1590 год) [Соболева, 2002]**

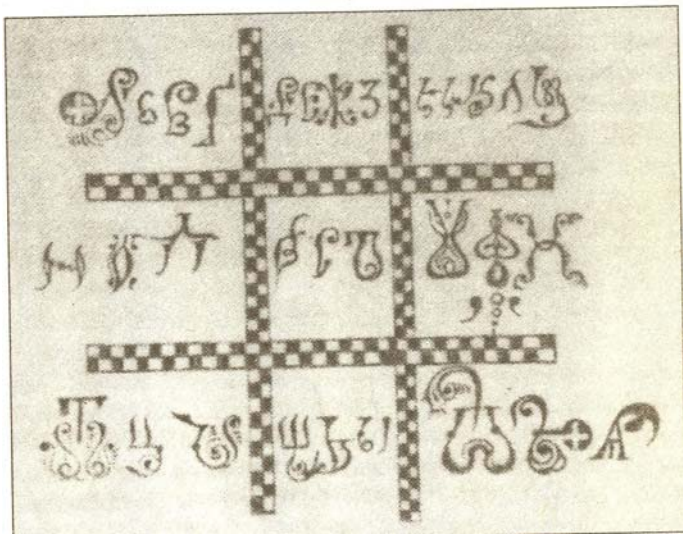


Рис. 1.4. **Открытый текст геометрической системы простой замены (вторая половина XVII в.) [Соболева, 2002]**

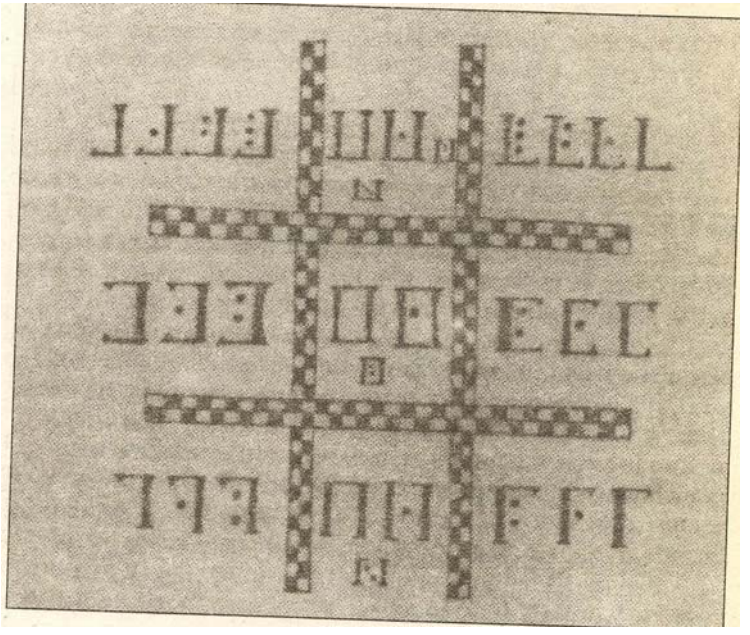


Рис. 1.5. **Шифрованный текст геометрической системы простой замены (вторая половина XVII в.) [Соболева, 2002]**

С древних времен до конца XVII в. основным средством шифрования на Руси были различные варианты шифра простой замены (получившие название «иные письмена»), их можно разделить на три группы.

1. Замена знаков основного русского алфавита – кириллицы[1] на греческие буквы, а позднее латинские. Также была рас-

[1] В принципе и до Кирилла и Мефодия на русских землях существовала письменность (в основном руническая и с помощью иероглифов). Заслуга равноапостольных славянских святых Кирилла и Мефодия, заключается в том, что они приспособили славянскую азбуку, созданную на основе древних славянских рун для христианского богослужения. Появление религиозных книг способствовало распространению грамотности на Руси, что в свою очередь дало толчок развитию науки, искусства и ремесел на Руси.

пространена замена на буквы мало распространенных на Руси алфавитов глаголицы (рис. 1.1) и пермской азбуки (рис. 1.2). Эта азбука была создана епископом Стефаном Пермским в 1372 г. на основе кириллицы, греческого алфавита и древнепермских рунических символов. Некоторое время пермская азбука применялась на северо-востоке европейской части России, но широкого распространения не получила и примерно с XV в. использовалась как тайнопись. Что касается глаголицы, то в XI–XIII вв. глаголицей писали отдельные «наиболее секретные» слова, а в XIV–XVI вв. глаголицей записывались целые фразы и абзацы.

2. Замена знаков открытого текста на специально придуманные обозначения. На рис. 1.3 приведен пример ключа подобного шифра. Здесь написание ряда букв видоизменено, а для некоторых придуманы специальные обозначения. Подобные шифры на Руси назывались **«измененными знаками»**. Этот способ тайнописи в Греции (откуда предположительно он пришел на Русь) назывался **тахиграфией**, он представляет собой изменение начертаний букв, когда писалась или часть буквы, или наоборот, ее написание дополнялось новыми элементами. Часто тахиграфия совмещалась с использованием иностранных алфавитов. Использовалась для тайнописи и такая технология как монокондил или по-другому лигатура. Суть этого метода заключается в соединении при написании нескольких знаков-букв в одно целое. Для увеличения стойкости подобных шифров сообщение нередко записывали справа налево или вверх ногами. Практиковалось также видоизменение знаков письма, которое получило название «вязь». Надо отметить, что подобные системы шифрования нередко сочетали в себе криптографию и стеганографию. Причудливые завитушки, вязь, различные выдуманные знаки противник мог принять за бессмысленные каракули, рисунки и др., а никак не за осмысленный текст.

3. Геометрические системы простой замены, или как их тогда называли **шифры в квадратах**. На рис. 1.4 приведен открытый текст подобной системы, а на рис. 1.5 шифрованный,

вместе они составляют ключ к шифру. Позднее такие системы получили название «масонский ключ».

Все эти виды тайнописи применялись на Руси, однако основной русской системой шифрования стал шифр простой замены, называвшийся «литорея», существовали две разновидности этого шифра «простая литорея» и «мудрая». «Простая литорея» предполагает замену большинства согласных букв кириллицы на другие, взятые из того же алфавита, причем замену производят по определенному правилу. Гласные буквы и некоторые согласные (Й, Ь, Ъ) остаются без изменений. Самым простым и распространенным был следующий ключ. Выписывали в строку подряд все согласные в количестве 10 букв. Под этой строкой составляли вторую строку из последующих 10 согласных, но их записывали в обратном порядке, т.е. справа налево:

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Замена проводится следующим образом: буква из верхней строки заменяется, на соответствующую ей букву из нижней строки и наоборот. Расшифрование осуществляется таким же образом. Для примера воспользуемся фрагментом Ермолинской летописи, датируемой 1463 г., в нем рассказывается о некоем жестоком княжеском слуге: «А прочих его чудес великое множество, невозможно ни описать, ни исчесть — потому что он во плоти есть ЦЬЯШОС (выделено авт.)». Расшифровывая последнее слово по приведенному ключу получаем: ДЬЯВОЛ. Летописец, очевидно, монах, зашифровал это слово, чтобы не поминать нечистого всуе. Замена только согласных букв, осуществлялась для упрощения использования шифра. Вообще согласные в русском языке несут больше информации, чем гласные. Приведем пример. Возьмем некоторое слово и выпишем только гласные, пропущенные согласные обозначим точками:

. А . Я . . А, понять что здесь написано весьма затруднительно, а теперь сделаем наоборот (оставим только согласные):

П . М . ТК . – очевидно, что это ПАМЯТКА (загаданное слово) или ПОМЕТКА.

Самый древний документ, известный на сегодня, и содержащий зашифрованный простой литореей фрагмент, датируется 1229 г. Наиболее широкое распространение этот шифр приобретает в XIV–XV в., а вообще эта шифрсистема использовалась и в XVIII в. Существовали усложнения «простой литореи», когда буквы верхней и нижней строк располагались в случайном порядке.

В «мудрой литорее» замене подлежали все буквы алфавита и гласные и согласные, таким образом, эта система представляет собой классический шифр простой замены [Бабаш, 2002], [Соболева, 2002].

Также на Руси были распространены цифровые, или счетные, системы шифрования, еще их называли «фиоть» или «хвиоть». Цифры в древней Руси записывались с помощью букв кириллицы и греческого алфавита (см. рис. 1.6). Для указания, что буква означает цифру или число, а не звук, над ней ставили особый знак ~, который назывался «титло».

а	б	г	д	е	ѕ	з
аз	ве́ди	глаго́ль	добро	есть	зело́	земля́
1	2	3	4	5	6	7
и	ѳ	і	к	л	м	н
иже́	фита́	и	ка́ко	люди	мысле́те	наш
8	9	10	20	30	40	50
ѯ	о	п	ч	р	с	т
кси	он	покой	червь	рцы	слово	твердо
60	70	80	90	100	200	300
у	ф	х	ѱ	ѡ	ц	
ук	ферт	ха	пси	от	цы	
400	500	600	700	800	900	

Рис. 1.6. **Буквенные обозначения цифр и чисел [Бабаш, 2002]**

Система основана на использовании определенных букв кириллицы, имеющих известное цифровое значение. Такие буквы-цифры для тайнописи раскладывали на слагаемые, обычно «раздваивая», в результате чего вместо одной буквы-цифры записывали две. Например, буква «Д» имела известное значение «4», а после «раздвоения» записывалась двумя буквами, из которых каждая была равна точно половине преобразуемой буквы. Писали рядом две буквы «ВВ», каждая из которых означала «2». Так поступали при зашифровке четных букв-цифр. Для нечетных применяли пары приближенных половинок. Например, вместо буквы «Е» (5) писали «ГВ» (т.е. 3+2). При этом буквы, не имеющие числового значения, не шифровались. В последствии, числовое значение буквы стали разбивать на произвольные слагаемые, причем не на два, а на большее количество. Так например, буква S = 6, помимо традиционного ГГ, могла представляться как АЕ (1 + 5), АВГ (1 + 2 + 3) и др. В результате получается простейшая система многозначной замены, при этом, очевидно, что чем больше числовое значение буквы, тем большим количеством вариантов она может быть представлена в шифрованном тексте [Бабаш, 2002].

С помощью такого шифра увековечил свое имя в 1307 году писец Домид, приписав к написанной в Пскове книге «Апостол» шифрованный текст (для удобства «титло» над буквами-цифрами опущено, а незашифрованное начало фразы переведено на современный русский язык): «а писал ВВ.МЛ.КК.ДД.ВВ.Ъ. ……рекше: двдъ, органъ, мысль, истина...» (последнее слово из-за порчи листа рукописи не читается) [Соболева, 2002].

Ко второй части этой записи мы вернемся чуть позже, а пока расшифруем первую: ВВ = 2 + 2 = 4 = Д, МЛ = 40 + 30 = 70 = О, КК = 20 + 20 = М, ДД = 4 + 4 = 8 = И, ВВ = 2 + 2 = 4 = Д, таким образом мы получаем имя писца Апостола 1307 года: ДОМИДЪ [Симонов, 1977], [Соболева, 2002].

Другим вариантом цифровой тайнописи являлся так называемый описательный, примером его применения может служить текст XV века: «Аще хощеши уведати имя писавшего

книгу сию, и то ти написую: «Десятерица сугубая и пятерица четверицею и единъ; десятерица дващи и единъ, десятья четыре сугубо и четырежди по пяти; дващи два с единем; единица с четверицею сугубо; в семь имени словъ седмерица, три столпы и три души, царь». И сего числа в семь имени РОЕ» [Бабаш, 2002]. Расшифруем эту тайнопись. Слово «сугубо» в те времена было синонимом слова «дважды», таким образом : «десятерица сугубая и пятерица четверицею» это: 10·2 + 4·5 = = 40 = М; «единъ» это 1 = А; «десятерица дващи» – 10·2=20=К, «единъ» это опять 1=А; «десятья четыре сугубо и четырежди по пяти» 10·4·2 + 4·5 = 100 = Р, «дващи два с единем» – 2·2 + 1 = = 5 = Е; единица с четверицею сугубо (1+4) 2 = 10 = і (или в современной транскрипции Й). Тогда имя автора МАКАРЕЙ. Далее следует своеобразный проверочный код: букв в слове 7 столпы и души, означают гласные и согласные, которых в слове по 3, а царь это полугласная Й, и, наконец, РОЕ это 175 – сумма букв-цифр в слове.

Иногда шифрованные записи носили шутливый характер, для примера обратимся к обрывку берестяной грамоты XIII века, найденной в Новгороде [Бабаш, 2002]:

Н	**В**	**Ж**	**П**	**С**	**Н**	**Д**	**М**	**К**	**З**	**Л**	**Т**	**С**	**Ц**	**Т**	**…**
Е	**Ъ**	**Я**	**И**	**А**	**Е**	**У**	**А**	**А**	**А**	**Х**	**О**	**Е**	**И**	**А**	**…**

Если прочитать это сообщение по колонкам, то получаем следующий текст: НЕВЪЖЯПИСАНЕДУМАКАЗАЛХТОСЕЦИТА…, если адаптировать эту фразу к современному русскому языку и разделить слова пробелами, получим:

НЕВЕЖДА ПИСАЛ НЕ ДУМАВ СКАЗАЛ А КТО СИЕ ЧИТА(Л) …, далее очевидно следовал не лестный отзыв об умственных способностях читателя. Для нас этот фрагмент важен тем, что это один из первых случаев применения на Руси шифра перестановки, пусть и в самой примитивной форме.

Самым древним способом сокрытия информации в текстах, использовавшемся на Руси, был акростих. Акростих (от греч. akros – крайний и stichos – строка) – стихотворение, в котором первые буквы строк образуют слово или фразу. Примером

акростиха может служить стихотворение «Загадка акростишная» русского поэта Ю.А. Нелединского-Мелецкого (1752–1829):

Довольно именем известна я своим;
Равно клянется плут и непорочный им;
Утехой в бедствии всего бываю боле;
Жизнь сладостней при мне и в самой лучшей доле.
Блаженству чистых душ могу служить одна;
А меж злодеями – не быть я создана.

Если прочитать первые буквы строк сверху вниз, то получится «секретное» слово ДРУЖБА. Изобретателем акростиха считается известный древнегреческий комедиограф, философ и врач Эпихарм Сиракузский (примерно 550–460 гг. до н.э.). На Русь акростих пришел из Византии и начал широко применяться с XI в., акростих на нашей земле имел множество наименований: началострочие, началограние, краеграние, акростихиада, краестрочие, первобуквие и др. Акростих широко применялся поэтами, авторами и переписчиками книг, составителями надгробных эпитафий, в основном для увековечивания своего имени. В.И. Даль называл акростих иместишием [Соболева, 2002].

Применялся акростих и как средство защиты информации. Фактически применение акростиха можно отнести к стеганографическим методам защиты информации. На слух акростихи не воспринимаются. Чтобы их обнаружить, нужно написанное читать. Читающий заранее знает о существовании в тексте тайнописи, хотя в принципе может ее обнаружить самостоятельно. Древнерусские акростихи отличаются большим разнообразием. Известны многочисленные варианты тех или иных разновидностей акростихов. Так, чаще всего записи проявляются при чтении снизу вверх. Встречаются акростихи, в которых к обычной вертикальной записи добавляется целое слово или даже вся горизонтальная (верхняя или нижняя) строка, написанная открытым текстом – это угловые акростихи. Можно сказать, что у наших книжников акростихи были излюбленным видом тайнописи. Посредством акрости-

хов велась тайная деловая и личная переписка. В качестве примера приведем переписку двух религиозных деятелей – старцев Илариона и Феоктиста. Иларион в своем длиннейшем стихотворении первыми буквами строк выразил просьбу: «Старец господар Феоктист, даи ми книгу списат». Феоктист в ответ сочинил еще более длинное стихотворение, в котором таким же приемом составил ответ: «Старец господар Иларион, потруженная тобою любезне восприях и противу твоего, аще и не тако, но обаче, восписах ти вся, но ты же мя в том проси, никому не возвести» [Бабаш, 2002].

Для защиты информации широко применялись «неправильные акростихи». Такое название они получили потому, что записывались не только первыми буквами строк, но и двумя и более буквами, начинающими строки, и даже первыми слогами и словами строк. Ясно, что такая свобода действий существенно облегчала сочинителю составление весьма пространных тайнописных записей. Но вместе с тем такой произвольный подбор делает невозможным найти какую-то закономерность в чередовании читаемых букв, слогов и слов. Случайность чередования этих элементов исключает возможность правильно составить универсальный ключ. Иными словами, для каждой определенной записи читающий должен иметь тот ключ, которым эта запись составлялась, т.е. это уже криптографическая система защиты информации.

Пример «неправильного акростиха» следующий: Иоанн Величковский (XVII в.) составил различные тайнописи с именем Девы Марии. Одна из них умещается на шести строках (имя Мария повторяется 2 раза и выделено заглавными буквами):

МАти блага,
РИза драга-
Я же нас крыет,
МАлодушных,
РИзо нужны,
Якъ руно греет.

Здесь выделенные буквы или слоги в строках читают слева направо и сверху вниз. При этом первая буква третьей строки (Я) является не началом, а окончанием слова (драга/я).

Авторству Величковского принадлежит и более сложная запись, когда буквы «секретного сообщения» располагаются в произвольном порядке и перемешаны между собой:

*М*ног*А*я **И**з не**СУ**щих **С**озда
сей
тво*Р*ен*ИЯ*
да*ДЕ*
ми **Х**е**Р**у**И**м**С**кую
ТОму
пе**С**нь х*ВА*ления.

Здесь зашифрованы два имени: Мария Дева (выделено заглавными буквами и косым шрифтом) и Исус Христос (выделено заглавными буквами и жирным шрифтом). Очевидно, что прочитать такую тайнопись, не зная ключа крайне сложно.

Помимо стихотворений для сокрытия сообщений стали использоваться обычные тексты (принципы тайнописи те же, что для стихотворений) и даже бессмысленные наборы слов. Вернемся к шифрованной приписке – к Псковскому Апостолу 1307 г., если взять первые буквы четырех последних слов, то получаем ДОМИ, последнее нечитаемое слово, совершенно очевидно начиналось на Д, таким образом, и здесь получаем имя Домид. Переписчик зашифровал свое имя двумя способами – цифровой тайнописью и акростихом [Бабаш, 2002], [Гогешвили, 1991], [Панченко, 1973], [Соболева, 2002].

Обеспечение секретности было необходимо для следующих видов сообщений.

Информация, необходимая для организации государственного управления. Княжеские указы и распоряжения, отчеты с мест и др. В процессе становления русской государственности система управления постоянно совершенствовалась. Киевскому князю подчинялись другие князья (в современном понимании – руководители регионов). Создавались различные службы, регули-

ровавшие различные области человеческой деятельности (торговлю, ремесла, сбор налогов и податей, и др.). Разумеется, в рамках деятельности по управлению государством постоянно возникает необходимость передачи секретной, тайной информации, и наиболее эффективными методами защиты правительственной информации являются криптографические.

Военная информация. В первую очередь передача «ратной вести, своевременном уведомлении о появлении неприятеля, проведении сборов войск» [Астрахан, 1996], а также организация управления войсками во время боевых действий и в мирное время.

Дипломатическая информация. После становления древнерусского государства происходило налаживание связей с другими странами, в первую очередь с соседями. Основным внешнеполитическим партнером древней Руси была Византия (хотя при этом русские князья неоднократно воевали с этим государством), дипломатические отношения периодически поддерживались также с рядом стран Европы, Хазарией и викингами. Примерами дипломатической деятельности Киевской Руси могут служить посольства к византийскому императору Феофилу II в 838 году и королю Франции Людовику Благочестивому (839 г.) [Кудрявцев, 2002]. В это время развивается посольская служба, при этом следует отметить, что в те времена постоянных представителей в других государствах практически не было, послы отправлялись по мере необходимости. После крещения Руси князем Владимиром в 988 г. (отметим, кстати, что само это событие потребовало весьма серьезных дипломатических усилий) в дипломатической деятельности русского государства активно участвует Православная церковь. С усилением могущества древнерусского государства дипломатическая деятельность значительно активизировалась. Так во время правления знаменитого князя Владимира Мономаха (1113–1125 гг.) и его сына Мстислава Великого (1125–1132 гг.) «Русь поддерживала международные связи как с католическими, так и мусульманскими странами. Продолжали действовать союзные договоры с Венгрией и Польшей,

были заключены династические браки с владетельными домами Швеции, Византии, Польши, Венгрии, Германии и других стран» [Кудрявцев, 2002]. Значительное место дипломаты Древней Руси уделяли разведывательной и другой тайной деятельности (заключение тайных союзов и соглашений, вербовка агентуры, подкуп чужих правителей, чиновников и др.). (Подробнее о разведке, чуть далее). Вообще активная внешнеполитическая деятельность способствует развитию методов и средств защиты информации, так как послам и другим дипломатическим работникам приходится работать на территории иностранных государств (в том числе и потенциально или реально враждебных), то обеспечение конфиденциальности передаваемой на Родину информации приобретает крайне важное значение. Прав Д. Кан, утверждая, что «развитие криптографии находится в прямой зависимости от расцвета современной дипломатии». Важность работы криптографов оценили руководители многих государств [Бабаш, 2002].

Разведывательная информация. Важнейшим источником информации для любого государства является разведка. Разведывательную деятельность Киевской Руси можно разделить на стратегическую (агенты на территории иностранных государств, сообщающие политическую и военную информацию) и тактическую (сторожевая служба, сообщающая о приближении неприятеля и передовые отряды войска, ведущие разведку). Примером успешной работы стратегической разведки древней Руси могут служить походы киевских князей на столицу Византии Константинополь или как у нас его называли Царьград. В 860 г. русские дружины предприняли первый поход к столице Византии. Время нападения было выбрано крайне удачно. Византийская армия под предводительством императора Михаила III выдвинулась в Малую Азию для отражения нападения арабов, а флот ушел к острову Крит для борьбы с пиратами. Константинополь остался практически беззащитным. Осада города продолжалась неделю. Император Михаил III вынужден был срочно вернуться из Малой Азии и заключить мир с руссами. По условиям этого договора

Византия выплатила большую контрибуцию и предоставила русским купцам выгодные условия для торговли на территории империи.

Не менее удачным оказался поход легендарного князя Олега, воспетого А.С. Пушкиным. В 907 г. он подошел к Константинополю в то время когда мощный византийский флот отправился воевать с арабами, а полководец Андроник Дука поднял мятеж против центральной власти. Как и в предыдущий раз, дело кончилось контрибуцией и льготами и привилегиями русским купцам в Византии, помимо этого Византия обязалась выплачивать Руси ежегодную дань и содержать русских послов в Константинополе.

Летом 941 г. в поход на Византию отправился князь Игорь и опять лучшие сухопутные части империи и ее флот находились далеко от Константинополя воюя с арабами. К сожалению, в этот раз византийцы сумели получить информацию о нападении и организовать сопротивление. Войско Игоря понесло большие потери и вынуждено было отступить.

В 965 г. князь Святослав совершил поход против хазар, удар был нанесен в очень подходящий момент. Хазарский каганат был истощен ожесточенной борьбой с Византией в Причерноморье и на Кавказе. Русские войска взяли штурмом столицу хазар Итиль, эта победа привела к распаду враждебного Руси государственного образования – Хазарского каганата.

Перечисленные факты однозначно говорят, что русские князья были осведомлены о положении дел в стане врага и могли выбирать удобный момент для нападения. Что касается тактической разведки, то пограничная стража не раз предупреждала руководителей русского государства о нападении врагов, в основном это были кочевники – хазары, печенеги, половцы. О важности организации войсковой разведки в поучении к своим детям писал Владимир Мономах: «На войну вышед, не ленитеся, не зрите на воеводы; ни питью, ни едению не лагодите, ни спанью; и стороже сами наряживайте, и ночь, отовсюду нарядившие, около вои тоже лязите, а рано встанете; а оружья не снимайте с себе вборзе, не разглядевши

ленощами, внезапу бо человек погыбаеть» [Кудрявцев, 2002]. Для ведения разведки русские князья назначали специальных людей из числа дружины. Основной задачей всех видов разведки было предупреждение об агрессии против русского государства и обеспечение подготовки собственного нападения на противника. Задачами тактической разведки были сбор сведений о противнике, разведка дорог, переправ, мест удобных для стоянки войска, наблюдение за противником на поле боя. В древнерусском языке разведчики назывались «прелагатаи» или «соглядатаи» (лица засылаемые князем в стан врага или завербованная агентура) и «просоки» (отдельные воины или небольшие отряды, следившие во время войны за вражеским войском. Передвижение своих войск прикрывалось специальными отрядами, получившими название «сторожа». Разумеется, передача агентурной информации, сообщений с границ, а также информации от войсковой разведки требовала обеспечения их конфиденциальности, в том числе с помощью криптографических методов [Астрахан, 1996], [Кудрявцев, 2002], [Очерки, 1999].

Кстати, оригинальный способ передачи агентурной информации имел место в 988 г. при осаде князем Владимиром, который крестил Русь, греческого города Херсонес. Войско Владимира осадило хорошо укрепленный город, но греки оказывали ожесточенное сопротивление и осада могла продлиться длительное время. Но среди жителей Херсонеса нашелся сочувствующий русским человек по имени Анастас. Он пустил к русскому войску из лука стрелу, с прикрепленной к ней запиской. Текст записки был опубликован знаменитым отечественным историком Н.М. Карамзиным и гласил: «… за вами, к Востоку, находятся колодези, дающие воду херсонцам чрез подземные трубы; вы можете отнять ее» [Очерки, 1999]. Как пишет далее Карамзин «Великий князь поспешил воспользоваться советом и велел перекопать водопроводы… Тогда граждане, изнуряемые жаждою, сдались россиянам» [Очерки, 1999].

А вот пример использования в Древней Руси, такого способа информационной войны, как дезинформация. В 997 г. пе-

ченеги осадили один из русских городов, в этот момент князь с войском отсутствовал. Враги надеялись, что в городе закончится еда и его жители капитулируют. Осажденных спасла, как пишет Карамзин «хитрость умного старца». Этот человек «велел ископать два колодезя, поставить в них одну кадь с сытою (медовый взвар на воде), другую с тестом и звать старшин неприятельских будто бы для переговоров. Видя сии колодези, они (враги – *авт.*) поверили, что земля сама собою производит там вкусную для людей пищу, и возвратились к своим князьям с вестию, что город не может иметь недостатка в съестных припасах» [Очерки, 1999]. Получив такую информацию, печенеги отказались от продолжения осады.

Расширение территории древнерусского государства, а также развитие системы государственного управления требовали совершенствования системы связи. В 920 г. повелением киевского князя был учрежден своеобразный прообраз современной почты – повоз. «Повозная повинность обязывала весь люд (кроме духовенства и бояр) по первому требованию княжеских людей (и в первую очередь гонцов) предоставлять им безвозмездно лошадей, корм, повозки и даже лодки с гребцами, что способствовало ускорению передачи государственных и ратных вестей» [Астрахан, 1996]. Вообще следует отметить, что первая треть XII в. стала для Руси периодом наивысшего расцвета политической и военной мощи государства, экономики, науки и культуры.

К сожалению, в XII в. из-за амбиций князей и роста экономического и политического могущества различных областей Киевской Руси, и последовавшей затем междоусобной борьбы произошел разрыв политического и территориального единства древнерусского государства, которое, в конце концов, распалась на ряд самостоятельных земель и княжеств. На Руси наступил период феодальной раздробленности. Отдельные княжества фактически превратились в независимые государства, которые проводили самостоятельную внешнюю и оборонную политику. Дипломатическая деятельность стала включать не только сношения с зарубежными государствами,

но и отношения с соседними русскими княжествами. В каждом княжестве создавался свой государственный аппарат. Появлялись люди и службы, отвечающие за княжеский двор, хозяйство, финансы, суд, войско и др. В крупных княжествах (Киевское, Новгородское, Владимирское и др.) появились собственные дипломатические «службы», при князьях состоял целый штат переводчиков, которых тогда называли толмачами, и дипломатов, способных отстаивать интересы своих земель при осуществлении посольств и приема иноземных делегаций у себя, имелась также и служба разведки. Система связи была хорошо поставлена во многих княжествах, что позволяло уже во время выдвижения противника к границам княжества готовить войска к отражению нападения. Однако скорость передачи государственной и военной информации была слишком медленной. Требовалась постоянная, надежная более быстро действующая связь [Астрахан, 1996], [Кудрявцев, 2002].

В начале XIII в. на смену повозу пришла ямская гоньба, которая представляла собой конную эстафету и была организована в каждом княжестве. В результате договоренностей между князьями ямская гоньба обеспечивала связь на территории всей Руси. В начальный период монголо-татарского нашествия этот способ связи использовался для координации действий русских князей, к сожалению, вскоре большая часть русских земель оказалось под монгольско-татарским игом, которое задержало политическое, экономическое и культурное развитие Руси на столетия [Астрахан, 1996].

Тем не менее, в этот период ямская гоньба, как эффективное средство для передачи секретной информации, сыграла важнейшую роль накануне и во время сражений ставших поворотными пунктами нашей истории.

В 1239 г. новгородский князь Александр Ярославич, после описываемых событий получивший почетное прозвище Невский, организовал морские дозоры в Финском заливе и на реке Неве, в целях предупреждения нападения с Запада. В начале июля 1240 г. один из дозоров обнаружил в устье Невы шведские корабли. Выяснив место высадки и состав сил врага,

с помощью ямской гоньбы было послано тайное сообщение в Новгород «уведав силу ратных, иде против князя Александра, да скажеть ему станы» [Кудрявцев, 2002]. 15 июля 1240 г. в месте впадения реки Ижоры в Неву произошла знаменитая Невская битва, в которой князь Александр наголову разгромил шведских агрессоров.

После поражения на Неве шведы прекратили на время атаки на Русь, но Новгородское княжество постоянно пробовали на прочность немецкие рыцари-крестоносцы, окопавшиеся в Прибалтике. После захвата немцами Пскова для Новгорода возникала реальная угроза со стороны крестоносцев. В начале 1242 г. Александр Невский начал собирать войска для сражения с Тевтонским орденом и опять тайные вести о сборе войск передавались ямской гоньбой. Внезапным ударом Александр освободил Псков, однако главные силы крестоносцев, при этом еще не вступили в бой. Хорошо поставленная разведка и надлежащим образом сработавшая система связи (ямская гоньба), предоставили Александру Невскому информацию о противнике, что позволило выработать наилучшую тактику для предстоящего сражения. Оно состоялось 5 апреля 1242 г. на льду Чудского озера и получило название «Ледовое побоище». Крестоносцы потерпели тяжелое поражение от русского войска под командованием Александра Невского. Эта победа на долгие годы приостановила экспансию крестоносцев на Восток [Астрахан, 1996], [Кудрявцев, 2002].

Характерным примером использования условной сигнализации, служит случай произошедший в 1261 г., тогда татарский военачальник Бурундай с войском явился на территорию Галицко-волынского княжества, расположенного на юго-западе русских земель. Бурундай предъявил князю Даниилу ультиматум: «Если вы со мною мирны, то размечите (т.е. было велено разрушить укрепления – авт.) все свои города» [Широкорад, 2006]. Чтобы избежать татарского разорения, князь Даниил вынужден был подчиниться. Разрушение укреплений было поручено сыну Даниила Льву и брату Василько, к сожалению укрепления большинства городов были разрушены, но

когда Бурундай и Василько подошли городу Холм, «любимому городу короля[1] Даниила» [Широкорад, 2006], то выяснилось, что жители города хорошо подготовились к обороне и не собирались уступать татарам. Бурундай понял, что взять город теми силами, чт.е. у него не получится. «Тогда он обратился к Василько: «Этот город брата твоего, ступай, скажи гражданам, чтоб сдались». С Василько Бурундай отправил трех татар и толмача, чтобы слушал, что князь говорит горожанам. Но Василько не растерялся: набрал каменей в руки и, подъехав к стенам, стал кричать холмским боярам: «Константин холоп, и ты другой холоп, Лука Иваныч! Это город брата моего и мой, сдавайтесь!». Сказав это Василько три раза ударил камнем о землю (это был условный сигнал не верить его словам – *авт*.), давая этим понять, чтобы не сдавались, а бились с татарами. Боярин Константин все понял и отвечал Васильку: «Ступай прочь, если не хочешь, чтоб ударили тебя камнем в лицо, ты уже не брат королю, а враг ему». Татары, бывшие с Василько, все пересказали Бурундаю (про условный знак они ничего не знали и не обратили на бросание камней внимание – *авт*.), и тот ушел от Холма пограбить Польшу, а оттуда возвратился в степи» [Широкорад, 2006].

Важнейшую роль система разведки и связи сыграла во время подготовки Куликовской битвы. Московский князь Дмитрий Иванович (после победы на Куликовом поле ставший Дмитрием Донским) еще в начале 1370-х гг. организовал целую систему защиты границы Московского государства (проходившую тогда по реке Оке) от нападений ордынцев. Она включала в себя «сторожи крепкие», «заставы», которые выдвигались далеко в степь для наблюдения за передвижениями ордынских войск, пограничные крепости (Коломна, Серпухов и др.) а также организацию связи с этими отрядами

[1] В 1257 г. Папа Римский даровал Даниилу королевскую корону, в надежде, что тот перейдет в католичество, католиком Даниил так и не стал, но тем не менее Даниил и его потомки стали единственной королевской династией на Руси [Широкорад А.Б., 2006, с. 161–162].

с помощью особых посыльных, а с крепостями – ямской гоньбы. Для быстрой и эффективной мобилизации войска Д. Донской приказал учредить разрядные книги, «подробные росписи полков и воевод, благодаря которым были точно известны районы мобилизации, а так же состав и численность участников похода» [Кудрявцев, 2002].

23 июля 1380 г. в Москву прискакал ««сторож крепкий» Андрей Попов, сын Семенов и сообщил: «Идет на тебя государь, царь Мамай со всеми силами ордынскими, а ныне он на реке на Воронеже» [Кудрявцев, 2002]. После получения этой информации по всей Руси по ямским трактам полетели гонцы с секретными грамотами Московского князя о сборе войск для отражения ордынского нашествия. С целью выяснить дальнейшие планы врага выиграть время для сбора войск князь Дмитрий послал к Мамаю «юношу, доволна суща разумом и смыслом, имянем Захарию Тютьшова» [Кудрявцев, 2002]. Захарий должен был вручить Мамаю большие дары и начать переговоры с ордынцами пытаясь убедить их в покорности Московского князя хану. Для переговоров вместе с Тютчевым были посланы «два толмача, умеюща языкъ половетцискый» [Кудрявцев, 2002]. По пути в Орду Тютчев получил информацию об измене рязанского князя Олега и союзе с Мамаем литовского князя Ягайло. Эта важнейшая информация была доведена до князя Дмитрия, Захарий «послављ скоро вестника тайно к великому князю» [Кудрявцев, 2002][1].

Получив это сообщение, князь Дмитрий решает нанести удар по Мамаю до соединения его полчищ с войсками Олега и Ягайло. Тем временем передавая стража продолжала наблюдение за основными силами Мамая, подтверждая, что хан не

[1] Отметим, что Тютчев продолжил путь в Орду и прибыл к Мамаю. Дары и уверения в покорности Московского князя были отвергнуты ханом, за смелые и достойные ответы на резкие выпады Мамая в отношении Московского князя Тютчев, был чуть не убит, но благодаря хитрости Захарию удалось избежать смерти и вернуться на Русь [Очерки, 1999, с. 18].

торопится идти на Москву, кочует у реки Воронеж, ожидая подхода союзников. В середине августа 1380 г. русские войска собрались в Коломне и оттуда форсированным маршем двинулись на встречу врагу. Движение войска сопровождалось постоянным получением информации о противнике от «сторожи» и специально высланных для разведки передовых отрядов. Благодаря грамотной организации разведки и связи князю Дмитрию с войском удалось раньше Мамая прибыть на место предполагаемого сражения и занять более выгодную тактическую позицию, а также не допустить соединения ордынцев с войсками Ягайло и Олега. 8 сентября 1380 г. на Куликовом поле состоялось знаменитое, сражение, которое закончилось полной победой русского войска. Эта победа стала началом избавления Руси от монголо-татарского ига (хотя до полного избавления от него потребовалось еще 100 лет) и открыло путь к дальнейшему развитию русской государственности и превращении нашей страны в мощную державу. [Астрахан, 1996], [Кудрявцев, 2002], [Очерки, 1999].

Одним из немногих общественно-политических документов, где имеются шифрованные фрагменты является «Второе послание митрополита Киприана[1] 23 июня 1378 года». После кончины митрополита Алексия Киприан стремился занять высокий духовный пост в Москве. Против Киприана выступал московский князь Дмитрий Иванович. Киприан искал поддержки у игумена Троицкого монастыря Сергия Радонежского и игумена Симонова монастыря Федора, и отправитель, очевидно, учитывал, что содержание послания могло стать известным князю. Во избежание неприятностей Киприан отдельные части текста зашифровал. Им были сокрыты имя одного из адресатов (Сергия) и духовный сан другого (Федора), а также некоторые слова и предложения.

---

[1] Киприан (ок. 1336–1406), религиозный деятель, русский митрополит в 1380–1382 и с 1390 гг., в 1382 г. руководил неудачной обороной Москвы от нашествия хана Тохтамыша. Активный сторонник сына Дмитрия Донского, великого князя Василия I [Кудрявцев, 2002], [Словарь, 1984].

Этот документ интересен тем, что в нем обнаружено 8 мест, зашифрованных простой литореей, при этом использовались разные ключи! Рассмотрим послание подробнее. К сожалению, до нас дошли лишь копии (их также называют списками) «Послания». Всего их сохранилось четыре – Мясниковский (начало XV в., наиболее древний) и три более поздних – Основной, Чудовский и Барсовский (они датируются концом XV – началом XVI вв.). Во всех списках имеются шифрованные записи. Больше всего тайнописи осталось в древнейшем списке – шесть фрагментов, в остальных – по две-четыре записи. Сколько же было зашифрованных мест в исходном тексте, написанном митрополитом Киприаном – неизвестно.

В Мясниковском и Чудовском списках простейшим ключом (приведенным ранее) сделана единственная запись: «шлея мули гелкъпору...» При расшифровании получаем: «Всея Руси честъному...» В двух других списках этот фрагмент приведен уже в расшифрованном виде.

В «Послании» имеются еще три записи, в которых применен тот же простейший ключ, однако в словах заменялись не все согласные, а лишь часть: «...игумену Семчию и ичурепу Федору... (т.е. ...игумену Сергию и игумену Федору...)». Вторая запись: «...едипъруцмепъ л шари. Не укаисъля от шал... (...единомудрен с вами. Не утаилося от вас...)». И третья запись всего в одно слово: «мода (рода)». Ясно, что если в таком частично дешифрованном тексте произвести, согласно простейшему ключу, замену всех согласных, то вместо расшифрованного текста получится новая тайнопись. Для чтения нужен именно тот ключ, которым пользовался сочинитель тайнописи. Все эти три тайнописи содержатся только в одном – древнейшем списке, а в более поздних они либо опущены полностью или частично, либо приведены в расшифрованном виде. В Барсовском списке «Послания» есть два отдельных слова, зашифрованных усложненным ключом: «вобдввсни (неблагословенни)» и «пбокдати (прокляти)». Наконец, в «Послании» приведены еще две шифрованные записи: «Одеюрееви мивропродиву (Олексееви митрополиту)» и «Дв оудушь отдумени

(Да будут отлучени)». Заметим, что во второй из этих записей переписчик допустил несколько ошибок, написав: «дщ вудушь отдумини». Ключ к этим двум записям настолько сложен, что ни один из четырех переписчиков не расшифровал их – они в зашифрованном виде сохранились во всех списках.

Столь подробное рассмотрение здесь зашифрованных литореей фрагментов в разных списках «Второго послания митрополита Киприана 23 июня 1378 г.» нужно, чтобы показать, что, во-первых, применявшиеся для шифрования ключи даже в одном документе разнообразны. Во-вторых, переписчики вмешивались в текст тайнописи, в большинстве случаев его расшифровывали, иногда лишь частично, а также при переписке допускали ошибки, затрудняющие понимание написанного, или вовсе отбрасывали непонятное.

Подведем некоторые итоги. В процессе становления и развития русского государства в IX–XIV вв. криптографическая деятельность играла весьма важную роль в организации системы государственного управления, передачи военной, дипломатической и разведывательной информации. Главным достижением данного периода является создание на Руси достаточно надежной и эффективной системы связи – повоза, а в последствии – ямской гоньбы. Из приведенных примеров можно сделать однозначный вывод, что, ямская гоньба сыграла весьма существенную роль в процессе преодоления феодальной раздробленности Руси и создания Московского государства. Она была одним из ведущих средств государственного управления.

Для обеспечения секретности передаваемой информации использовались различные методы, в том числе криптографические, однако следует отметить, что время регулярных служб по защите информации еще не пришло. Мероприятия по защите информации проводились по мере необходимости, при этом выбор того или иного способа защиты информации осуществлял сам князь или довольно ограниченный круг его доверенных людей, они же и осуществляли подобные мероприятия, в том числе шифрование и расшифрование тайных

сообщений. Не существовало каких-либо универсальных подходов к выбору методов и средств защиты информации, все зависело от определенной ситуации и в схожих случаях могли приниматься совершенно различные решения. С усилением русского государства, его военной и экономической мощи, расширения масштабов внешнеполитической деятельности потребовало проведения мероприятий по защите информации на регулярной основе, пониманию того, что этим должны заниматься специально подготовленные люди и службы. О создании и работе первой криптографической службы нашей страны будет рассказано в следующей главе.

Список рекомендуемой литературы

1. Астрахан В.И., Гусев В.В., Павлов В.В., Чернявский Б.Г. Становление и развитие правительственной связи в России. – Орел: ВИПС, 1996.
2. Бабаш А.В., Шанкин Г.П. История криптографии. Ч. I. – М.: Гелиос, 2002.
3. Гогешвили А.А. Акростих в «Слове о полку Игореве» и других памятниках русской письменности XI–X III веков. – М, 1991.
4. Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Криптография: страницы истории тайных операций. – М.: Гелиос АРВ, 2008.
5. Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптография в эпоху Наполеона // Математика для школьников, №1. – М.: 2009, с. 46-55.
6. История военной связи / под общей редакцией А.И. Белова. – М.: Воениздат, 1984.
7. Кан Д. Война кодов и шифров. – М.: РИПОЛ КЛАССИК, 2004.
8. Кудрявцев Н.А. Государево Око. Тайная дипломатия и разведка на службе России. – М., ОЛМА-ПРЕСС, 2002.

9. Очерки истории внешней разведки в 5 т. / под ред. Е.М. Примакова и С.Н. Лебедева. – М.: «Международные отношения», 1999.
10. Панченко А.М. Русская стихотворная культура XVII века. – Л., 1973.
11. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа. – М.: КРОН-ПРЕСС, 1999.
12. Симонов Р.А. Математическая мысль Древней Руси. – М., 1977.
13. Советский энциклопедический словарь. М., Советская энциклопедия, 1984.
14. Соболева Т.А. История шифровального дела в России. – М.: ОЛМА-ПРЕСС-Образование, 2002.
15. Сперанский М.И. Тайнопись в юго-славянских и русских памятниках письма. Энциклопедия славянской филологии. Вып. 3-4. – Л., 1929.
16. Черняк Е. Пять столетий тайной войны. – М.: Международные отношения, 1991.
17. Чудинов В.А. Вселенная русской письменности. – М.: АЛЬВА-ПЕРВАЯ, 2007.
18. Широкорад А.Б. Дипломатия и войны русских князей. – М.: Вече, 2006.

Глава 2.

Российская криптография XIV–XVIII вв.

2.1. Становление криптографии в Российском государстве

В XIII–XIV вв. в связи с распространением грамотности на Руси зародилась и начала развиваться почтовая переписка. Князья, духовенство, знатные люди писали грамоты на дорогом пергаменте. Послание скатывалось в трубочку, зашивалось в холщевый чехол и запечатывалось восковой печатью. Гонец вез грамоту в специальном мешочке на груди или в дорожной сумке-калите. Большая часть населения использовала для письма бересту.

Тайное частное послание переписывалось с помощью специально нанятого человека. В одном из обрывков новгородской грамоты есть такие слова «...человеком грамотку пришли тайно...».

Иван Грозный

Во время царствования Ивана IV Грозного (1530–1584 гг.) осуществлялись крупные дипломатические и военные акции – покорение Астраханского и Казанского ханств, Ливонская война, установление торговых связей с Англией и некоторыми другими государствами, присоединение Сибири. Все это, естественно, оказало влияние на дальнейшее развитие конфиденциальной государственной и военной связи.

Этой же цели служило и упорядочение несения службы на границах Московского государства. 16 февраля 1571 г.

был утвержден Приговор (устав) «О станичной и сторожевой службе», установивший расписание доставки гонцами и сторожами имеющих государственное значение вестей из столицы на места и обратно.

Доставка ратных вестей в большие города и центры государства кроме гонцов и сторож осуществлялась также с помощью ямской гоньбы, которая получила дальнейшее развитие и была независима от разведки и сторож. В 1550 г. был основан Ямской приказ – центральное учреждение в России, ведавшее почтовыми сообщениями. К важным центрам государства и пограничным городам были проложены ямские тракты.

Следует подчеркнуть, что ямская гоньба в Российском государстве была учреждена исключительно для нужд правительства и для проезда послов иностранных государств. Право пользования ямскими подводами определялось особыми грамотами, называвшимися подорожными, которые появились еще до учреждения ямской гоньбы и выдавались обычно только княжеским гонцам или другим должностным лицам, выполнявшим аналогичные поручения. Наличие подорожных грамот у гонцов способствовало более успешному выполнению возложенных на них обязанностей по срочной доставке особо важной правительственной корреспонденции. Тем более, что подписывались такие грамоты, как правило, великими князьями, а в дальнейшем царями. Роль правительственных гонцов в рассматриваемый период могли выполнять не только ответственные должностные лица ямского приказа, но и военные курьеры военного ведомства (разрядного приказа).

Кроме основных ямских направлений в XVI в. существовали и другие, второстепенные направления к городам, имевшим политическое, военное и экономическое значение. Ямская гоньба использовалась также для связи с появившимися в середине XIV в. на восточной и юго-восточной окраинах государства казачьими войсками (запорожскими, донскими, кубанскими, терскими).

Ко времени правления Ивана Грозного, понимавшего, что ведение «большой политики» немыслимо без соблюдения

государственной тайны, относится и начальный этап становления криптографии в России, как явления государственного. Образованный в 1549 г. Посольский приказ, отвечавший, в числе прочего, за организацию посольской и внутриполитической шифрованной переписки, обеспечивал весьма высокий уровень ее конфиденциальности.

Таким образом, в XVI в. в России впервые сложилась довольно стройная система связи высших органов управления централизованным государством, обеспечивавшаяся специальными категориями служилых людей следующих структур исполнительной власти:

- ямского приказа (почтового ведомства) – организационное обеспечение системы ямской гоньбы и доставка корреспонденции второстепенного значения;
- разрядного приказа (военного ведомства) – доставка особо важной правительственной корреспонденции военными курьерами (гонцами);
- посольского приказа (внешнеполитического ведомства) – организация и обеспечение криптографической защиты внешне- и внутригосударственной переписки.

В XVI в. царь Иван Грозный проявлял большую заинтересованность в добывании секретной информации противников России. Сохранилось любопытное письменное свидетельство некоего М. Литвина о делах того времени. Вот, что он пишет: «У нас (в Литве) большое число московских перебежчиков, которые, разузнав наши дела, средства и обычаи, свободно возвращаются к своим, пока они у нас, тайно передают наши планы… Между московскими перебежчиками… был один священник, который пересылал князю своему (И. Грозному) с договоров, указов и других бумаг, тайно добытых в королевской канцелярии, копии… Хитрый этот человек (Иван IV) назначил награду возвращавшимся перебежчикам, даже пустым и бестолковым: рабу – свободу, простолюдину – дворянство, должнику – прощение долгов, злодею – отпущение вины…» [Очерки, 1999].

В XVII в., вопреки желанию российского государя, поляки выбрали королём воеводу Я. Собеского. Российский посол в

Польше (резидент-представитель) В. Тяпкин посылал царю Алексею Михайловичу сведения (в шифрованном виде).

У Яна Собеского возникли подозрения против Тяпкина. Его служба перехвата и дешифрования предоставила ему информацию о негативных для короля посланиях Тяпкина. При личной встрече с Тяпкиным Собеский гневно высказал своё недовольство тем, что тот писал «ссорные и затейные письма к царю, от которых до сих пор войска наши не соединились и взаимная между нами дружба не могла утвердиться».

Некоторые историки предполагают, что информация о содержании писем Тяпкина дошла до поляков через агентурные каналы. Среди русской верхушечной знати были сторонники сближения с Польшей, представлявшие для польских разведчиков определённую «питательную среду» [Очерки, 1999].

При царе Алексее Михайловиче, втором царе из династии Романовых, был создан приказ тайных дел (1654 г.). В ведении Приказа находилась и шифровальная служба государя.

При Алексее Михайловиче бежал за границу один из служащих, имевших доступ к материалам тайного приказа. Он кормился за рубежом за счет продажи своих сенсационных «откровений». В частности, он сообщил следующее: «А устроен тот приказ при нынешнем царе для того, чтобы его царская мысль и дела исполнялись все по его хотению, а бояре б и думные люди о том ничего не ведали». Таким образом, шифровальное дело находилось под личным контролем царя, и никто из его окружения доступ к нему не мог иметь. Так сохранялась тайна секретной переписки государства. К ней не допускались даже члены боярской думы. И это было вполне оправдано.

В январе 1664 г. шведский представитель в Москве в своем донесении королю Швеции писал о том, что у него появился тайный и ценный осведомитель. Он отмечал: «Оный субъект, хотя и русский, но по своим симпатиям добрый швед… обещался и впредь извещать меня обо всем, что будут писать русские послы и какое решение примет Его царское Величество…»

Этим осведомителем являлся Г.К. Котошихин, служащий Приказа Тайных дел (или Посольского приказа.) Он получал

весьма скромное денежное содержание, но весьма добросовестно выполнял свои служебные обязанности. Однако за небольшую ошибку в царском документе (неточное наименование царских регалий) по царскому указу был «бит батогами».

Обида на царя и недостойное материальное содержание толкнули Котошихина на измену. Он перешел на сторону шведов, противников России. Шведы щедро оплачивали информацию, представляемую своим новым агентом. Однако он вскоре был вынужден бежать в Швецию.

В Швеции Котошихин прожил недолго. В 1667 г. он был казнен по приговору шведского суда за умышленное убийство шведского подданного.

«Какъ царю случиться о чемъ мыслити тайно… и въ той думъ бываютъ тъ бояре и окольничіе ближніе, которые пожалованы изъ спальниковъ, или которымъ приказано бываетъ приходити; а иные бояре и окольничіе думные люди въ тое палату, въ думу и ни для какихъ ни буди дълъ не ходятъ, развъе царь укажетъ»

Котошихин

[Князьков, 1914, с. 160].

В это же время была организована система регулярного перехвата и перлюстрации (тайное вскрытие и копирование) корреспонденции зарубежных представителей, находившихся в России. В.О. Ключевский пишет об этом, ссылаясь на свидетельства иностранцев: «письма…, якобы вскрывались, прочитывались и потом уничтожались» [Очерки, 1999]. Здесь стоит высказать гипотезу, что уничтожались как раз шифрованные письма, которые в приказе тайных дел прочитать не могли и действовали по принципу: «так не доставайся ж ты никому».

После кончины царя Алексея Михайловича в 1676 г., тайный приказ, ведавший секретной перепиской, был упразднен. По вполне понятным причинам среди бояр было немало людей, которые спешили ликвидировать и его архив. Тем не менее, один из бывших руководителей приказа дьяк Д. Башмаков сумел сохранить для потомков мешок с «тайными азбуками» – шифрами. Он передал его наследнику – бу-

дущему царю Петру I. Петр I очень внимательно отнесся к этим бумагам. Опыт отца в защите информации он эффективно использовал [Очерки, 1999].

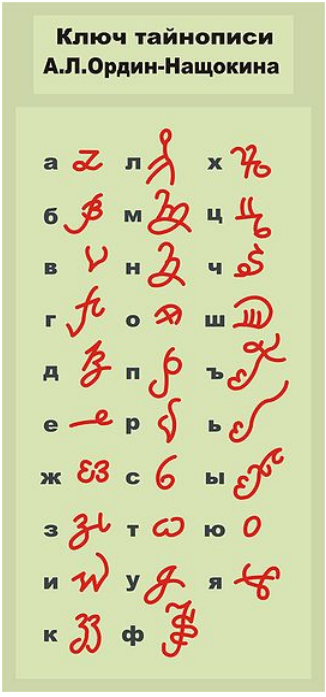


Рис. 2.1. **Ключ тайнописи русского дипломата А.Л. Ордин-Нащокина (XVII в.)**

2.2. Русская криптография в эпоху Петра Великого

Император Петр Великий (1672–1725) вошел в историю России как великий реформатор. Главным итогом петровских реформ стало преодоление серьезного отставания России от европейских держав в военной, экономической, политической

областях. Петр I коренным образом изменил структуру государственного управления и исполнительной власти русского государства, создал боеспособные армию и флот, сумевшие в ходе Северной войны одержать победу над Швецией, имевшей одну из лучших армий в Европе. Во время правления Петра произошел существенный прорыв в экономике России, было создано множество предприятий, мануфактуры, оружейные заводы, металлургические и горнодобывающие предприятия, верфи для строительства кораблей и др. Серьезный импульс получило развитие торговли, в том числе и международной. Огромное значение Петр придавал повышению образовательного уровня населения России. По его инициативе открывались учебные заведения, была учреждена Академия наук, сотни молодых людей отправились учиться за границу, с другой стороны в Россию было приглашены для работы и преподавательской деятельности многие иностранные специалисты. Особо следует отметить дипломатическую деятельность первого русского императора, как пишет историк Н.Н. Молчанов [Молчанов, 1984]: «В сфере дипломатии особенно наглядно обнаружились результаты его (Петра – *авт.*) титанической работы по укреплению могущества России, превратившейся в великую державу». Разумеется, эффективное государственное управление, военные победы и дипломатические успехи были бы невозможны без активной криптографической деятельности. Петр это отлично осознавал и уделял большое внимание криптографии как надежному средству сохранения государственных секретов [Буганов, 1989], [Словарь, 1984], [Соболева, 2002].

Император
Петр Великий

Напомним, что Петр вместе со своим сводным братом Иваном был провозглашен царем в 1682 г., а реальную власть получил в 1689 г. В 1721 г. Петр стал императором. С детских лет он проявлял большой интерес к науке, технике, военному делу. Петром были созданы «потешные» полки, ставшие впоследствии основой новой русской армии. Он построил на Яузе ботик – «дедушку русского флота». В 1687 г. под руководством, жившего в России, голландца Франца Тиммермана Петр начинает изучать математику, артиллерию, фортификационное дело. Большое значение для повышения образовательного уровня молодого русского царя, стало его участие в Великом Посольстве 1697–1698 гг. В ходе этой поездки Петр посетил ряд европейских стран, в том числе наиболее передовые на тот момент Англию и Нидерланды. Петр сумел ознакомиться с различными типами государственного устройства европейских стран, изучить состояние их армий, дипломатическими приемами, развитием науки и техники (особенно интересовали Петра знания в области кораблестроения, навигации и другие вопросы создания военного флота). Безусловно, высокий уровень образования Петра сказался и на криптографической деятельности в России, так в частности Петр сам изобретал шифрсистемы, заставлял заниматься этим своих соратников, и даже лично проводил криптоанализ некоторых русских шифров для оценки их стойкости.

Заметим, что Петр I считал шифры монополией царя российского. Он строго наказывал своих подданных за использование «негосударственных» шифров («цифирей»). Однако частные лица все же пользовались собственными шифрами. Среди них можно указать царевну Софью Алексеевну, которая использовала шифр в переписке со своим фаворитом князем В.В. Голицыным.

К концу XVII в. Россия становится самой крупной европейской державой, занимающей огромную территорию от Днепра на западе и до Тихого океана на востоке. Для организации эффективного управления этой огромной территорией в первую очередь была необходима быстрая, надежная и

конфиденциальная связь. Основным средством передачи сообщений в это время была почта. Наиболее распространенным методом защиты информации являлась физическая защита. Ямщики отвечали за сохранность почты и целость печатей, и здесь они порой попадали в тяжелые ситуации.

В июне 1684 г. почтарь Алексей Вахуров был захвачен лесными разбойниками по пути в город Клин. Разбойники сорвали с почтовых сум печати, но, убедившись, что денег нет, бросили их, забрали всех лошадей и сбежали. Подобрав сумки, ямщик направился пешком в Клин и через 10 часов явился к воеводе Я. Алфимову. Воевода допросил ямщика, осмотрел сумы с письмами. Вся корреспонденция оказалась нетронутой. Алфимов отрядил стрелков в погоню за разбойниками и сообщил обо всем в Москву.

Гораздо хуже пришлось ямщику А. Котку, которой вынужден был прошагать пешком по весенней распутице 68 верст от Клина до Москвы. В январе 1692 г. Петр I своим указом назначил начальником почты «виленской и рижской» А. Виниуса. А уже в апреле того же года Виниус отправил в Посольский приказ депешу, в которой сообщил следующее. Пришел к нему на двор пеший ямщик хотеловского яма Алексей Коток с почтовыми сумками. Одна из них оказалась распечатанной. Почтарь сказал, что эту сумку он принял в таком виде у зимнегорского охотника (ямщика по вольному найму) Данилки Савельева. На следующей почтовой станции в Вышнем Волочке с Котком не стали разговаривать и велели отправляться дальше с испорченной почтой. То же сделали в Торжке и Твери, а в Клину не дали даже подвод, и пошел ямщик пешком в столицу. Но он, Коток, ни в чем не виноват – в его подорожной записано, что крестецкий ямщик Ивашка Анкудинов принял сумы в целости, а передал зимнегорскому почтарю одну сумку распечатанной. Виниус просил назначить следствие. При расследовании выяснилось, что в пути лошадь Анкудинова поскользнулась на мосту и упала на бок. В результате на одной сумке сломалась печать. Злого умысла в нарушении печати нет. Тем не менее, Анкудинова наказали – «били батогами» [Вигилев, 1977].

Другим способом защиты информации было введение цензуры. Предпоследнее десятилетие XVII в. в России сложилась весьма тяжелая внутриполитическая обстановка. Три человека считались главой государства – царевна Софья и два царя (среди них – будущий император Петр I), наводили свои порядки стрельцы, поговаривали о будущей войне с Крымом. Все слухи могли проникнуть за границу и вызвать там нежелательный резонанс. Поэтому правительство приняло решение о введении гласной почтовой цензуры писем, отправленных в западноевропейские страны, цензуры явной, а не тайной перлюстрации, которая широко применялась на почтовых дворах Западной Европы.

В 1690 г. думный дьяк посольского приказа Е.И. Украинцев составил указ смоленскому воеводе окольничему Ф. Шаховскому такого содержания: «А буде о каких своих делах шляхте или мещанам доведется кому за рубеж писать, и они б те грамотки приносили незапечатаны, и те грамотки посылать ему, Ивану Кулбатскому (отпускавшему почту из Смоленска – авт.) с ведома воеводы... А без его воеводы ведома шляхте и мещанам никому за рубеж ни о каких вестях с ездоками и с почтою не писать. И тем людям, также и переводчику И. Кублатскому, от великих государей быть в опале и, смотря по делу, которое в грамотках явится, быть в жестоком наказании». Такая же цензура проводилась и в Москве [Вигилев, 1977].

Впоследствии Петр пошел еще дальше, он издал закон «о донесении на тех, кто запершись пишет, кроме учителей церковных, и о наказании тем, кто знал, кто запершись пишет, и о том не донесли». Лиц «писавших запершись» квалифицировали как политических преступников, независимо от того, что они писали [Лурье, 2006].

При этом интересно отметить, что Петр I в 1698 г. издал почтовый указ, повелевающий «отнюдь ничьей грамотки не распечатывать и не смотреть...» при этом «курьер должен был, как можно меньше знать, что он перевозит, и быть очень довольным оплатой своего труда» [Бабаш, 2002].

В духе этого указа поступили и в таком случае. Вдовствующая царица Прасковья (вдова умершего в 1697 г. Ивана)

состояла в тайной переписке со своим фаворитом. Один подьячий поднял случайно оброненную записку. Подьячего жестоко наказали. Правда, и фаворита отправили в ссылку. Сам же Петр не очень-то следовал своему указу, так как вся иностранная почта доставлялась в Посольский приказ для вскрытия и досмотра.

С созданием регулярной армии возникла настоятельная потребность в необходимости совершенствования управления войсками в мирное и военное время. Уже во время азовских походов против турок в 1695 и 1696 гг. Петр I впервые организовал работу военно-полевой почты, возглавлял ее первый русский почтмейстер А.А. Виниус. Отправления по линии этой почты назывались чрезвычайными [Астрахан, 1996].

Особое значение при Петре I для защиты информации во время военных походов и дипломатической деятельности приобрела криптография.

В конце XVII века центром криптографической деятельности России был Посольский приказ. Здесь создавались шифры, вручались или рассылались корреспондентам ключи, осуществлялось зашифрование отправляемых документов и расшифровка входящей корреспонденции, для этого в приказе имелись специальные сотрудники. В документах того времени достаточно часто употребляется слово «перевод» в значении «расшифрование», и упоминаются «переводчики» – лица, занимающиеся не только собственно переводом корреспонденции, но и расшифровкой. Так, например, переводчиком польских писем являлся некто Голембовский. Он же расшифровывал, получаемые из Польши письма. Вице-канцлер, П.П. Шафиров, отсылая Г.И. Головкину письма польских министров, писал: «А цифирь такая, чаю, есть у Голембовского» [Соболева, 2002].

Шифры использовались во время Азовских походов и Великого Посольства. Однако наибольшие потребности в осуществлении криптографической деятельности возникли в начале XVIII в., когда за рубежом появились дипломатических представительства России, с которыми необходимо было поддерживать связь.

В 1700 г. началась Северная война со Швецией, что потребовало организации эффективного управления войсками на весьма значительном театре военных действий, а также координации действий с союзниками, и здесь нельзя было обойтись без шифров. И, наконец, реформы системы государственного управления огромной страной, также требовали обеспечения секретности переписки внутри страны.

Для повышения эффективности управления государством и дипломатической деятельности начале XVIII в. Петр учреждает Походную посольскую канцелярию, ее создание было вызвано частыми поездками русского государя. Это учреждение было преимущественно личной канцелярией царя. Именно оттуда исходили его важнейшие распоряжения, касавшиеся всех сфер управления государством, в канцелярию направлялась информация из всех управленческих структур России, а также отчеты о выполнении тех или иных распоряжений государя. Однако главная функция канцелярии была дипломатическая деятельность, поэтому в названии фигурирует слово «посольская». Походная посольская канцелярия становится центром российской криптографической деятельности, именно здесь сосредоточивается вся работа по шифрованию и расшифрованию переписки Петра и других руководителей государства с различными корреспондентами в России и за рубежом, а также по созданию шифров и рекомендаций по их использованию. О месте расположения канцелярии указывалось коротко, но ясно «Пребывает там, где Его Величество» [Матвеев, 2001]. Вместе с тем в Москве продолжает функционировать Посольский приказ, через который по-прежнему проходила некоторая часть шифрованной переписки. Согласно книге [Соболева, 2002] первое упоминание о канцелярии в документах датируется 1702 г. в связи с поездкой Петра в Архангельск, руководил канцелярией глава Посольского приказ и первый министр Ф.А. Головин.

Шифрсистемы, которые применялись в России в эпоху Петра Великого, как и в прежние годы, основывались на простой замене, т.е. знаки открытого текста заменялись на буквы (при этом буквы могли принадлежать как алфавиту открыто-

го текста, так и другой азбуки), цифры или специально придуманные знаки. При этом следует отметить, что в шифрах Петровской эпохи употреблялись только, привычные нам, арабские цифры, так как в начале XVIII века Петром была выведена из употребления архаичная буквенная кириллическая нумерация, заимствованная у греков. В качестве знаков шифрованного текста употреблялись и буквенные сочетания [Бабаш, 2002], [Соболева, 2002].

Тексты, которые надо было зашифровать, могли быть написаны на русском, французском, немецком, а иногда даже греческом языках. Как известно Петр прекрасно владел несколькими европейскими языками, в то же время на государственной службе состояло много иностранцев, именно в переписке с ними в основном использовались немецкий и французский. При этом следует отметить, что с точки зрения стойкости предпочтительнее использование русского языка. За границей было очень мало людей владевших русским языком, а знание лингвистических особенностей языка может существенно помочь криптоаналитику в дешифровании.

Новым явлением для российских шифров Петровской эпохи, по сравнению с предыдущими временами, стало наличие во многих из них «пустышек» – знаков шифрованного текста, которым не соответствует никакой знак открытого текста, т.е. они не несли никакого смысла. Как правило, пустышек было немного, обычно 5–8 знаков. Наличие пустышек увеличивает стойкость шифра, так как они дают криптоаналитику неверную информацию о количестве знаков в алфавите открытого текста, разбивают структурные лингвистические связи открытого текста и изменяют статистические закономерности, т.е. именно те свойства текста, которые используют при дешифровании шифра простой замены. Кроме того, пустышки увеличивают длину шифрованного текста по сравнению с открытым, что усложняет их взаимное сопоставление. Кроме того, в некоторых случаях отдельные знаки применялись для зашифрования точек и запятых, содержавшихся в открытом тексте, также для этого могли использоваться пустышки. Это особо оговаривалось в кратких правилах пользования шифром.

Вскоре к обычному алфавиту простой замены стали добавлять обозначения для наиболее употребительных слогов, слов и целых фраз, т.е. стали употребляться номенклаторы. Петровские номенклаторы были весьма простыми, они содержали небольшой словарь, называвшийся «суплемент» и содержавший некоторое количество слов (имен собственных, географических наименований или каких-то устойчивых словосочетаний, которые могли часто использоваться в открытых текстах, корреспондентов, использовавших данный шифр).

Шифр Петровской эпохи представлял собой лист бумаги, на котором от руки был написан ключ – таблица замены (обычно под горизонтально расположенными в алфавитной последовательности буквами кириллицы или иного алфавита, подписаны соответствующие элементы шифроалфавита), а также суплемент (если это был номенклатор). Ниже могли помещаться пустышки и краткие правила использования шифра.

Еще одной особенностью петровских шифров является то, что шифралфавит мог составляться из символов разных типов, например, смеси букв разных алфавитов, цифр и др. В качестве примера приведем письмо написанное и зашифрованное лично Петром I в июне 1708 г. Это письмо было направлено князю В.В. Долгорукому и речь в нем идет о мерах по подавлению крестьянского восстания К. Булавина, которое бушевало в это время в южных областях России. Ключ к этому шифру приведен на рис. 2.2.

Рис. 2.2. **Ключ к шифру простой замены [Соболева, 2002]**

В данном случае в качестве символов шифралфавита применяются русские, латинские, греческие буквы, арабские цифры и специально придуманные знаки. Письмо начинается с большого незашифрованного фрагмента [Соболева, 2002]:

«Господин маеоръ. Письма Ваши до меня дошли, из которых я выразумел, что вы намърены оба полка, т.е. Кропотовъ драгунской и пъшей из Кіева, у себя держать, на что отвътствую, что пъшему, ежели опасно пройтить въ Азовъ, то удержите у себя, а конной, не мъшкавъ, конечно отправьте на Таганрогъ. Также является изъ вашихъ писемъ нъкоторая медленіе, что намъ не зело пріятна, когда дождетесь нашего баталіона и Ингермонландского и Билсова полковъ, тогда тотчас» (далее следует шифртекст (рис. 2.3), обратите внимание, что шифробозначение для буквы О отличается от приведенного ранее дополнительными точками).

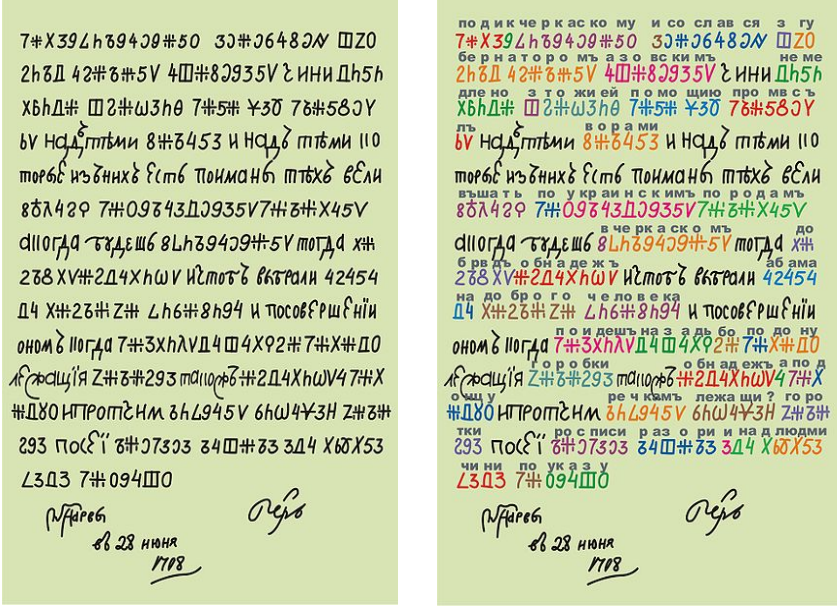


Рис. 2.3. **Шифртекст письма Петра I (слева) и его расшифровка (справа) [Бабаш, 2002].**

Значительную часть письма составляет «клер» – незашифрованные слова и предложения. Это делалось в интересах облегчения и убыстрения процессов зашифрования и расшифрования. Из-за того, что некоторые знаки похожи по начертаниям, в шифрованной части письма много описок. Так вместо знака буквы Б написан знак буквы Т (и наоборот) на 3-й строке, на 8-й строке два раза и на 10-й. Вместо знака буквы Ы написан знак буквы В на 3-й строке и на 8-й. Недописка знака буквы Г (в виде латинской буквы Z) на 6-й строке привела к тому, что он стал знаком буквы П (в виде цифры 7) На 8-й строке в шифрованном слове буква Х оказалась не зашифрованной и стала знаком буквы Д. Наряду с описками есть и явные ошибки при шифровании. Так на 11-й строке вместо знака буквы Д написан знак буквы Б. На 12-й строке буква Е должна писаться прописной латинской h. Вместо этого написана заглавная латинская Н. На 13-й строке вместо знака буквы Д написан знак буквы Т и др. [Сперанский, 1929]. Ошибки и описки хоть и сбивают с толку, но понять смысл текста позволяют (клер выделен косым шрифтом):

«…поди к Черкаскому и сослався з губернаторомъ азовскимъ *чини* немедленно з Божией помощию промысълъ *надъ тъми* ворами *и надъ тъми которые изъ нихъ есть поиманы тъхъ вели* въшать по украинскимъ городамъ *а когда будешь* в Черкаскомъ *тогда* добрыхъ обнадежъ *и чтобъ выбрали* атамана доброго человека *и по совершеніи ономъ когда* поидешъ назадь по Дону *лежащія* городки *такожъ* обнадежъ а по Донцу *и протчим* речкамъ лежащие городки *по сеі* росписи разори и над людми чини по указу. *Из Нарвы в д 28 июня 1708. Piter*».

Помимо клера можно наблюдать частичное разбитие шифртекста на слова, хотя все это облегчает и убыстряет процессы шифрования расшифрования, но крайне снижает стойкость шифра. Из открытой части сообщения криптоаналитик получает информацию о характере зашифрованного текста, исходя из этого он может строить предположения о вероятных словах в зашифрованном тексте. Клер и разбитие на слова дают представление о лингвистической структуре сообщения. Все это существенно облегчает дешифрование.

Справедливости ради следует отметить, что клер и другие слабости имели место не только в петровскую эпоху, жертвовали стойкостью ради удобства эксплуатации шифров в разных странах и в более поздние времена.

Рассматривая криптографическую деятельность государственных институтов России эпохи Петра Великого подробнее видно, что весьма широко шифры применялись в дипломатической деятельности государства Российского. Уже в конце XVII в. Петр определяет ключевое направление внешней политики и военной деятельности России – выход к Балтийскому морю. Основным противником России становится Швеция, захватившая исконно русские земли на побережье Балтики. Однако прежде чем начинать войну на Севере, необходимо было заключить мир с Турцией, так как войны на два фронта Россия выдержать не могла. В октябре 1698 г. в населенном пункте Карловиц около Белграда открывается конгресс, посвященный заключению мира с Турцией. В нем участвуют Россия, Австрия, Польша и Венеция. Российскую делегацию возглавляет П.Б. Возницын, переговоры идут крайне трудно, фактически участники конгресса пытаются и не без успеха, заключать сепаратные соглашения с Турцией, не учитывая интересов России. Все же титаническими усилиями российской дипломатии в январе 1699 г. удается заключить перемирие с турками. Интересно отметить, что информацию о перимерии, опубликованную в голландских газетах, посол России в Нидерландах А.А. Матвеев передал в Москву раньше чем официальная делегация.

Но перемирие еще не мир. Для заключения полноценного мирного договора Петр предпринимает военно-дипломатическую акцию, в Стамбул в августе 1699 г. направляется посольство во главе с Е.И. Украинцевым. Посольство следует на 30 пушечном корабле «Крепость». Эта акция была направлена на то, чтобы показать возросшую военную мощь России. Переговоры начались 19 ноября и продолжались несколько месяцев с великим трудом. Только 3 июля 1700 г. Украинцев сумел подписать мирный договор сроком на 30 лет. Шифрованное сообщение об этом тут же было отправлено в Москву. Связь тогда осуществля-

лась курьерами и доставка сообщения из Константинополя в Москву занимала в среднем 36 дней. В августе сообщение было доставлено Петру, на следующий день Россия объявила войну Швеции [Молчанов, 1984].

Однако заключенный мир был весьма не прочен. Настроение султана могло измениться в любой момент. В апреле 1702 г. Петр посылает в Турцию в качестве первого в истории российской дипломатии постоянного представителя за рубежом Петра Андреевича Толстого. Для связи с Россией П.А. Толстой (1645–1729) был снабжен цифирной азбукой (т.е. шифром), которая приведена на рис. 2.4.

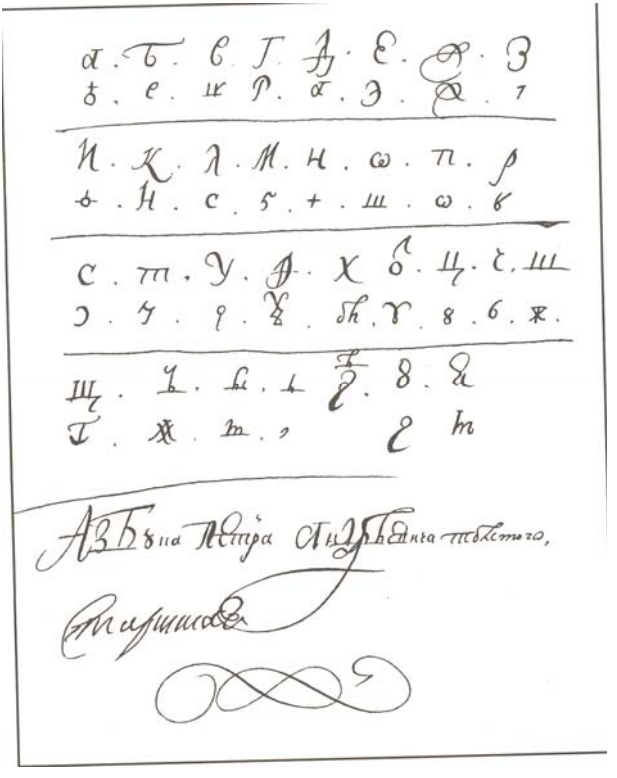


Рис. 2.4. **Шифр П.А. Толстого [Соболева, 2002]**

Это шифр 1700 г., который представляет собой простую замену, в которой буквам кириллической азбуки соответствуют специально придуманные знаки. Здесь же имеются две записи. Первая из них: «Список с образцовой цифирной азбуки, какова написана и послана в Турскую землю с послом и стольником с Толстым сими литеры» [Соболева]. Вторая особенно интересна: «Такову азбуку азволнил (т.е. изволил) 1700 г. написать своею рукою Великий государь по друго диво еси же». Из этой надписи следует, что автором данного шифра был сам Петр Великий [Соболева, 2002]. Видимо это один из первых шифров, собственноручно составленных русским царем.

При этом помимо чисто дипломатических задач Петр повелел Толстому вести и разведывательную работу. Толстой получил «наказ Петра в виде «тайных статей», представлявших собой разведывательное задание из 17 параграфов. Русскому послу предлагалось выведать и описать «тамошние народы и их нравы», государственное устройство, определить круг лиц, которые управляют страной. «Разузнать», с какими государствами Порта (Турция – *авт.*) поддерживает военные и дипломатические отношения, к чему более склоняется правящая верхушка – к сохранению мира или к подготовке войны. Разведать с какими странами Турция вероятнее всего может начать войну, «какие государства и какой народ больше любит». Петр интересовался финансовым положением Оттоманской Порты и состоянием ее вооруженных сил. Особое внимание обращалось на морской флот и его действия на Черном море» [Кудрявцев, 2002]. Практически П.А. Толстой должен был вести разведывательную деятельность во всех областях, касающихся жизни Османской Империи, военной, экономической и политической.

По прибытии в Турцию Толстой развернул бурную деятельность, вскоре ему удалось найти «подходы» ко многим высокопоставленным чиновникам, в том числе матери султана. Основным направлением деятельности Толстого было недопущение военного выступления Османской империи против России, что ему удавалось обеспечить в течении ряда лет.

Большую помощь в добыче информации русскому дипломату оказывали иерусалимский патриарх Досифей и его племянник Спилиот. Основной задачей Спилиота была доставка секретной корреспонденции между Толстым и патриархом, но нередко он сообщал полезную информацию и давал ценные советы. В частности Спилиот консультировал Толстого как поступить в том или ином случае при проведении переговоров с турецкими чиновниками. Русский дипломат высоко оценивал оказываемую помощь, он писал в Москву «что и патриарх и его племянник забыв страх смертной, радостною душою великому государю работают» [Очерки, 1999]. Заметим, что Досифей внес интересное «рацпредложение» в шифрпереписку с русским двором, он предложил не называть имена корреспондентов, а обозначать их специальными символами. Вот как он сам описывал это новшество: «…которое письмо имеет с лица круг, тое к великому государю, а которое имеет треугольный знак, есть к высочество Вашему (канцлеру Г.И. Головкину). Посылаем и образец печати. И как придет к Вам такое письмо, в котором есть та печать, ведому буди, чт.е. наше послание» [Бабаш, 2002]. Кстати через Досифеея шла секретная переписка представителей России с молдавским господарем. Помимо Досифея и Спилиота Толстому удалось найти и других помощников из числа православного населения Османской империи, при этом как докладывал русский дипломат канцлеру Г.И. Головкину «эти люди чистосердечно трудятся без боязни и от мене заплаты никакие не требуют» [Очерки, 1999].

Среди добытой Толстым информации была и криптографическая, так в 1703 г. в Москву поступила информация о военно-морских силах Турции. Толстой сообщил не только о том, какие типы кораблей состоят на вооружении турецкого флота, об их вооружении, укомплектованности команд, состоянии верфей, тактике боевых действий, но и о системе условных кодированных сигналов турецкого флота.

В том же году Толстому удалось получить сведения о засылке в Россию турецкой агентуры, в частности он сообщил о повышенном интересе турок к Воронежу (где в то время строи-

лись корабли для русского черноморского флота) и форпосту России на Черном море – крепости Азов. На основании этой информации Петр I дает шифрованную директиву адмиралу Ф.М. Апраксину: «Зело берегитеся шпионов на Воронеже; а на Донское устье можно никого приезжава не пускать, кроме своих матросов, ни крестьян, ни черкас» [Кудрявцев, 2002].

В начале 1707 г. с помощью агентуры Толстой ознакомился с содержанием секретной переписки французского посла в Стамбуле Ферриоля, который добивался нападения Турции на Россию. Благодаря своевременно полученной информации Толстой предпринял усилия по недопущению подобного развития событий, при этом активно использовался подкуп турецких чиновников. Среди «облагодетельствованных» Толстым присутствуют великий визирь (фактически глава правительства), рейс-эфенди (министр иностранных дел) и муфтий.

Весной 1709 г. Петр наносит визит в Азов, многие в Турции восприняли это как повод для войны, считая что он прибыл для руководства нападением на Турцию. Толстому стоило немалых усилий убедить султана и его окружение в мирных намерениях России и мир удалось сохранить. В Москву Толстой посылает шифрованное сообщение о том, что «с великим труда иждивением и немалой дачею (взятками – авт.) удалось убедить Великого визиря, что русский царь прибыл в Азов ни для чего иного, разве ради гуляния, ибо царское величество имеет нрав такой, что в одном месте всегда быть не позволит» [Очерки, 1999].

Но все хорошее когда-то кончается. 20 ноября 1710 г. Турция разорвала мирный договор с Россией, Толстой своевременно получил информацию о войне, но передать ее не успел. После объявления войны П.А. Толстой был заключен в тюрьму, где пробыл более 1,5 лет. Даже находясь в заключении Толстой продолжал разведывательную деятельность, ему удавалось получать политическую и военную информацию, однако возникла проблема: как передать информацию на Родину? Дело в том, что турки не допускали контактов заключенного с внешним миром, а также изолировали сотрудников

его посольства. Никто из дипломатов западных стран, аккредитованных в Стамбуле не захотел поддерживать контакты с попавшим в заключение русским послом. Но Петр Андреевич нашел выход, он пригласил к себе посла молдавского господаря Кантемира, который тайно присягнул на верность Петру I. Турки не отказали молдавскому послу в посещении коллеги, через него Толстому удалось передать записку русскому царю о своем положении, впоследствии молдавский посол не раз посещал заключенного русского дипломата, таким образом, Толстому удалось организовать канал связи с Россией. Интересно отметить, что молдавский господарь Дмитрий Кантемир сам составлял шифры для переписки с Россией. Так в наших архивах сохранилась «Азбука цифирная, какову послал князь Дмитре Костянтинович Кантемир в 1721 г.» [Соболева, 2002]. Этот шифр представляет собой номенклатор, буквы русского алфавита заменяются на числа и другие буквы кириллицы. Также имеется небольшой суплемент, специальные обозначения введены для ряда персон, упоминавшихся в переписке. Это были:

«Царское Величество российский государь;
Королевское Величество французский государь;
Султанское Величество турецкий государь;
резидент французский Правоте;
князь Василий Лукич Долгорукий;
князь Антиох Кантемир;
князь Дмитрий Кантемир»

[Соболева, 2002].

После неудачного для России прутского похода 1711 г. армии во главе с царем против турок, закончившегося перемирием, начинаются переговоры о заключении нового соглашения о мире с Турцией. Российскую делегацию возглавляет подканцлер П.П. Шафиров, фактически русские находились в Стамбуле на положении заложников. Однако русской делегации удалось наладить канал тайной связи с Родиной при помощи иностранцев. После того как 5 апреля 1712 г. мир все же был заключен (кстати

одним из условий с русской стороны было освобождение из тюрьмы П.А. Толстого, что и было сделано, Толстой вернулся в Россию в 1714 г.) Шафиров писал Петру:

«Если б не английский и голландский послы, то нам нельзя было бы иметь ни с кем корреспонденции и к вашему величеству писать, потому что никого ни к нам, ни от нас не пускали, и конечно б тогда война была начата и нас посадили бы, по последней мере в жестокую тюрьму; английский посол, человек искусный и умный, день и ночь трудился, и письмами и словами склонял турок к сохранению мира, резко говорил им, за что они на него сердились и лаяли; и природному вашего величества рабу больше нельзя было делать; при окончании дела своею рукою писал трактат на итальянском языке начерно и вымышлял всяким образом, как бы его сложить в такой силе, чтоб не был противен интересу вашего величества; голландский посол ездил несколько раз инкогнито к визирю, уговаривал его наедине и склонял к нашей пользе, потому что сам умеет говорить по-турецки. И хотя мы им учинили обещанное вознаграждение, однако нужно было бы прислать и кавалерии с нарочитыми алмазами, также по доброму меху соболью» [Молчанов, 1984]. Разумеется, английский и голландский дипломаты получили вознаграждение, надо отметить, что помощь российской делегации была обусловлена тем, что Турция в то время была союзником Франции, главного врага Англии и Голландии. Война Турции с Россией была выгодна Франции и соответственно противоречила интересам вышеназванных стран.

Более трагически сложилась судьба русского посланника в Швеции князя Андрея Яковлевича Хилкова (1676–1718). Хилков прибыл в Швецию летом 1700 г., он знал о готовящейся войне, но мужественно отправился в опасную командировку, для того чтобы шведы раньше времени не догадались о военных намерениях России. Возлагалась на русского дипломата и разведывательная миссия, князю надлежало выяснить «с какими делами и для чего живут в Стокгольме посланники иностранных держав» [Кудрявцев, 2002]. Так совпало, что

Хилков вручил верительные грамоты шведскому королю Карлу XII 30 августа, как раз в день объявления Россией войны Швеции. Шведский король был возмущен «коварством русских», он приказал конфисковать имущество Хилкова, а его самого вместе тремя другими сотрудниками русского посольства (переводчиком и двумя подъячими) посадить под домашний арест в здании, которое русская миссия арендовала под посольство. Несмотря на очень плотный надзор российскому послу разрешили вести переписку с Родиной. После начала войны в Швеции были интернированы «торговые и работные люди из России, общим числом 111 человек» [Кудрявцев, 2002], у них конфисковали все имущество, а самих их собрали в русском купеческом дворе в центре Стокгольма, откуда направляли на принудительные работы. Хилкову удалось вступить с ними в контакт и убедить шведов, что данные лица не являются военнопленными, а в последствии даже отсудить у шведов некоторую часть купеческих капиталов. На эти деньги Хилков смог нанять информаторов и связников для осуществления своей разведывательной деятельности. Поскольку купцы прибыли из разных регионов Швеции русскому посланнику путем опросов удалось выяснить экономическое положение в королевстве. В ноябре 1700 г. в результате поражения русских войск под Нарвой в Швеции оказалось большое количество русских пленных. Хилкову удалось добиться возможности встречаться с ними, поскольку пленники содержались в разных частях королевства, то князю удалось собрать важную военную, политическую и экономическую информацию. Помимо русских подданных Хилкову удалось создать большую агентурную сеть из шведских подданных, при этом среди его агентов числились несколько сотрудников, в обязанности которых входило охранять Андрея Яковлевича. Эта агентурная сеть снабжала Хилкова, а через него руководство России важнейшей военной, политической и экономической информацией из стана врага [Кудрявцев, 2002], [Очерки, 1999].

Для передачи разведывательной информации Хилков использовал шифры и стеганографию. Он писал невидимыми

чернилами, бумагу надо было нагреть, после чего помимо текста невинного содержания проступал секретный текст. Кстати надо отметить, что сам Петр лично принимал участие в организации стеганографической защиты информации. Использовались и простые методы, как запрятывание шифровок, так и применение симпатических (невидимых) чернил. Так в 1706 г. Петр писал фельдмаршалу Огильви: «Февраля в 17 день цифирь Реновая (новая – *авт.*). А посланы в 22 день: замешкались за тем, что азбуку переписывали и в пуговицу вдевали. Посланы с маером (майром – *авт.*) Вейром» [Соболева, 2002]. Кстати упоминание в шифрованном письме имени человека, с которым посылался новый ключ, было обычным для русской криптографической службы тех лет, это повышало надежность канала передачи информации. Секретные письма зашивались в одежду, запрятывались в каблуки и т.п. Что касается симпатических чернил о них речь идет в письме, посланным Петром одному из русских дипломатов в апреле 1714 г.: «Посылаю к вам три скляницы для тайнова писма: чем перво писат под А. которая войдет в бумагу и ничево знат не будет; потом под В. – теми чернилы потом писат, что хочешь явъново; а третье пот С. – то, когда от нас получишь писма, оною помазат, то чернилы сойдут, а первое выступит» [Бабаш, 2002], [Очерки, 1999].

Наиболее важной информацией переданной Хилковым в начале Северной войны, стали сведения о подготовке в 1701 г. рейда шведской эскадры, под руководством адмирала Шеблада на Архангельск. При этом эскадра маскировалась под китобойную флотилию, корабли шли под флагами Англии и Голландии. Своевременно полученная из Швеции информация, чуть позже подтвержденная шифрованными сообщениями русских дипломатов из Дании и Голландии, где шведы пополняли запасы, позволила гарнизону подготовиться к отражению атаки. Была срочно и тайно сформирована береговая батарея, а действия предоставленных «рыбакам» русских лоцманов привели к посадке на мель двух шведских судов прямо по прицел русских орудий. Эти корабли вынуждены были сдаться, а остальная часть эскадры спасаться бегством.

Напомним, что Архангельск в то время был единственным местом в России, через которое велась торговля с Западной Европой. В то время Россия не могла полностью обеспечить потребности своих вооруженных сил в оружии, сырье, военных материалах за счет внутренних ресурсов. Недостаток ликвидировался путем закупок необходимых товаров в основном в Англии и Голландии, с другой стороны товары традиционного российского экспорта (лес, продовольствие, парусина, пенька и др.) позволяли получать значительные денежные средства, так необходимые для ведения тяжелейшей войны. Таким образом, захват или даже прекращение на некоторое время функционирования Архангельского порта (например, из-за разрушения причалов и другой портовой инфраструктуры) привело бы к существенным экономическим потерям России. Благодаря шифрованному сообщению А.Я. Хилкова закрыть тогдашнее российское «окно в Европу» шведам не удалось. Кстати победа над шведским флотом у Архангельска стала одним из первых успехов России в Северной войне, что после поражения под Нарвой, безусловно, укрепило моральных дух российских вооруженных сил и общества в целом.

Хилков продолжал добывать важную разведывательную информацию почти всю войну. Письма направлялись в Копенгаген, в русское посольство в Дании. Информация Хилкова дополнялась сведениями, полученными персоналом посольства и отправлялась в Россию. Открытая информация поступала в русское дипломатическое ведомство, а тайная (зашифрованная и срытая с помощью симпатических чернил) попадала к царю [Кудрявцев, 2002], [Очерки, 1999].

С 1704 года в ведении разведывательной работы и переписки с Родиной Хилкову помогал, попавший в плен под Нарвой офицер А.И. Манкиев. Он оказался очень ценным помощником, так как знал шведский, латинский и польский языки. Помимо традиционного канала связи через Данию русским разведчикам удалось передать большой объем важной информации в 1706 и 1708 гг., с офицерами, которые возвращались в Россию в результате обмена военнопленными. После пораже-

ния шведов под Полтавой режим содержания Хилкова и его помощников был ужесточен. Королевскому прокурору Швеции удалось нащупать канал утечки информации, Хилкова пытались перевербовать, двое его помощников скончались при загадочных обстоятельствах. Хилков зачислил в штат посольства Манкиева и продолжил свою работу на благо России. Так в 1710 г. он передал Петру важную информацию о настроениях шведского общества по поводу продолжения войны с Россией: «здесь общая наклонность к миру, мешает один король – он скорее переведет до последнего человека, но не помирится пока все не возвратит» [Очерки, 1999].

Сообщал также Хилков о тяжелом экономическом положении Швеции, страна была буквально истощена войной, росло недовольство постоянными призывами новобранцев в армию, высокими налогами и др. Разумеется эти сведения были крайне важны для российского руководства. В 1714 г. Хилков передал важную информацию о системе государственного управления в Швеции, он «извещал Петра о расширении штатов в шведских коллегиях иностранных дел, торговли, юстиции, военных дел и большой казны, о введении там новых должностей ревизоров и о распродаже патентов на эти должности» [Очерки, 1999]. Подводя итог дипломатической деятельности А.Я. Хилкова, следует отметить, что его миссия была единственным источником информации из Швеции во время войны, сведения политического, военного и экономического характера были крайне важны для царя и руководства России. Естественно передача информации из стана врага требовала применения средств защиты информации шифров и стеганографии. Андрей Яковлевич Хилков умер от туберкулеза в начале 1718 г., полгода не дожив до освобождения последних русских пленных. Тело князя Хилкова было доставлено в Россию и захоронено с воинскими почестями в Александро-Невской лавре в Санкт-Петербурге. Алексей Ильич Манкиев вернулся в Россию и продолжил деятельность на благо России на дипломатическом поприще.

А.Я. Хилков и П.А. Толстой работали в странах враждебных России, конечно работа наших дипломатов в союзных и

нейтральных странах была менее опасна, но также велась с напряжением всех сил. При этом всем сотрудникам дипломатических миссий ставились и разведывательные задачи. Разумеется, все российские дипломаты вынуждены были заботиться о сохранении секретности передаваемых сообщений. «Петровские послы все свои мало-мальски важные донесения писали «цифирью», шифром» [Молчанов, 1984].

В 1701 г. помимо перечисленных постоянные представительства имелись еще в четырех странах: Австрии, Голландии, Дании и Польше. Шифрованная переписка царя и чиновников дипломатического ведомства с дипломатическими представителями России за границей осуществлялась постоянно; даже кратковременные дипломатические миссии сопровождались вручением отбывающему за рубеж «цифирьной азбуки». Обычно шифровалась переписка Петра с другими европейскими монархами. В рамках данного подраздела нет возможности подробно рассказать о содержании шифрованных сообщений российских дипломатов. Заметим лишь, что за весь период Северной войны руководство России, в первую очередь сам царь, получили множество шифрованных сообщений, содержащих важнейшую политическую, военную, экономическую и иную информацию. В качестве примера приведем сообщение, посланное российским представителем в Нидерландах А.А. Матвеевым в сентябре 1708 г.:

«Из секрета здешнего шведского министра сообщено мне от друзей, что швед, усмотря осторожность царских войск и невозможность пройти к Смоленску, также по причине недостатка в провианте и кормах, принял намерение идти в Украйну, во-первых, потому, что эта страна многолюдная и обильная и никаких регулярных фортенций с сильными гарнизонами не имеет; во-вторых, швед надеется в вольном казацком народе собрать много людей, которые проводят его прямыми и безопасными дорогами к Москве; в-третьих, по близости может иметь удобную пересылку с ханом крымским для призыву его в союз, и с поляками, которые держат сторону Лещинского (назначенного Карлом XII королем Польши – *авт.*); в-четвертых,

наконец, будет иметь возможность посылать казаков к Москве для возмущения народного» [Молчанов, 1984].

Своевременно полученная информация о намерениях шведского короля позволила Петру и его генералам разработать эффективную тактику борьбы со шведами и нанести 28 сентября 1708 г. у деревне Лесная сокрушительное поражение 16 тысячному корпусу генерала Левенгаупта, шедшего на соединение с основными силами шведов с большим обозом. Эту победу Петр впоследствии назвал «матерью полтавской баталии» [Павленко, 1989]. Значительные людские потери шведов и лишение обоза серьезно сказались на дальнейшем ходе военных действий, восполнить их у шведов уже не было никакой возможности. Вот что по поводу требований Карла XII о присылке подкреплений из Швеции писал в ноябре того же года в Россию посол в Дании В.Л. Долгорукий: «Хотя как возможно во всей швецкой земле берут рекрут, и за великой скудностью людей пишут стариков, у коих от старости зубов нет, и робят, которые не без труда поднять мушкет могут, однакож собрав и таких, не чают, чтобы мочь знатного с такими людьми учинить, когда лучшие свои войска растерял, не учиняя с ними ничего…» [Молчанов, 1984]. Разумеется, подобное донесение не могло вызвать а России ничего, кроме глубокого удовлетворения.

Активизация дипломатической деятельности России и, соответственно увеличение объема шифрпереписки, вызвало увеличение штата главного криптографического учреждения России – походной посольской канцелярии. В 1705 г. в ней служат: «тайный секретарь (П.П. Шафиров), два переводчика, два подьячих малороссийского приказа, да по вся годы посылаются в Свейский поход старый подьячий Василий Степанов и три молодых» [Соболева, 2002].

Штат канцелярии постоянно расширялся, очень скоро она из временного учреждения превратилась в постоянное, причем с 1709 г. оно стало называться просто посольской канцелярией. В 1710 г. канцелярия окончательно «прописалась» в Санкт-Петербурге. Канцелярия стала ведущим государствен-

ным органом по осуществлению криптографической деятельности в России. В ней была сосредоточена почти вся работа по зашифрованию и стеганографической защиты переписки Петра и других руководителей государства Российского с их корреспондентами, а также расшифрование входящей корреспонденции и проявление тайнописи. В компетенцию канцелярии входит также создание новых шифров, вывод из обращения устаревших, разработка составов для невидимого письма, обеспечение ключевой информацией и средствами тайнописи корреспондентов шифрованной связи (в первую очередь дипломатов и военачальников) и т.п. При этом наиболее важные депеши направлялись лично царю, в Кабинет его императорского величества, небольшая часть шифрпереписки поступала в Посольский приказ, остававшийся в Москве. Руководят деятельностью отечественной криптографической службы лично государственный канцлер граф Г.И. Головкин и вице-канцлер барон П.П. Шафиров (оба назначены царем в 1709 г.). Именно этим лицам докладывались отчеты о составлении и введении в действие новых шифров, а также добычи сведений об иностранных шифрсистемах (т.е. дипломатическое ведомство России начало уделять внимание, такому аспекту криптографической деятельности, как дешифрование). Столь высокий уровень руководства службой, которая обеспечивала конфиденциальность дипломатической переписки, а также внутригосударственных сообщений, вошел в России в традицию, которая сохранялась на протяжении почти полутора веков [Астрахан, 1996], [Соболева, 2002]. В 1716 г. в Посольской канцелярии был введен коллегиальный порядок решения всех вопросов. Вот что по этому поводу пишет российский историк Т.А. Соболева: «… в начале XVIII века Посольская канцелярия не имела права рассматривать важнейшие политические дела, поскольку это право принадлежало Сенату. Члены Сената – «господа тайные советники» – обычно на своих заседаниях слушали изготовленные в Посольской канцелярии рескрипты к русским министрам за границей. Тайные советники собирались иногда в присутствии царя в

доме канцлера «на конференцию» о наиболее серьезных вопросах иностранной политики» [Соболева, 2002].

В 1717–1721 гг. Петр I проводит радикальную реформу системы государственного управления страной. Вместо ставших неэффективными многочисленных приказов, между которыми не было четкого разграничения функций, постепенно создавались новые органы – коллегии, ведавшие отдельными отраслями государственного управления. Еще раньше в 1711 г. Боярскую думу заменил Сенат, который стал высшей законодательной инстанцией. В декабре 1712 г. царь сделал первые предварительные распоряжения об учреждении коллегий, и в том числе Коллегии иностранных дел, где сосредоточилась вся международная деятельность России. Криптографическая деятельность стала осуществляться в 1-й экспедиции этого ведомства. Сообщения, направляемые Коллегию иностранных дел, просматривались секретарями экспедиции сразу при их получении из почтового ведомства. Зашифрованные письма расшифровывались ими же или их подчиненными: нотариусом-регистратором, канцеляристом и копиистами. После этого секретари были обязаны доложить содержание сообщения президенту и вице-президенту Коллегии, при этом было необходимо о них докладывать во время заседаний коллегии. Если руководства на рабочих местах не было, необходимо было посылать расшифрованные письма к ним на дом. В обязанности секретарей также входило записывать последовавшие на них резолюции и, в случае необходимости сочинять ответные рескрипты. Эти рескрипты зачитывались на следующем заседании, при этом, «согласно указу от 5 апреля 1716 г. («Каким образом указы и прочие дела писать в Посольской к, и черновые их списки, и переписанные набело подписывались всеми членами коллегии» [Турилова, 2001]) и скреплялись подписью секретаря. Затем текст рескрипта зашифровывали и направляли в соответствующий адрес с курьером» [Соболева, 2002].

Вся деятельность по разработке и изготовлению шифров проводилась под непосредственным руководством самого царя, канцлера и вице-канцлера. Помимо осуществления собст-

венно дипломатической деятельности коллегии вменялось в обязанность вести регистрацию всех иностранцев, приезжающих в Российскую империю, а также выдача паспортов гражданам России, отъезжающим за границу для дипломатической, торговой деятельности, учебы и т.п. Коллегия постоянно собирала все сведения об иностранцах. С июня 1718 г. ей вменялось в обязанность тайное прочтение (перлюстрация) всех писем, поступающих из-за границы и отправляемых туда [Астрахан, 1996], [Буганов, 1989], [Молчанов, 1984], [Словарь, 1984], [Соболева, 2002].

Окончательное законодательное утверждение Коллегии иностранных дел произошло, 13 февраля 1720 г., когда Петр I «прислал канцлеру графу Головкину подписанное и скрепленное резолюцией «быть по сему» «Определение Коллегии иностранных дел» [Соболева, 2002]. Этот документ определял штат российского внешнеполитического ведомства и распределение обязанностей между его сотрудниками. Как прежде посольской канцелярией, руководство коллегией иностранных дел осуществляют Г.И. Головкин (президент коллегии) и П.П. Шафиров (вице-президент). Важную роль в работе коллегии играли «канцелярии советники», это были «тайный канцелярии советник» А.И. Остерман и В.В. Степанов. В обязанности советников входили наиболее важные аспекты деятельности коллегии, они ведали перепиской с иностранными государями, русскими министрам за границей, а также составляли различные декларации и резолюции. На советников также был возложен надзор за исполнением дел, поручаемых секретарям. Последние и выполняли основную массу работы – руководили отделами или, как их называли, «экспедициями» Коллегии, также в штат коллегии входили переводчики. В 1720-х гг. секретарями были И. Веселовский, П. Голембовский, Ф. Беневени и др. [Соболева, 2002].

О последнем расскажем подробнее. Флорио Беневени итальянец на русской службе, хорошо знавший Восток, тамошние нравы и обычаи, владевший персидским и турецким языками. Исходя из этих обстоятельств Петр поручил Беневе-

ни ответственную миссию возглавить русское посольство, направляемое в Персию (ныне Иран) на пути в Тегеран миссия проезжала через Бухарское ханство, а на обратном еще и Хивинское. Помимо дипломатической миссии итальянец должен был вести разведывательную работу. Посольство отбыло в Бухару в 1719 г., потом была переправа через Каспийское море и в 1720 г. прибыла в Тегеран. Русская миссия проработала в Персии более 1 года. Все это время Беневени направлял в Санкт-Петербург важную информацию политического, военного и экономического характера. Эти сведения весьма пригодились Петру летом 1722 г., когда русская армия начала персидский поход, который возглавлял сам царь. Военная кампания оказалась удачной, в результате Россия приобрела территории на западном побережье Каспийского моря. В конце 1721 г. Беневени и его спутники вернулись в Бухару.

В Бухаре миссия проработала 3 года, здесь как и в Персии Беневени занимался активной разведывательной работой. В частности в Санкт-Петербург поступила информация о наличии в Бухарском ханстве больших запасов золота и серебра. Работу рудников контролировал сам хан, а само существование и место расположения держалось в большом секрете. Тем не менее Беневени удалось получить эту информацию. Сообщал он также сведения о деятельности в ханстве представителей Турции и Персии, их влиянии на хана и его окружение, различных группировках при дворе и т.п. Эта информация имела важное значение для формирования российской политики по отношению к Бухаре. После окончании деятельности в Бухаре русская миссия направилась в Хиву и отсюда в Россию шел поток важной информации. Лишь в 1725 г. миссия вернулась в Россию, таким образом, работа Беневени и его спутников в Азии продолжалась около 6 лет. Сведения общественно-политического, военного, экономического характера, собранные экспедицией Беневени сыграли важную роль в дальнейшем развитии отношений с Бухарой и Хивой. В конце концов, во второй половине XIX века оба ханства стали частью Российской Империи. После возвращение из путешествия Ф.

Беневени был принят на службу в Коллегию иностранных дел, где вскоре, благодаря хорошему знанию стран Востока, возглавил отдел «турецкого и других языков», осуществлявший дипломатическую деятельность на восточном направлении [Очерки, 1999].

Сообщения от Беневени шифровались шифром простой замены, который так и назывался «Азбука Флорио Беневени», он не имел пустышек, для обозначения точек использовались десять двузначных чисел [Соболева, 2002].

В начале 1710 г. Петр вводит новый гражданский шрифт взамен церковно-славянского, теперь шифрованные письма пишутся этим шрифтом. Петр Великий заботиться об образовании своих подданных, по всей стране организуются школы, «всех дворян обязывают учиться, не дозволяя уклоняющимся жениться!» [Молчанов, 1984]. В 1713 г. все высшие государственные учреждения и иностранные послы переезжают в Санкт-Петербург. Преобразование системы государственного управления страной, осуществляемые Петром, касаются и повышением эффективности системы связи. В 1720 г. вводится Генеральный регламент, определяющий процесс функционирования системы управления России, в этом документе впервые четко устанавливался и порядок работы с правительственной корреспонденцией вот как это происходило:

«В соответствии с регламентом, вся правительственная корреспонденция в зависимости от степени ее важности и срочности была разделена на определенные группы. Так, особо важные правительственные документы, например именные указы императора с его личными распоряжениями, всеподданнейшие донесения и доклады на его имя, реляции, манифесты направлялись по каналам «необыкновенной», «чрезвычайной» почты, через правительственных гонцов и нарочных курьеров. Особо важную корреспонденцию из личной канцелярии императора доставляли кабинет-курьеры, входившие в штат Кабинета его императорского величества и имевшие воинские звания обер-офицерского состава. Когда же небольшая группа кабинет-курьеров (по штату 6 человек)

не справлялась с доставкой всей исходящей из Кабинета особо важной корреспонденции, для выполнения обязанностей правительственных курьеров широко привлекались военные чины от капрала до полковника, в зависимости от важности даваемого им поручения. А по делам особо важным, как, например доставка писем императора главам иностранных государств, привлекались генералы (в петровское время преимущественно П.И. Ягужинский и Л.К. Нарышкин). Сенат также имел в своем распоряжении прикомандированных армейских офицеров, которых использовал в качестве курьеров для доставки адресатам своей исходящей корреспонденции» [Астрахан, 1996].

Сеть постоянных дипломатических представительств России за рубежом расширялась, так в 1719 г. были созданы миссии во Франции, Пруссии, Англии, Мекленбурге (Германия), Гамбурге, Венеции, Курляндии, Бухаре. Все российские дипломаты обязательно имели шифры для организации переписки с царем и Посольской канцелярией, а в последствии Коллегией иностранных дел. Кроме постоянных дипломатических представительств появились за границей первые российские консульства. В 1707 г. имелось лишь одно консульство в Амстердаме. В 1719 г. количество консульств увеличилось, появились три консульства в Голландии, по одному в Париже, Вене, Антверпене и Люттихе. Со всеми дипломатическими миссиями России «организовывалась тайная шифрованная переписка» [Соболева, 2002]. Кстати отбор в коллегию иностранных дел был очень строгий, задачи и принципы организации Коллегии определил сам царь: «К делам иностранным служителей коллегии иметь верных и добрых, чтобы не было дыряво, и в том крепко смотреть, и отнюдь не определять туда недостойных людей или своих родственников, особенно своих креатур. А ежели кто непотребного во оное место допустит или, ведая за кем в сем деле вину, а не объявит, то будут наказаны яко изменники» [Молчанов, 1984]. Здесь следует отметить, что сотрудники коллегии помимо важнейшей внешнеполитической

информации имели доступ к информации о российских шифрах, поэтому пристальное внимание Петра к людям, работавшим здесь вполне объяснимо. Вся работа коллегии была строго регламентирована. Право на проход в помещения, занимаемые коллегией, имели только ее сотрудники. Особое внимание было уделено сохранности криптографических секретов. «Инструкция от 11 апреля 1720 г., в которой устанавливалось устройство коллегии иностранных дел, заканчивалась предписанием о том, как хранить государственные печати и цифирные азбуки» [Соболева, 2002]. Петр I при охране криптографических секретов России уделял большое внимание «режимным мероприятиям», сотрудники криптографической службы «изолировались от общения с «несанкционированными» лицами и получали достаточное материальное вознаграждение, охранявшее их от «соблазна» [Бабаш, 2002]. В 1724 г. был утвержден штат архива Коллегии иностранных дел из 6 человек, во главе с Петром Курбатовым, среди прочих документов в архиве стала храниться вся дипломатическая шифрпереписка Российской Империи [Козлов, 2001].

В 20-х гг. XVIII в. шифрсистемы, используемые российскими дипломатами начинают меняться от шифров простой замены переходят к замене пропорциональной, когда наиболее часто встречающимся знакам открытого текста присваиваются несколько шифробозначений, что затрудняет использование «классического способа» криптоанализа шифра простой замены – частотного анализа. На рис. 2.5 приведен такой шифр российского посланника в Пруссии А.Г. Головкина.

Здесь используется русский алфавит, при этом каждой согласной букве соответствует по одному шифробозначению, а гласным – по два, одно из которых – буква латинского алфавита, а другое – двузначное число или два двузначных числа. Также имеются 13 пустышек (все буквы кириллицы), как помечено: «пустые между слов дабы растановок не знать». Кроме того, есть особые, также буквенные обозначения для запятых и точек. Таких обозначений пять [Соболева, 2002].

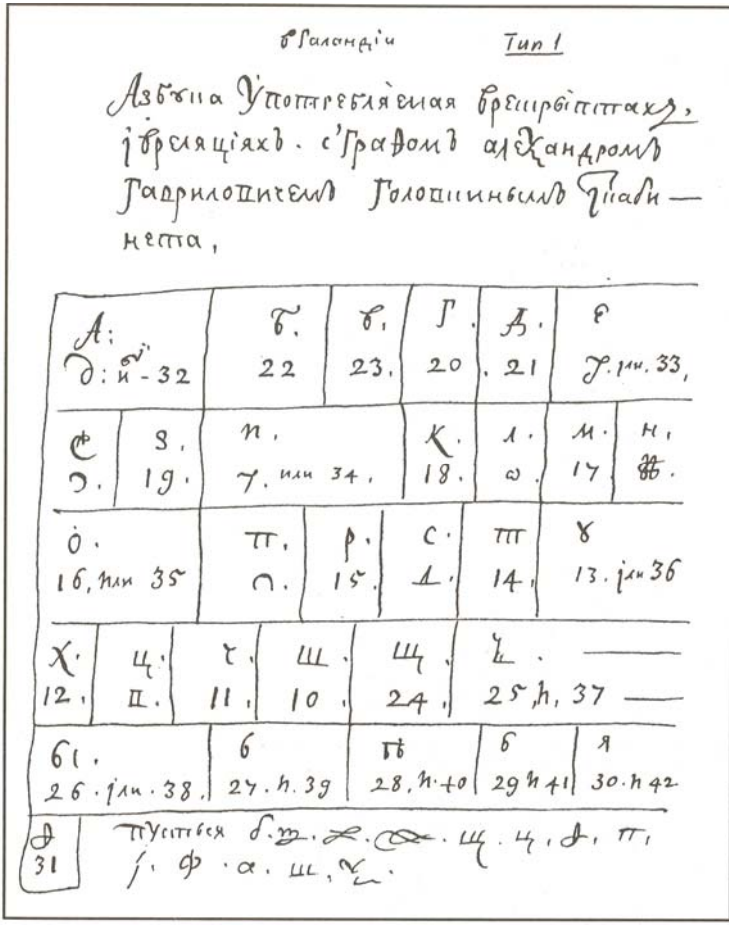


Рис. 2.5. **Русский шифр пропорциональной замены [Соболева, 2002]**

Вместе с тем для шифрования русской дипломатической переписки продолжали широко применятся и различные варианты шифра простой замены, в качестве примера может служить «Азбука, данная из государственной Коллегии иностранных дел 3 ноября 1721 г. камер-юнкеру Михаилу Бесту-

жеву, отправленному в Швецию» [Соболева, 2002]. Это «классическая» простая замена, шифртекст представляет собой смесь букв кириллицы, цифр и специально выдуманных знаков, алфавит открытого текста – русский. Шифр предназначался для обеспечения секретности переписки М. Бестужева с царем и Коллегией иностранных дел.

Наибольший интерес при описании русских дипломатических шифров представляет собой тетрадь, в которую подшиты шифры канцлера и президента Коллегии иностранных дел Г.И. Головкина, которыми он пользовался в 1721, 1724 и 1726 гг. У корреспондентов Гавриила Ивановича имелись первые экземпляры ключей, а у канцлера – вторые. Всего в эти годы наш канцлер использовал 17 шифров, помимо упомянутых «Азбуки Александра Гавриловича Головкина» и «Азбуки Флорио Беневени» имеются «Азбука князя Бориса Ивановича Куракина», «Азбука Алексея Бестужева», «Азбука губернатора астраханского господина Волынского», и др. [Соболева, 2002]. «Азбука Алексея Бестужева» это тоже шифр простой замены, алфавит открытого текста – русский, шифртекст представляет собой однозначные и двузначные числа и буквы латинского алфавита, кроме того имеется десять двузначных цифровых шифрообозначений для точек и запятых, в этой же функции в данном шифре выступает число 100 [Соболева, 2002].

При этом следует отметить, что свои собственные шифры разрабатывали и направляли в Коллегию иностранных дел некоторые русские дипломаты, например А. Бестужев, в архивах сохранилась надпись на одном из конвертов с шифром «Такова азбука послана от резидента Алексея Бестужева при реляции ево №88, полученной в Москве октября 8-дня 1722 г., в которой он доносит, что прежняя пропала» [Соболева, 2002]. На самом листке с ключевой документацией написано: «Азбука в государственную Коллегию иностранных дел из Копенгагена от А. Бестужева отправлена 8/19-го 1722» [Соболева, 2002]. Сохранилось два экземпляра ключа, один использовался в Коллегии, а другой был у автора шифра, по возвращении из загранкомандировки, в соответствии с правилами ключ был сдан в коллегию.

Многие шифры Петровской эпохи, имеющиеся в наших архивах, хранятся в специальных конвертах, на которых имеются надписи о том, кому и с какой целью предназначается данный шифр. Изучение этих надписей позволяет установить, что шифры для обеспечения секретности переписки с Петром или коллегией иностранных дел в обязательном порядке вручались всем лицам, направлявшимся за границу по государственным делам. При этом обеспечение шифром не зависело от того, было ли данное лицо дипломатом или нет. Например, сохранилась «азбука для переписки с господином бригадиром и от гвардии майором Семеном Салтыковым, который отправлен к его светлости герцогу Мекленбургскому. Дана Салтыкову 1 декабря 1721 г.» [Соболева, 2002].

В Архиве внешней политики Российской Империи (АВПРИ) имеется и шифр, разработанный российским послом, работавшим в разное время в Риме, Англии, Нидерландах, Ганновере и Франции князем Б.И. Куракиным. Два экземпляра ключа к нему были присланы в Коллегию 9 ноября 1722 г., в этом шифре использовался латинский алфавит. Присылались ключи в коллегию в особых конвертах, опечатанных личными сургучными печатями создателей шифров. Пересылка новых шифров осуществлялась довольно часто, так как срок действия каждого шифра был ограничен, выведенные из действия шифры доставлялись в коллегию и сдавались в архив. Так известно письмо российского дипломатического представителя в Турции И.И. Неплюева, в котором перечисляются выведенные из обращения шифры. Обычно, для замены отслуживших свое «цифирных азбук» новые готовились специалистами коллегии заранее, но так было не всегда. На одном из шифров из фондов АВПРИ имеется надпись «Азбука цифирная, присланная от генерала графа Вейсбаха, которую он велел до указа корреспонденцию чинить с господином оберштальмейстером, отправленным из Киева в Полшу, генералитенту» [Соболева, 2002]. Очевидно в данном случае возникла необходимость срочно сменить шифр, подходящего экземпляра в коллегии видимо не оказалось и генерал Вейсбах де факто ввел в действие свой шифр.

Информация, которая содержится в дипломатической шифрованной переписке России Петровской эпохи, исследовалась Е.П. Подъяпольской [Подъяпольская, 1959], также ряд сведений об используемых шифрах и корреспондентах конфиденциальной переписки можно найти в книгах [Буганов, 1989], [Князьков, 1914], [Молчанов, 1984], [Соболева, 2002]. Уникальные документы, в том числе и шифрованные, содержатся в фундаментальном издании [Письма].

В первую очередь, шифрованная связь поддерживалась между Петром и Коллегией иностранных дел с российскими представителями за рубежом. Среди них были в Австрии – П.А. Голицын, И.Х. Урбих, П.И. Беклемишев, А.П. Беселовский; при прусском дворе – Альбрехт Лит, а затем А.Г. Головкин, посол в Англии, Голландии, Австрии А.А. Матвеев, а также упомянутые ранее Бестужевы, И.И. Неплюев и князь и многие другие дипломаты, чьи шифры сохранились в российских архивах. Переписывались русские послы и между собой. Матвеев, будучи в Лондоне, переписывался с Урбихом, русским послом в Вене, Куракин переписывался одновременно с несколькими русскими зарубежными представителями. Г.Ф. Долгорукий и его племянник В.Л. Долгорукий держали друг друга в курсе политики двух союзных с Россией государств – Польши и Дании. Разумеется, вся эта переписка эта шифровалась [Соболева, 2002].

Использовали шифры и торговые представители России за рубежом, кстати, они, как и дипломаты часто совмещали основной вид деятельности с разведкой. В российских архивах сохранились шифры нашего представителя в Италии С.В. Рагузинского, в Голландии О. Соловьева и морского агента Ф.С. Салтыкова [Соболева, 2002].

Теперь рассмотрим русскую военную шифрпереписку Петровской эпохи. Отметим, что шифры, используемые для защиты российских военных секретов, практически не отличались от шифров дипломатов, мало того большая часть их изготавливалась в дипломатическом ведомстве, а некоторое небольшое количество создавалось лично Петром и его воена-

чальниками. Помимо уже перечисленных на этой странице источников информацию о военных шифрах Петровской эпохи можно получить из следующих работ: [Голиков, 1789], [Материалы, 1914], [Сборник, 1873], [Тромонин, 1843].

Главным военным событием Петровской эпохи, безусловно, является Северная война (1700 1721). Для выхода России к Балтийскому морю по инициативе Петра был создан антишведский Северный союз, в который помимо России вошли Дания, Саксония и Речь Посполитая (Польша). При организации этой коалиции русские дипломаты и сам царь развили бурную дипломатическую деятельность, она сопровождалась обильной шифрперепиской с политическим и военным руководством союзных стран, а так же дипломатами. Функционирование шифрованных каналов связи между союзниками имело место в течении всей войны.

С началом боевых действий естественно возникла необходимость организации управления армией, а за тем и флотом, что было невозможно без обеспечения надежной защищенной связи между руководством страны и военачальниками в действующей армии, командирами отдельных частей и соединений, действующих автономно, военным командованием союзников. Эту задачу Петру и его соратникам удалось решить.

Высший командный состав армии и флота имел шифры для переписки с царем и между собой. Известны шифрованные письма Петра I к адмиралу Ф.М. Апраксину, фельдмаршалам Светлейшему князю А.Д. Меншикову, князю А.И. Репнину, Б.П. Шереметеву, Г.Б. Огильви, фельдмаршалу-лейтенанту Гольцу, генералам Ренну, Розену, Полонскому, бригадирам П.И. Яковлеву, Г.И. Кропотову, Ф.Н. Балку и многим другим. При этом отметим, что большую часть писем Петр, зашифровывал сам, а также лично составил ряд шифров. Ответы на письма царя военачальники также шифровали, при этом нередко собственноручно.

Как и в дипломатической переписке, для защиты военных сообщений использовались шифры, составленные на разных языках. В основном в этот период применялись шиф-

ры с русским, немецким и французским алфавитом открытого текста, при этом помимо отдельных букв шифровались также слоги, слова, и целые предложения соответственно русские, немецкие, французские, т.е. большинство шифров представляли собой номенклаторы. Сам Петр I предпочитал французские шифры.

При использовании разноязыких шифров иногда случались казусы, так в одном из писем фельдмаршал Огильви докладывл Головкину, что не смог прочесть ни одно из присланных распоряжений ему Петра так как: «Французские цифирные грамотки нихто читать не может, тако не знаю, что на них ответствовать… Прошу… извольте мне на все мои письма ответ учинить немецкою цифирью, ибо той французжкой никто не разумеет» [Соболева, 2002]. О том же Огильви докладывал и самому Петру; «…никого здесь нет, который бы французское ваше мог разуметь, понеже Рен ключ оттого потерял... Изволте ко мне через цифирь мою писать, чтоб я мог разуметь» [Соболева, 2002].

Причину перехода с немецкого шифра на французский Петр объяснил так: «Французскою азбукою к вам писали для того, что иной не было. ***А которую вы перво прислали, и та не годна, понеже так, как простое письмо, честь можно*** (выделено авт.). А когда другую прислал, то от тех пор ею, а не французскою, к вам пишем. А и французский ключ послан» [Соболева, 2002].

Выделенный фрагмент данной цитаты имеет очень большое значение, это одно из первых документальных подтверждений наличия в России такого важного аспекта криптографической деятельности как криптоанализ[1]. При этом важно отметить, что занимался оценкой стойкости российских

[1] Напомним, что криптоанализ – наука о дешифровании шифров, он применяется к «чужим» шифрам для получения информации и к собственным для оценки их стойкости и, соответственно, возможности использования для защиты своих секретов, В данном случае Петр признал стойкость шифра Огильви недостаточной и отказался от его применения.

шифров не кто-нибудь, а сам царь!!! Об этом далее, а пока продолжим рассмотрение особенностей использования шифров для обеспечения конфиденциальности русской военной переписки.

Были случаи, когда расшифровать полученное сообщение было невозможно из-за отсутствия ключей. Такая ситуация сложилась, например, 29 января 1706 г. Петр собственноручно по-французски написал письмо князю Репнину. Частично это письмо было шифрованным, но у корреспондентов не оказалось ключа для расшифрования письма царя. Относительно отсутствия ключей генерал Ренн (воевавший в то время с вместе с Репниным) писал Петру: «Пресветлейший, державнейший царь, великомилостивейший Государь. Во все покорность Вашему пресветлому Величеству доношу: вчерашнего дня получил я личбу цифрами чрез посланного от Вашего пресветлого Величества смоленских полков прапорщика, по которой с господином генералом князем Никитой Ивановичем (официальное имя Репнина было Аникита, поэтому ранее даны его инициалы А.И. – примеч. авт.) будем вразумляться. Только мое несчастие, что той личбы ключи отосланы в обозе. Благоволи, Ваше пресветлое Величество, приказать прислать ключи, а мы и без ключей покамест, как можно мыслить и по указу Вашего пресветлого Величества поступать будем, также и друг друга покидать не будем...» [Соболева, 2002].

Все же приведенные случаи являются досадным исключением, в целом доставка ключевой документации была хорошо организована, при этом учитывалась возможность утраты ключевой информации в результате боевых действий. Чтобы этого не произошло, принимались различные меры. Ключ к шифру вручался непосредственно тому лицу, с кем предстояло переписываться. Однако ключи или их части могли передаваться с нарочными. Для этого их упаковывали в конверт, который опечатывался несколькими сургучными печатями. Как уже упоминалось ранее в письме (или на конверте) писалось имя нарочного. Как и шифрпослания, ключевая информация нередко пряталась в одежду, обувь, снаряжение

и др. При этом часто корреспонденты были обязаны доложить о благополучном получении ключевой информации, только после этого организовывался канал шифрованной связи. Например, в 1709 г. Я.В. Полонскому было поручено следить за движением войска старосты бобруйского и не допускать его соединения с корпусом шведского генерала Крассау. Полонскому вменялось докладывать обстановку шифром. «При этом посылаем к Вам ключ,– писал Петр,– и ежели сей посланный здорово с ним поедет, и о том к нам отпиши, дабы мы впредь нужные письма могли тем ключом писать и посылать» [Соболева, 2002]. Следует отметить, что в переписке Петра слово «здорово» означало «успешно», «благополучно» и др.

Полученные сообщения Петр I проверял лично во избежание их возможной перлюстрации. Вот его оценка полученной корреспонденции: «Полученные наветы пришли благополучно, и то по печатям гораздо смотрено» Следует отметить, что в то время искусство безуликовой перлюстрации посланий и подделки печатей, как и обнаружения скрытых посланий, было уже хорошо развито. Так что внешний осмотр полученных сообщений не гарантировал обнаружения факта имевшей место перлюстрации. Хотя безуликовая перлюстрация была непростой задачей [Бабаш, 2002].

Иногда в одно и тоже воинское соединение посылались совершенно разные ключи, такой случай имел место в 1707 г. Петр I не доверял Огильви и прикомандировал к нему А.И. Репнина, который наблюдал за действиями фельдмаршала. Репнин получил особый шифр. «При сем,– писал Петр 28 мая 1707 г. – посылаетца Вам азбука особливыми литерами и знаками имян изображенная, против которой изволте в нужное время ради снисения оною азбукою к нам писать» [Соболева, 2002].

Спустя две недели Петр посылает Репнина срочно ехать в район города Быхов с целью организовать боевые действия против литовского генерала Синицкого, перешедшего на сторону Станислава Лещинского. При этом Репнину предписывалось взять шифр у генерала Р.Х. Боура, который уже свыше двух месяцев находился в лагере под Быховом и пытался зама-

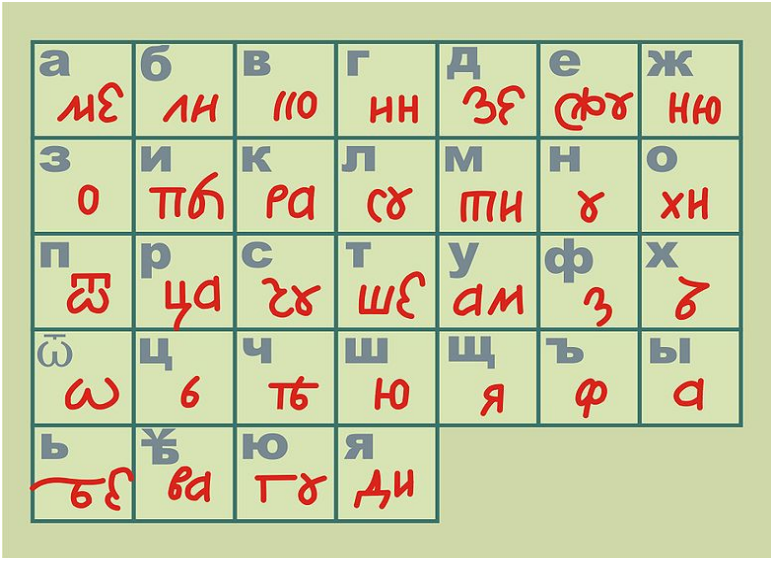
нить Синицкого в ловушку и арестовать. Переписка царя с Боуром шифровалась с помощью немецкого шифра. «Немецкой цифирью» был и шифр в переписке с фельдмаршалом-лейтенантом Гольцем» [Соболева, 2002], [Словарь, 1984]. Вообще практика наблюдения за генералами – иностранцами была обычным делом, так генералу Георгу-Густаву Розену в 1706 г. был приставлен сержант Преображенского полка А.В. Кикин. Розен использовал немецкий шифр, такой же имелся у Кикина [Соболева, 2002].

Теперь же приведем оригинальный военный шифр 1708 г., который использовался для шифрования сообщений во время Северной войны. На рис. 2.6 представлен ключ к этому шифру и его адаптация к современному русскому алфавиту. Это номенклатор (суплемент приведен далее) на основе шифра разнозначной замены, в качестве знаков шифрованного текста используются буквы и биграммы (двухбуквенные сочетания), алфавит русский.

Этот шифр имел следующие правила пользования: «Сии слова без разделения и без точек и занятых писать, а вместо точек и запятых и разделения речей вписывать из нижеписанных букв (это пустышки, которые, как и знаки суплемента определить пока не удалось – *авт.*)» [Соболева, 2002].

Суплемент – это небольшой словарь с именами некоторых государственных деятелей и географическими наименованиями, необходимыми для переписки о событиях на вполне определенном театре военных действий (графъ Фризъ, Речь Посполитая, князь Примась, гетманъ Огинский, Сапега. прусы польские, Литва, Великопольша и др.) [Соболева, 2002]. Наличие суплемента нашло отражение в правилах пользования, где говорится: «Буде же когда случится писать нижеписанных персон имяна и прочее, то оныя писать такими знаки, какия против каждой отмечено, однакож писать все сплош, нигде не оставливая, а между ими ставить помянутыя буквы, которыя ничего не значат» [Соболева, 2002].

Для примера зашифруем слово ПОЛТАВА, шифртекст будет выглядеть так: ОТХИСУШЕМЕКОМЕ.



А	Б	В	Г	Д	Е	Ж	З	И	К	Л
ме	ли	ко	ин	зе	жу	ню	о	пы	ра	су
М	Н	О	П	Р	С	Т	У	Ф	Х	Ы
ти	у	хи	от	ца	чу	ше	ам	з	ъ	от
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Ъ	Ю	Я	
ь	ъ	ю	я	ф	а	бе	ва	гу	ди	

Рис. 2.6. **Русский шифр разнозначной замены (1708 год) [Соболева, 2002]**

Хотя шифрованный текст писался слитно без пробелов. Но шифрообозначения подобраны таким образом, что при расшифровке это не вызывало никаких трудностей. Большинство согласных в виде слога. Причем каждая согласная участвует только в одном каком-то слоге. Исключения составляют: буква Ф без слога и согласная З, которая используется как в

слоге ЗЕ так и в одиночном исполнении З. Все гласные в основном без слогов. Исключения составляют только гласные А и И, которые могут быть также в составе слогов АМ и ИН соответственно.

Следует отметить, что шифры такого типа являются несколько более стойкими, чем «классическая» простая замена, но они чувствительны к ошибкам при шифровании. Как к замене нужной буквы на другую букву, так и к пропуску или вставке лишней буквы [Бабаш, 2002].

Особое место занимает шифрованная переписка А.Д. Меншикова, с 1704 г. он был фактическим заместителем царя на фронте и вообще – один из самых доверенных лиц Петра I. После Полтавской победы царь присвоил Меншикову чин генерал-фельдмаршала, еще раньше он получил титул Светлейшего князя. В ходе Северной войны Меншиков вел обильную шифрованную переписку с Петром и другими руководителями России, военачальниками и прочими корреспондентами по военным, политическим, хозяйственным и прочим вопросам. При этом отметим курьезный факт – Светлейший князь был практически неграмотным и наибольшее, на что его хватало, это поставить на письме свою подпись. Делопроизводство ему помогал вести обильный штат секретарей, адъютантов и пр. Тем не менее, Меншиков оказался первым из русских, кого иностранное академическое учреждение избрало своим членом. 25 октября 1714 г. из Лондона пришло письмо, подтверждающее членство Светлейшего в Королевском обществе, подписал его не кто иной, как сэр Исаак Ньютон! (Кстати сам Петр был избран членом французской академии лишь в 1717 г.). Правда следует отметить, что, не смотря на малограмотность, Меншиков обладал феноменальной памятью, огромной работоспособностью, большим опытом в военных и других делах. Все это позволило ему долгое время находится у вершины пирамиды власти государства Российского [Павленко, 1989].

Теперь же подробнее рассмотрим содержание шифрпереписки «полудержавного властелина», как называл Меншикова А.С. Пушкин. Разумеется, главным корреспондентом Мен-

шикова был Петр, до Полтавского сражения основной темой переписки были военные вопросы. Так в январе 1708 г. накануне решающих сражений Северной войны Петр I послал Меншикову шифрованное «Рассуждение», которое должно было рассматриваться 3 февраля в Вильно на военном совете, и просил Светлейшего высказать свои соображения по данному вопросу. В другой раз «Петр требовал, чтобы Меншиков со своей стороны прислал «Рассуждение» цифирью» [Соболева, 2002].

Весьма важное сообщение о состоянии шведской армии было отправлено Меншиковым Петру в начале 1708 года: «Рядовые солдаты к королю приступили, прося, чтоб им хлеба промыслил, потому что от голода далее жить не могут» [Павленко, 1989]. Это сообщение показывает, что только недавно принятая тактика изматывания противника, лишение его запасов продовольствия и фуража, начала давать свои результаты.

Хотя система связи для осуществления управления войсками в Петровскую эпоху постоянно совершенствовалась, случались и сбои. Один из них произошел осенью 1708 г. Как было отмечено выше из-за эффективных действий русских войск шведы «голод имеют великий» [Павленко, 1989]. Положение шведской армии усугубилось 28 сентября, когда в результате сражения при деревне Лесная, шведы лишились шедшего к ним большого обоза. В этой ситуации стратегическое значение приобрел город Батурин, где изменник Мазепа сосредоточил большие запасы продовольствия, фуража и прочего имущества, в котором так нуждались Карл и его армия. Началось своеобразное «соревнование» с одной стороны к городу шли русские во главе с Меншиковым, а с другой Карл и Мазепа со своими войсками. Хотя захват Батурина русскими был крайне желателен, Петр не хотел рисковать своими войсками, он понимал, что шведская армия существенно превосходит силы Меншикова.

План царя был таков, если можно опередить шведов, то Батурин надо брать, если нет – отступать, не ввязываясь в бой. Времени у Меньшикова было очень мало, так как русским войскам не удалось помешать шведам реку Десну и перед

шведской армией была открыта прямая дорога на город. Об этом Петр и пишет Меншикову 31 октября: «Неприятель, пришед, стал у реки на Батуринском тракте и для того изволь не мешкать», 1 ноября: «Объявляем вам, что нерадением генерал маеора Гордона шведы перешли сюды. И того ради изволте быть опасны, понеже мы будем отступать к Глухову. Того ради, ежели сей ночи к утру или поутру совершить возможно, с помощью божиею, оканчивайте. Ежели же невозможно, то лутче покинуть, ибо неприятель переберетца в четырех милях от Батурина» [Павленко, 1989], и наконец 2 ноября, получив от разведки данные о замедлении продвижения противника (изможденная голодом и болезнями армия не могла совершать марш быстро, как бы того не хотелось Карлу): «Сей день и будущая ночь вам еще возможно трудитца там, а далее завтрашнего утра (ежели чего не сделано) бавитца (т.е. пребывать) вам там опасно» [Павленко, 1989].

Однако эти указания царя опоздали, 2 ноября Меншиков берет Батурин штурмом (гарнизон города составляли сторонники Мазепы), часть запасов забирает с собой, а остальное уничтожает. Этот эпизод показывает, что в условиях быстро меняющейся военной обстановки скорость передачи информации курьерами может оказаться недостаточной. Хотя на этот раз для русских все обошлось благополучно, не полученные вовремя сообщения не повлияли на исход боевых действий. Получив известие об успехе Меншикова, Петр отправляет ему поздравление: «Сего моменту получил я Ваше зело радостное писание, за которое Вам зело благодарны…» [Павленко, 1989].

Об особых отношениях царя и Меншикова свидетельствует письмо Петра к его супруге Дарьи Михайловне «у них все благополучно и от князя (Петр – *авт.*) получает ежедневные ведомости» [Павленко, 1989]. Хотя номинальным главнокомандующем русской армии числился Б.П. Шереметев, фактически командовал сам Петр, а в его отсутствии Меншиков (напомним, что звание генерал-фельдмаршал Светлейший получил только после Полтавы). Руководящие указания Петра («пункты») Меншиков нередко получал раньше, чем фор-

мальный командующий. Об этом свидетельствует письмо Петра I Б.П. Шереметеву, отправленное из Воронежа 1 апреля 1709 г.: «… Пункты… отдали мы господину генералу князю Меншикову и с тех для ведома … посылаем к вам копию, цифирью писанную. Подтверждаю дабы вы чинили по тем пунктам, которые с Воронежа Вам посланы, а писаны оныя цифирью, а таковые даны и генералу князю Меншикову» [Соболева, 2002].

Переписка Петра с Меншиковым касалась не только военных вопросов, как губернатор Санкт-Петербурга Александр Данилович докладывал о положении в столичной губернии, выполнении кораблестроительной программы, порученной ему царем, обсуждалось и много других тем. Помимо Петра Меншиков вел обширную шифрованную переписку с значительным количеством других корреспондентов. Среди них дипломаты Г.Ф. и В.Л. Долгорукие (номенклатор для переписки с последним представлен на рис. 2.7).

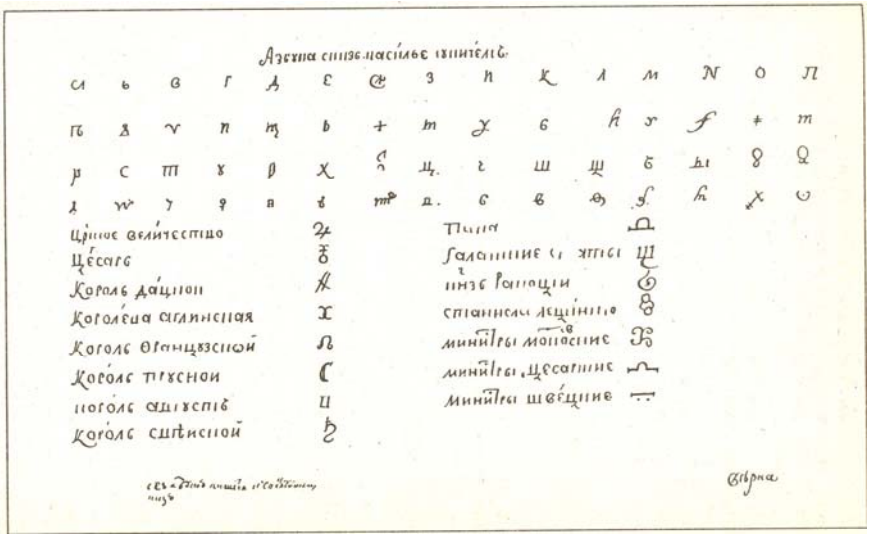


Рис. 2.7. **Шифр для защиты переписки между А.Д. Меншиковым и В.Л. Долгоруким [Соболева, 2002]**

Еще одним корреспондентом Меньшикова был бригадир Г.И. Кропотов. В 1709 г. он был направлен царем на границу с Молдавией в крепость Каменец-Подольский. Миссия Кропотова была очень важной, ему надлежало воспрепятствовать возможному передвижению Карла XII из Турции в Молдавию и далее по горному проходу Кампулунг в Венгрию. Кропотов должен был захватить шведского короля, если он отважится на такое путешествие. Разумеется, все свои сообщения Кропотов был должен шифровать: «о вышеописанных делах … писать цифирью» [Соболева, 2002]. В основном, Кропотов вел переписку с А.Д. Меншиковым и молдавским господарем Михаилом Раковицей, в шифрованной переписке с последним состоял также переводчик Кропотова А. Ботвинкин. Также шифровалась переписка между Раковицей и молдавским послом в России Георгием Кастриотом. Судьба М. Раковицы сложилась трагически, за сотрудничество с Россией он был убит турками, Кропотов продолжал находиться на молдавской границе и вести оттуда шифрованную переписку и в 1710 г. [Соболева, 2002].

Разумеется, поворотным пунктом Северной войны стало сражение под Полтавой. Описание самой битвы выходит за рамки данного труда, отметим лишь один интересный момент, связанный с использованием весьма оригинальных способов передачи информации. При осаде шведами Полтавы в июне 1709 г. (т.е. не задолго до знаменитого сражения), гарнизон города общался с основными силами русской армии при помощи шифрованных писем, которые помещались в полые ядра. Такие «контейнеры» выстреливались из пушек, так как другие способы связи с осажденным гарнизоном были невозможны. При этом для подтверждения получения письма использовалась свето-звуковая сигнализация с особым кодом. Так 19 июня 1709 г. комендант Полтавы И.С. Келлин получил от Петра I шифрованное письмо (для надежности оно было отправлено 6 экземплярах), в конце которого были такие слова: «Когда сии письма получите, то дайте в наши шанцы сегодня знак, не мешкав, одним великим огнем и пятью пушеч-

ными выстрелами рядом…что вы те письма получили» [Соболева, 2002]. 21 июня Келлин описанным выше способом переправил Меншикову шифрованное письмо, в котором сообщил о наблюдавшейся из Полтавы «тревоге в шведском лагере и перегруппировке войск неприятеля в связи с переходом русской армии на правый берег Ворсклы» [Соболева, 2002]. Кстати отметим, что Петр очень спешил из Азова, чтобы поспеть к сражению, но в случае опоздания доверил Меншикову руководство войсками следующей шифровкой: «однако понеже въ нужномъ дълъ и часъ потерять нужной бываетъ худо, то для того, ежели что надлежитъ нужно, то, не дожидаясь меня, съ помощью Божіею, дълайте». Но, как известно, Петр успел и лично возглавил русскую армию в сражении, определившем будущее России.

Другим «оригинальным средством» передачи информации, использовавшимся на поле боя Петром I была специально обученная собака. Она доставляла зашифрованные приказы Петра командирам русской армии и приносила императору ответные донесения. С этого времени практика использования собак для связи была развита довольно широко в российской армии. Так, например, в 1912 г. были созданы специальные питомники для обучения собак-связников в лейб-гвардии Измайловском полку (Санкт-Петербург) и лейб-гвардии Гусарском полку (Царское село). В советской армии собаки-связники применялись очень активно, в частности они участвовали в боях на реке Халхин-Гол (1939 г.) и Великой Отечественной войне. В период ВОВ собаками было доставлено около 200 000 донесений. Во время этой войны собаки использовались и для прокладки проводных линий связи, они размотали 7883 км телефонного кабеля [Гладыш, 2005].

С развитием российского военного флота была создана служба наблюдения и связи. Для передачи сообщений использовались наиболее быстроходные суда, они же вели наблюдение за флотом противника. Эту же задачу выполняли береговые наблюдатели. Связь между кораблями осуществлялась с помощью световых сигналов, выстрелов, а так же с по-

мощью флажного семафора, когда каждое положение рук сигнальщика соответствует одной букве. Таким способом передаётся определённое высказывание (полный аналог текста) с помощью элементарных визуальных сигналов. Использовался также флажный код, при таком способе передачи информации каждой букве алфавита соответствует флаг определённой формы и расцветки, вывешиваемый на мачте. Таким образом, можно составить комбинацию флагов соответствующую любому сложному высказыванию. Для повышения скорости передачи информации используются сигналы из одного, двух или трёх флагов, но при этом каждый флаг или их комбинация соответствуют целой фразе. Для шифровки и расшифрования используются специальные кодовые книги – своды сигналов. Текст передается «по буквам» только для совершенно необычных сообщений, и это обстоятельство сигнализируется особым вымпелом над комбинацией флагов. В данном случае мы имеем полный аналог номенклатора для оптической связи. Служба наблюдения и связи доказала свою эффективность во время кампании на Балтийском море 1720 г. В это время на Балтике действовал объединенный англо-шведский флот (англичане решили таки помочь шведам в борьбе с Россией). Благодаря своевременно полученной информации о передвижениях флота противника, удалось подготовить к обороне прибрежные города и осуществлять маневр основными силами флота, в сражение с которыми командующий объединенным флотом английский адмирал Норрис вступать не решался. Мало того, когда 28 июня 1720 г. соединение из 60 галер под командованием М.М. Голицына атаковало у мыса Гренгам шведскую эскадру, крейсировавшие неподалеку англичане не решились помочь союзникам. В результате 4 шведских фрегата были взяты на абордаж и стали нашим трофеем, а остальные спешно покинули «поле боя». Вообще русский галерный флот в 1720 г. действовал весьма активно, высаживались десанты на шведское побережье и противнику наносился большой ущерб (уничтожались промышленные предприятия, склады, военные гарнизоны и др.). Благодаря получаемой от

службы наблюдения и связи русским «малым судам» удавалось избегать встречи с объединенным флотом.

Единственным «успехом» адмирала Норриса стал десант на небольшой остров Нарген в конце мая 1720 г., на острове была обнаружена пустая изба и баня, обе постройки были сожжены, после чего десант ретировался на корабли. Подводя итоги этой компании можно утверждать, что 600000 фунтов, потраченные англичанами на эту экспедицию были выброшены на ветер. Русские, наоборот использовали этот поход в информационной борьбе. Петр дал указание князю Куракину «как можно шире сообщить в Европе через газеты об успехах Норриса. А особливо об избе и бане» [Молчанов, 1984]. По поводу этих событий Меншиков ехидно заметил в письме к Петру: «Уступите добычу сию им на раздел, а именно баню шведскому, а избу английскому флотам» [Молчанов, 1984].

В 1716 г. был принят «Устав воинский», первый в истории России документ подобного рода. В соответствии с Уставом учреждены должности «адъютантов, ординарцев, курьеров для передачи и доставки секретных донесений» [Астрахан, 1996], а также отредактированы «Правила действия военно-полевой почты». Военная полевая почта, стала активно использоваться для быстрого обмена конфиденциальной корреспонденцией между крупными воинскими соединениями и вновь создаваемыми центральными органами управления армией и флотом – Военной коллегией и Адмиралтейств-коллегией. Для доставки особо важной и срочной воинской корреспонденции в адрес императора или президентов оборонных коллегий при главнокомандующих армиями были учреждены должности военно-полевых курьеров. Следует отметить, что «собственноручно отредактированные Петром I «Правила действия военно-полевой почты» являются, по сути, первым дошедшим до нас документом той эпохи, в котором было четко и определенно сформулировано назначение военно-курьерской связи» [Астрахан, 1996].

Использовались шифры и для обеспечения конфиденциальности переписки по важным внутриполитическим во-

просам. Например, обильная переписка велась по поводу крестьянского восстания Кондратия Булавина бушевавшего на Дону в 1707–1709 гг. Шифр простой замены 1708 г. приведен ранее (см. рис. 2.2–2.4). В этом же году использовался и шифр разнозначной замены (см. рис. 2.3), этот вариант шифра отличается тем, что в нем на одну пустышку меньше и суплементом. Словарь этого шифра был связан с тематикой восстания и содержал такие понятия как, Булавин, губернатор Азовский, войсковой атаман и казаки и др.

Как отмечается в книге [Соболева, 2002] в государственном архиве Татарстана хранится письмо Петра I азовскому губернатору И.А. Толстому, в котором говорится о том, что в Азов высылается экземпляр ключа к вышеозначенному шифру. Вот его текст:

«Господин губернатор! Понеже Вы уже известны о умножении вора Булавина и что оный идет внизъ; того ради, для лучшаго опасении сихъ нужныхъ местъ, послали мы к вамъ полкъ Смоленский изъ Киева, и велели ему на спехъ иттить; а сего поручика нашего господина Пескарского послали к Вамь, дабы уведать подлинно о вашемъ состоянии и нътъ ли какой блазни у васъ межъ солдаты. Также (от чего Боже сохрани, ежели Черкаскъ не удержится) имеешь ли надежду на своихъ солдатъ, о чемъ о всемъ дай немедленно знать чрезъ сего посланною, сь которымъ послана к вамь цифирь для корреспонденции к намъ. Также другой ключъ для корреспонденции съ господиномъ маеоромъ (гвардии Долгорукимъ), который посланъ на техъ воровъ съ воинскими людьми, прочее наказано оному посыльному словесно. Piter».

Помимо Петра и И.А. Толстого, ключ к данному шифру имелся у А.Д. Меншикова, адмирала Ф.М. Апраксина, который занимался строительством кораблей и береговой инфраструктуры на юге России, В.В. Долгорукого, командующего вооруженными силами, действующими против восставших. Участвовал в подавлении восстания и вышеупомянутый Г.И. Кропотов, вот какие наставления по организации конфиденциальной связи дает ему А.Д. Меншиков: «… между тем временем как к

нам, так и к господину маеору Долгорокому писать с нарочными курьерами, которых хотя шпигами или под видом переметчиков сквозь воровские войска посылать, ежели каким иным способом послать будет невозможно, и такие с ними письма писать цифирью» [Соболева, 2002].

Имелись особые шифры для секретной переписки царя и других руководителей России с главами пограничных районов и губерний, а во время войны и «прифронтовых» территорий и городов. В частности шифрпереписка велась с киевским губернатором Д.М. Голлицыным и обер-комендантом Нарвы К.А. Нарышкиным. С учреждением Сената Петр I начинает шифровать свои письма и этому органу государственной власти, зашифрованные фрагменты этих писем обычно касались военных вопросов [Соболева, 2002].

Весьма интересным документом является блокнот с шифрами, которыми пользовался Петр I. Это была тетрадь со сторонами, размером 20х16 см, листы которой скреплялись веревкой. На каждой странице было записано по одному шифру. Это были шифр, который был прислан Петру из Коллегии иностранных дел во Францию в 1720 г. для переписки «от двора ко двору», шифр «дли писем к графу Г. и барону П.», шифры для переписки с князьями Григорием Федоровичем Долгоруким и А.И. Репнину (1715 г.), «азбука, которая была прислана от двора его царского величества при указе №..., а полученная 30 июля 1721 г.» и, наконец, упомянутая «азбука цифирная, какову прислал Дмитрий Константинович Кантемир в 1721 г.» [Соболева, 2002].

Интересно отметить, что в Петровскую эпоху практиковалось использование одних и тех же шифров на различных каналах связи. При этом он мог использоваться для обеспечения конфиденциальности переписки по различным вопросам. Так приведенный шифр разнозначной замены с небольшими изменениями использовался на театре боевых действий Северной войны и на Дону. Нередко шифры использовались вообще без каких либо изменений. Так известно [Соболева, 2002], что шифр Петра, с помощью которого он переписывал-

ся с Ф.Н. Балком в 1710–1711 гг., позже использовал Д.М. Голицын, а в 1720 г. его получил князь Борис Мещерский. Шифр ранее, используемый для переписки П.П. Шафировым, в 1715 г. был использован для обеспечения конфиденциальной связи между Г.И. Головкиным и П.И. Ягужинским, а 1716 г. его получил П.И. Беклемишев. Один и тот же шифр использовался для защиты переписки между сотрудниками Коллегии иностранных дел с Я.В. Полонским, Н.Ю. Ифлантом, С.В. Рагузинским, С.Г. Нарышкиным. Имелись и другие примеры подобного рода. Следует отметить, что если шифр не скомпрометирован, то длительное использование его на различных каналах связи вполне возможно. Однако с точки зрения обеспечения безопасности связи длительное и одновременное использование шифра существенно повышает риск его компрометации. В Петровскую эпоху, созданием шифров занимался весьма ограниченный круг лиц, при этом у самого царя, канцлера и других руководителей имелось много различных обязанностей, и посвящать много времени разработке новых шифров они не могли. Существовала также проблема доставки новых шифров корреспондентам, особенно на театре военных действий и послам во враждебных России странах. Именно по этим причинам повторное использование шифров было широко распространено в России на протяжении всего XVIII в. [Соболева, 2002].

Приведем один интересный эпизод, связанный с «несанкционированным» использованием шифра. С мая 1718 по октябрь 1719 г. на Аландских островах (ныне Финляндия, тогда, как и вся эта страна принадлежали Швеции, однако в 1714 г. были захвачены русскими войсками [Буганов, 1989]) шли мирные переговоры между делегациями России и Швеции, их целью было положить конец Северной войне. Эти переговоры получили название Аландский конгресс, российскую делегацию на них возглавляли Я. Брюс и А.И. Остерман. О ходе переговоров Остерман информировал Петра и Коллегию иностранных дел с помощью особого шифра. Однако у Остермана был еще один шифр на немецком языке, который он

использовал в тайной переписке с П.П. Шафировым. Дело в том, что Остерман, при поддержке Шафирова проводил на переговорах линию о заключении после примирения со Швецией военного союза, в целях экспансии в западную Европу. Эта линия, мягко говоря, расходилась с официальной линией России, истощенной 21-летней войной. Новые завоевательные походы были не нужны, мало того Петр готов ради скорейшего заключения мира со Швецией вернуть ей часть территорий, находившихся под русским контролем (в частности в Финляндии) и передать под контроль союзников ряд занятых русскими войсками территорий в Германии и Польше. Так же не надо забывать о сложной ситуации на южных и восточных рубежах России – извечный враг Турция был очень силен, продлились набеги крымских татар, имелись противоречия с Персией. Именно восточный вектор стал приоритетным в политике нашей страны после окончания Северной войны. Исходя из сказанного, новая война на Западе России была не нужна, так что если бы Петр узнал о деятельности Остермана, тот мог подвергнуться вполне обоснованным репрессиям. Поэтому «заговорщики» и использовали особый шифр. Кстати сам факт ведения шифрованной переписки втайне от Петра, если бы стал известным, мог для ее участников привести к самым серьезным последствиям [Молчанов, 1984]. К счастью никаких вредных последствий дипломатическая деятельность Остермана не принесла. 30 ноября 1718 г. Карл XII при осаде крепости Фредрикстен в Норвегии был убит шальной пулей. Аландский конгресс работал еще почти год, но мир так и не был заключен. Преемница и сестра Карла королева Ульрика не решилась заключить мир с Россией, надеясь на помощь Англии. Война продолжалась еще 2 года и закончилась 30 августа 1721 г. Ништадтским миром (подписан в городе Ништадт, Финляндия), русскую делегацию возглавляли все те же Брюс и Остерман. О заключении мира немедленно было сообщено шифрованным письмом царю Петру.

Теперь поговорим о криптоанализе. Скорее всего, этот вид криптографической деятельности возник в России имен-

но в Петровскую эпоху. Ранее уже была приведена цитата из письма Петра, показывающая большой интерес царя к обеспечению стойкости отечественных шифров. Вот еще одна нелестная оценка царя одного из российских шифров: «Сия цифирь зело к разобранию легка» [Бабаш, 2002]. Стали проявлять в России интерес и к шифрам иностранных государств, конечно о регулярном дешифровании иностранной переписки речь пока не шла, однако заинтересованность в получении информации таким методом уже была. Русским дипломатам, разведчикам и другим представителям за границей предписывалось добывать любую информацию, касающуюся шифров, организации связи, открытых текстов (против атаки «открытый текст – шифрованный текст» подавляющее большинство шифров того времени было не устойчиво). На этих лиц и их зарубежную агентуру также возлагалась задача организации перехвата иностранных сообщений за границами России.

Отметим, что во время Северной войны русскими войсками были захвачены Нарва, Рига, Дерпт и другие крепости в Прибалтике, большие трофеи достались русской армии после побед у Лесной, Переволочной и конечно же Полтавы. Мало того после поражения под Полтавой «первый шведскій министръ, графъ Пиперъ, увидя, что ему спастись невозможно, самъ пріѣхалъ въ Полтаву купно съ секретарями королевскими Цедергольмомъ и Дибеномъ» [Князьков, 1914], т.е. они добровольно сдались русским, а ведь именно секретари нередко вели шифрованную переписку коронованных особ и министров. Могли оказаться шведские шифры и среди трофеев в упомянутых битвах. Пока автору не удалось найти каких-либо фактов на этот счет, этот вопрос требует дальнейших исследований.

Кроме шифрованных сообщений врагов интересовала Петра и информация, содержащаяся в шифрпереписке руководителей и дипломатов, союзных России, и нейтральных государств. Такая переписка велась, Петр I не запрещал иностранным представителям использовать шифры, но требовал представление ему открытых текстов шифрованных посланий

(речь, естественно, идет о тех посланиях, которые удавалось перехватить). Эти представители могли хранить свою тайну от кого угодно, но не от первого Императора России. Однако не всегда иностранные представители выполняли это указание, но в этом случае Петр I не шел на осложнение дипломатических отношений. Так, например 1710 г. Петр I потребовал, чтобы посол Дании Юст Юль представил зашифрованный документ с расшифрованным текстом на обороте (речь в документе шла о полномочиях посла). Юль заявил, что такой документ выдает шифр, на что Петр I ответил, что особенной беды в том не будет, так как между царем и королем датским не должно существовать никаких тайн [Юль, 1899].

Иностранные представители свой отказ мотивировали тем, что наличие открытого текста к перехваченному шифрованному раскроет ключ. Тем самым они косвенно подтверждали, что надеются на тайные каналы передачи своих сообщений. Среди способов тайной передачи секретных сообщений была и стеганография (использование невидимых чернил).

Помимо Дании шифрованную переписку с королем Фридрихом и министром И.Г Кайзерлингом вел прусский посланник. Общались с помощью шифров со своими монархами, министрами и вельможами представители Австрии, Англии, Голландии, Франции и других государств.

Особый интерес Петра и других руководителей России вызывала шифрованная переписка саксонского курфюрста и польского короля Августа II. Помимо самого монарха польскую шифрпереписку, в частности вели Ян Шембек, А.Н. Синявский, К.Ф. Шанявский, С. Денгоф, а саксонскую – И.Ф. Арнштедт, Я.Г. Флеминг и другие [Соболева, 2002].

Кстати польскую корону Август получил с помощью России. Дело в том, что в Польше король избирается сеймом (так там называется парламент), после смерти в 1696 г. короля Яна Собесского, на престол претендовали Август и французский принц де Конти. При этом Франция собиралась послать в Польшу воинский контингент, а поскольку тогда Франция была союзницей Швеции, победа де Конти не устраивала Рос-

сию. Поэтому российские власти предприняли целый ряд мер политического, дипломатического, разведывательного и военного характера для возведения на польский престол Августа. Все эти мероприятия сопровождались обильной шифрперепиской между Москвой и российскими представителями в Польше. В этих событиях участвовал и сам Петр, так 12 июня 1697 г. он направил сейму специальное послание, в котором напомнил полякам, о том, что их страна состоит в союзе с Россией против Турции и прямо заявил, что избрание де Конти для России неприемлемо: «мы такого короля французской и турецкой стороны видеть в Польше не желаем» – писал русский царь [Кудрявцев, 2002]. Также были предприняты шаги дипломатического характера, в частности Петр направил письма бургомистру Данцига и королю Дании, в которых просил сделать все возможное, что бы помешать высадке французов в Польше. И, наконец, самым весомым аргументом было выдвижение к польским границам русского корпуса под командованием боярина М.Г. Ромодановского. Петр через российских представителей в Польше заявил полякам, что не допустит вторжение французских войск в Польшу и готовности ввести в Польшу русские войска. Тем временем российские представители в Польше во главе с А.В. Никитиным развернули активную деятельность по привлечению поляков на сторону Августа, применялись приемы информационной войны, велась активная разведывательная и агентурная работа, применялся и прямой подкуп потенциальных избирателей. Все эти меры дали результат, в 1697 г. саксонский курфюрст Фридрих Август, под именем Августа II стал королем Польши.

В ходе Великого посольства Петр посетил Августа, между ними сложились дружеские отношения. «Расставаясь, Петр и Август в знак приязни и верности слову обменялись шляпами и шпагами» [Кудрявцев, 2002]. Окончательно союз между Петром и Августом был заключен 11 ноября 1699 г. в Москве, саксонский курфюрст обязался немедленно начать войну против Швеции. Петр весьма ценил вновь приобретенного союзника, саксонская армия была весьма многочисленной и

считалась весьма хорошо обученной, к тому же Август мог привлечь к войне против Швеции войска Речи Посполитой. Интересно отметить, что даже в 1706 г. после многочисленных побед русской армии, Карл XII считал главным противником не ее, а саксонцев. Что касается Петра, то он настолько доверял саксонским союзникам, что поручил командование русскими войсками при первой осаде Нарвы (1700 г.) саксонским военачальникам фельдмаршалу герцогу Шарлю де Круа и генералу Галларту. Увы, доверие Петра саксонцы не оправдали де Кроа изначально крайне скептически относился к русской армии, свои крайне нелицеприятные отзывы по этому поводу он высказывал в письмах Августу, а чтобы русским не стало известно об их содержании использовался шифр [Буганов В.И., 1989], [Молчанов, 1984].

Отметим, что негативное отношение к способностям русских войск было характерно для многих офицеров-иностранцев участвовавших в первом Нарвском походе, доходило до того, что высокомерное и пренебрежительное отношение к русским солдатам со стороны их иностранных командиров, вызывало приступы лютой ненависти. Разумеется, данное обстоятельство оказывало крайне отрицательное влияние на моральное состояние русских полков. 18 ноября 1700 г. к Нарве подошел Карл XII и внезапно атаковал русские войска. Бой закончился для наших войск тяжелым поражением, русская армия потеряла всю артиллерию, а почти все офицеры (включая де Кроа) попали в плен [Буганов, 1989], [Кудрявцев, 2002], [Молчанов, 1984].

Поражение русской армии под Нарвой существенно повлияло на позицию Августа по отношению к продолжению Северной войны. Несмотря на личную дружбу с Петром, Август с самого начала стремился к сепаратному миру со шведами. Перед глазами саксонского курфюрста и польского короля стоял показательный пример другого члена антишведской коалиции – Дании. В 1700 г. (еще до вступления России в войну) Карл, не без помощи англичан и голландцев, молниеносным десантом разгромил датские войска и вывел из войны эту страну. Август

опасался (и не зря!!!), что его владения может постигнуть подобная участь, поэтому отнюдь не горел выполнять свои союзнические обязательства по отношению к России.

Хотя саксонские войска участвовали в боевых действиях, особых успехов не имели, мало того шведы нанесли им ряд тяжелых поражений. Дошло до того, что как уже упоминалось ранее Карл «назначил» своего короля Польши – Станислава Лещинского, положение Августа было незавидным, и он продолжал стремиться к миру со шведами.

Одним из тех, кто сообщал Петру о предполагаемой измене Августа, был Иоганн Рейнгольд фон Паткуль. Этот лифляндский дворянин был капитаном шведской армии, в своей стране он подвергся необоснованным репрессиям и вынужден был бежать за границу. Паткуль проявил себя как талантливый дипломат и разведчик. В 1699 г. Паткуль приехал в Москву и предложил Петру план создания антишведского союза. Как мы знаем, русское руководство уже вело активную деятельность в этом направлении. Петр оценил желание Паткуля добровольно служить России и «зачислил на русскую службу и определил в тайные советники, присвоив ранг чрезвычайного посла и воинское звание генерал-майора» [Очерки, 1999]. Позднее в 1704 г. Петр присвоил Паткулю за заслуги очередное звание генерал-поручика.

Имея многочисленные связи среди высшего руководства Австрии, Пруссии, Польши, Саксонии Паткуль сумел добыть важнейшую информацию политического характера, которая позволила российскому руководству быть в курсе действий и намерений своих союзников. К сожалению, эта информация была неутешительной. Так через свою агентуру Паткуль получил возможность ознакомления с секретной перепиской руководства Пруссии со Швецией. Напомним, что Пруссия заключила тайный союз с Россией против Швеции, формально же сохраняла нейтралитет, информация же Паткуля говорила о готовности Пруссии перейти на сторону Швеции. Русским дипломатам и лично Петру пришлось приложить огромные усилия по недопущению подобного развития

событий. Кстати сам Паткуль, имевший определенное влияние на прусских министров активно работал в этом направлении. В конце концов Пруссию удалось удержать от перехода на сторону шведов.

Однако наиболее ценной информацией переданной Паткулем в Россию были сведения о возможной измене Августа, «в своих донесениях в Москву Паткуль неоднократно отмечал непоследовательность польского короля в отношении союзнического договора» [Очерки, 1999].

Летом 1705 г. Паткуль очевидно получил исчерпывающие доказательства готовящейся измены Августа, он срочно попросил личной встречи с Петром. Петр предложил встретиться в городах Вильно, Ковно или Гродно, а «если дело столь неотложное воспользоваться шифром и передать информацию письменно» [Кудрявцев, 2002]. Однако сделать ничего не удалось, дело в том, что в августе 1705 г. саксонский курфюрст отправил к Карлу своих министров Ингофа и Фингстейна для переговоров о сепаратном мире. Через свою агентуру Паткуль узнал об этом и как полномочный посол России выразил Августу свой протест. Чтобы сохранить свою измену в тайне саксонцы арестовали русского представителя, несмотря на все протесты России освободить его не удалось. Дело в том, что Петр из политических соображений хотел любой ценой сохранить союз с Августом и вынужден был терпеть провокации «союзника», к тому же он до конца не мог поверить в измену человека, которого считал своим другом и считал все происходившее досадным недоразумением. Август же проявил верх двуличия, он убеждал русских, что все происходящее дело рук его министров и происходит без его ведома (сам он тогда находился в Польше). Однако российским разведчикам позднее удалось убедиться, что «в секретных письмах он (Август – *авт*.) полностью одобрил поведение своего Тайного совета» [Молчанов, 1984]. Как отмечалось ранее для секретной переписки Август пользовался шифрами, возможно наши разведчики получили доступ к открытым текстам сообщений или сумели раздобыть ключ, а возможно это один из первых

успехов наших криптоаналитиков в дешифровании зарубежной шифрпереписки. Данный вопрос требует дополнительных исследований.

Развязка наступила в конце августа 1706 г., тогда Карл стремительным броском явился в Саксонию, сопротивления ему никто не оказал, боясь потерять свое наследственное владение Август заключает со шведами Альтранштадтский (город в Германии, вблизи Лейпцига) договор о мире. По условиям этого договора Август отказывается от польской короны в пользу Лещинского, выходит из союза с Россией, а также обязуется выдать шведам всех пленных и перебежчиков, среди последних первым в списке был Паткуль. 10 октября 1707 г. русский разведчик И.Р. Паткуль был казнен шведами [Кудрявцев, 2002], [Молчанов, 1984], [Очерки, 1999].

Август сумел выторговать у Карла, что положения договора некоторое время останутся в тайне, русской разведке удалось узнать об этом лишь в ноябре 1706 г., правда при этом удалось добыть копию договора. Эту копию «для подлинного уведомления» Меншиков с театра боевых действий в Прибалтике выслал П.П. Шафирову, сопроводив шифрованным письмом: «Уже ныне мы подлинную ведомость получили о мире, каков учинил тайно король Август с королем швецким, и имеем з договорных статей списки» [Павленко, 1989]. Петр был очень расстроен предательством друга, он писал: «и в мысли не было, чтобы Август имел намерение о таком бесчестном мире с королем шведским, как действительно случилось» [Павленко, 1989]. Тем не менее, исходя из высоких политических соображений, впоследствии Петр простил предателя, силой русского оружия вернул Августу польскую корону, и формально продолжал считать его союзником, однако никакого доверия этому «союзнику» больше не было.

В заключении данной главы кратко рассмотрим криптографическую деятельность противников Петра. Основным соперником России в Петровскую эпоху была Швеция. Криптографией в Швеции занимались с древних времен. Тогда в Скандинавии использовалось руническое письмо. Руны (т.е.

знаки древнескандинавского алфавита) в алфавите были разбиты на три группы (см. рис. 2.8).

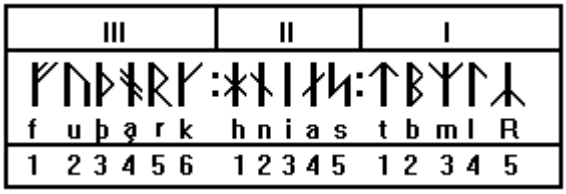


Рис. 2.8. **Скандинавские руны и их латинские эквиваленты**

Основная система шифрования представляла собой шифр простой замены – каждой руне соответствовали два знака шифртекста (обычно косые черточки разной длины). Количество черточек сверху обозначало номер группы, а снизу – номер руны в группе. Встречались и усложнения этой системы, например руны в группах перемешивались (см. рис. 2.9).

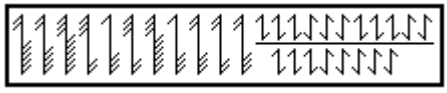


Рис. 2.9. **«Рунный» шифртекст**

До наших дней дошел памятник древней шведской криптографии – рёкский камень. Этот камень высотой более 4 мв находится на кладбище деревни Рёк. На нем нанесено 770 зашифрованных рун. Встречаются шифрованные рунические надписи и в других регионах Швеции.

Несмотря на то, что позднее в странах Скандинавии стала применяться латинская графика, руническое письмо употреблялось там до XIX в. Однако в XVI–XVIII вв. весьма небольшое количество людей знало рунические алфавиты, поэтому руническая запись даже без шифрования обеспечивала сохранение тайны переписки. В частности руны для защиты информации использовал шведский генерал Якоб де ла Гарди во время тридцатилетней войны (1618–1646 гг.).

В XVI–XVIII вв. Швеция играла активную роль в европейских делах. Ее армия в этот период времени участвовала в ряде крупных войн. Разумеется, задача обеспечения безопасности связи стояла весьма остро. Шифрование применялось для защиты дипломатических и военных сообщений. Так в 1676 г. за несколько дней до сражения между шведской и датской армиями под городом Лунд шведский король Карл XI отправил генералу Фабиану фон Ферсену шифрованное письмо со своими соображениями по стратегии и тактике шведов в предстоящей битве. Благодаря этой информации шведы одержали победу. Сражение под Лундом было одним из самых кровавых в истории Скандинавии, обе стороны понесли в нем большие потери.

Шведы использовали характерные для Европы того времени шифры, в основном номенклаторы. Интересно отметить, что дешифрование шведского номенклатора 1632 г. на рубеже XIX–XX вв. при проведении одного исторического исследования в интересах шведских властей, Р. Торпади послужило поводом к созданию шведского криптоаналитического бюро, которое получило название «комната 100». В 1700 г. основным шведским шифром был алфавитный словарный код на 4000 величин [Kahn, 1967]. Более подробную информацию о криптографической деятельности в Швеции можно получить из цикла статей [Бутырский, 2007].

Каких либо фактов успешного криптоанализа русских шифров Петровской эпохи шведами пока не обнаружено, а вот доступ шведской агентуры к открытым текстам шифрованных сообщений имел место. Примером может служить случай в местечке Биржи, где в 1701 г. состоялась встреча Петра с Августом II. Карл XII заранее узнал об этой встрече и направил к саксонцам агента, офицера шотландского происхождения. Этому агенту удалось получить чин поручика саксонского кирасирского полка и завести хорошие отношения с секретарями обоих государей. Благодаря этому шведский агент получил сведения о всех решениях принятых в Биржах и о содержании переписки между делегациями и их столицами [Кудрявцев, 2002].

Перехватывали русские сообщения и турки. Так в 1710 г. во время Прусского похода армия Петра оказалась в окружении, хотя турецкая армия в 4 раза превосходила русскую, она была полностью деморализована, столкновение с созданной Петром регулярной русской армией привело турок в шок. Но Петр и его военачальники об этом не знали, русские войска также были изможднены тяжелыми боями. Моральный дух российских войск могло поднять сообщение о том, что генерал Ренне, по приказу Петра овладел городом Браилов и зашел туркам в тыл, таким образом, уже для турецкой армии создалась угроза окружения. К сожалению, гонец, посланный Рене к Петру, попал в плен к туркам и важная информация не дошла до царя. Туркам удалось ознакомиться с содержанием сообщения, видимо оно или не было зашифровано или туркам удалось вскрыть шифр. Так или иначе, Прутский поход закончился неудачей для России. При заключении перемирия наша страна вынуждена была пойти на серьезные уступки туркам [Буганов, 1989].

Первый документально подтвержденный факт дешифрования российского шифра петровской эпохи имел место в 1719 г. Американский историк Д. Кан с ссылкой на английские архивы утверждает, что именно в этом году английский черный кабинет впервые дешифровал один из русских шифров простой замены [Kahn, 1967]. Однако отметим, что как упоминалось выше в уже в начале 20-х гг. XVIII в. в России активно применяются шифры пропорциональной замены, трудоемкость дешифрования которых значительно выше по сравнению с простой заменой.

Интересно отметить, что двумя годами ранее англичане достигли существенных успехов в дешифровании переписки нашего основного противника – Швеции. Многим читателям известно имя знаменитого английского писателя Д. Дефо, автора книги о Робинзоне Крузо. Но далеко не все знают, что Дефо – один из крупнейших профессионалов секретной службы Великобритании. Он осуществлял серьезные разведывательные операции, собирал важные сведения в интересах

английского двора. В феврале 1717 г. якобисты (сторонники свергнутого короля Якова II) замышляли восстание против действовавшего короля Георга I. Шведский король Карл XII был сторонником якобистов и оказывал им поддержку. Хотя Англия в период Северной войны занимала позицию дружественного нейтралитета по отношению к Швеции, Карл надеялся, что в обмен на помощь Якову в восстановлении на престоле, тот окажет прямую военную помощь Швеции в войне с Россией (как отмечалось выше, в 1720 г. англичане все же решились на прямое участие в войне, но толку от этого вышло мало). Английские правительственные агенты проникли в резиденцию шведского посла графа Юлленборга и нашли там немало «уличающих» документов, в том числе и личную переписку посла. Эта переписка была дешифрована известным британским криптоаналитиком того времени Э. Уоллесом. В организации этой акции принимал участие Д. Дефо. Шведский король Карл XII стал мишенью для враждебных выпадов со стороны англичан, а Дефо составил проект «обуздания» всех шведов, не исключая их короля [Гольев, 2008], [Kahn, 1967].

Теперь рассмотрим криптографическую деятельность украинского гетмана И.С. Мазепы (1644–1709). Мазепа 25 июля 1687 г. был избран гетманом Украины при активной поддержке фаворита правительницы Софьи князя В.В. Голицина, в первый период Северной войны он сохранял лояльность России, но уже тогда задумывал измену. В конце концов, гетман изменил Петру и перешел на сторону шведов. Мазепа проявлял большой интерес к почте. В начале XVIII в., когда скорая гоньба в Киев пришла в полный упадок, он неоднократно просил Петра I восстановить почту. В письмах гетмана есть одна весьма любопытная деталь: Мазепа упорно добивался запрещения пересылки челобитных запорожского старшины и полковников с нарочными гонцами. На первый взгляд кажется, что гетман руководствовался только интересами государства с целью экономии средств. В действительности это был весьма ловкий ход хитрого гетмана. Достаточно хорошо известно, что украинские полковники, знавшие об измене и

двурушничестве Мазепы, неоднократно посылали свои доносы царю. С установлением почты можно было путем организации перлюстрации заранее узнавать планы своих врагов и принимать контрмеры.

Кстати отметим, что при пересылке сообщений об измене Мазепы активно применялась стеганография, пророссийски настроенные украинцы опасались возможного захвата гонцов сторонниками Мазепы, поэтому сообщения тщательно прятались. Очень образно это описал А.С. Пушкин в поэме «Полтава» [Пушкин]:

Червонцы нужны для гонца,
Булат – потеха молодца,
Ретивый конь – потеха тоже,
Но шапка для него дороже,
За шапку он оставить рад
Коня, червонцы и булат,
Но шапку выдаст только с бою
И то лишь с буйной головою.
Зачем он шапкой дорожит?
Затем, что в ней донос зашит,
Донос на гетмана злодея
Царю Петру от Кочубея.

Напомним, что в это время Петр I сравнительно мало интересовался украинскими делами. Помыслы великого преобразователя были устремлены на северо-запад к Балтийскому морю. Только этим можно объяснить, что в его царствование почта в Киеве, хотя и не прекращала своей деятельности, но работала с небольшой нагрузкой и частыми остановками. Правда, когда военные действия против Швеции переносились на Украину, возрождалась скорая гоньба на юго-западных трактах и почта работала четко и с полной отдачей. Почти весь XVIII в. киевская почта влачила жалкое существование. Она считалась самой ненадежной в государстве. И только на исходе столетия, когда началось интенсивное освоение причерноморских владений России, украинская почтовая линия выдвинулась по значимости на одно из первых мест.

Активно использовал Мазепа и шифры. В тайне от России Мазепа на протяжении всего времени пребывания в должности гетмана вел секретную переписку с поляками, в Москве об этом знали, но смотрели на «шалости» гетмана сквозь пальцы (Польша тогда являлась союзником России). Однако в 1705 г. Мазепой всерьез заинтересовались шведы. В роли вербовщика выступила мать польского князя Вишневецкого (сторонника шведов) – княгиня Дольская. В конце 1705 г. Мазепа получил приглашение от Вишневецкого на празднование крещения его дочери. Там Мазепа знакомится с Дольской, после возвращения из поездки гетман посылает княгине шифр для организации дальнейшей переписки (к сожалению, пока автору не удалось установить какая система шифрования использовалась в этом случае). В шифрованной переписке Мазепы и Дольской обсуждаются вопросы перехода гетмана на сторону шведов. Княгиня утверждает, что Карл XII и Станислав Лещинский высоко ценят Мазепу и что Карл обещает ему престол будущей независимой Украины. В одном из писем Дольская, ссылаясь на мифическую беседу с генерал-фельдмаршалом Б.П. Шереметевым, заявляет, что Мазепа будет смещен с поста гетмана и заменен на Меншикова. Это становится «последней каплей» для Мазепы, он через Дольскую вступает в тайную переписку с Лещинским и окончательно переходит на сторону шведов [Кудрявцев, 2002].

Об измене Мазепы стало известно из перехвата переписки его сторонников, так 24 октября 1708 г. был захвачен гонец прилукского полковника Дмитрия Горленка (сообщника Мазепы), при нем обнаружено послание, содержащее такие слова: «мы с ясновельможным добродетелем нашим паном гетманом соединились со шведами» [Павленко, 1989]. Командующий российскими войсками на Украине А.Д. Меншиков шифровкой сообщил Петру: «И тако об нем инако разсуждать не извольте, только что совершенно изменил» [Павленко, 1989].

Карл XII рассчитывал на то, что Мазепа приведет к нему крупное войско (гетман обещал 20000 казаков), однако вместе с Мазепой прибыло по разным данным от 2 до 4 тыс. человек. Поняв, что в военном отношении союз с гетманом почти ничего дает, решил использовать его в дипломатической игре. На-

деясь привлечь на свою сторону как можно больше польских магнатов, Карл заставил Мазепу написать письмо Лещинскому, в котором гетман обязался передать Украину под власть Польши, «как законное достояние польских королей». Русским удалось перехватить это письмо и по указанию Петра, текст этого письма был размножен и распространен на территории Украины. Среди украинцев не было никого более ненавистного, чем польские паны, письмо Мазепы вызвало всплеск ненависти к гетману и шведам. Партизанская война против шведов, которая уже шла на территории Украины, резко активизировалась. Этот пример показывает, что Петр уделял большое внимание вопросам информационной войны. При этом следует отметить, что как было ранее сказано, Мазепа для переписки с Лещинским и другими своими корреспондентами использовал шифр, так что возможно вышеприведенные случаи, так же как и ознакомление с перепиской Августа один из ранних случаев успешного криптоанализа в России.

Судьба предателя незавидна, после разгрома под Полтавой Мазепа вместе с Карлом XII бежит на территорию Османской империи, где вскоре умирает. Кстати после перехода Мазепы на сторону шведов в своих шифрованных письмах Петр изображал его специальным знаком в виде топора и виселицы. Интересно отметить, что другого своего врага – Кондратия Булавина Петр обозначал просто виселицей.

Шифры применялись и царевичем Алексеем, сыном Петра, в переписке со своими сторонниками, братьями Федором и Петром Апраксиными и др. Наибольшее влияние на царевича имел его духовник Яков Игнатьевич, с ним Алексей «вел частые беседы и состоял в тайной переписке». Сын Петра был ярым противником нововведений своего отца, вокруг него сформировалась «компания» сторонников возврата к старым порядкам. Алексей общался с иностранными представителями и заявлял, что в случае занятия им престола Россия свернет все реформы и прекратит политику Петра, разумеется, такая позиция наследника престола была на руку врагам России. Петр неоднократно увещевал сына одуматься, но все было напрасно, в конце концов, Алексей был обвинен в изме-

не и 24 июня 1718 года высшее руководство России, которое по настоянию Петра было уполномочено решить судьбу Алексея, вынесло ему смертный приговор. Правда, привести его в исполнение было не суждено, 26 июня царевич умер в тюрьме Петропавловской крепости. Среди обвинений царевичу Алексею указывалось на использование «цифирной азбуки». Дьяк Воронов, передавший шифр царевичу и обучивший его правилам шифрования, был казнен. Поп Ливерий, составивший этот шифр, был расстрижен и сослан в Соловецкий монастырь [Буганов, 1989], [Костомаров, 1989].

Кстати для расследования заговора царевича Алексея в феврале 1718 г. была учреждена Тайная канцелярия (известна также под названиями Розыскная канцелярия, Тайная розыскная канцелярия), это учреждение на более чем столетие стало центром политического сыска в Российской Империи. В дальнейшем канцелярия в своей деятельности активно использовала различные методы защиты информации, в том числе и шифры [Лурье, 2006].

Следствие по делу Алексея проходило в Москве, но много сторонников Алексея находилось в Санкт-Петербурге. Петр послал гонца к губернатору северной столицы А.Д. Меншикову с указом об аресте Кикина и Афанасьева (главных сторонников опального царевича), это случилось, после того как 3 февраля 1718 г. Петр узнал, что его слуга Баклановский проведав, что царевич во время допросов назвал своих сообщников, послал гонца в Санкт-Петербург, чтобы предупредить их. Царский курьер выехал из Москвы 6 февраля и через 3 суток прибыл в Санкт-Петербург и вручил Меншикову постановление об аресте в 23.00. Гонец Баклановского прибыл раньше, но принять каких-либо мер заговорщики не успели, 6 февраля «наложены на них цепи с стульями и на ноги железо». Во избежание подобных инцидентов Петр наложил существенные ограничения на функционирование почты, вот что он писал Меншикову: «ни для каких дел партикулярных ни за какие деньги не давал почтовых лошадей» [Павленко, 1989]. Было повелено, что только две подписи в подорожных имели силу Петра и Меншикова. Во исполнение данного распоряжения

Меншиков дает указание комендантам Выборга, Шлиссельбурга, Корелы и Нарвы «чтобы пропускать курьеров только с подорожными за моею рукою и печатью, а на почтовые станы, обслуживающие путь из Петербурга в Москву, послал гонца с предписанием никому не выдавать лошадей» [Павленко, 1989]. Вся переписка, касающаяся царевича Алексея шифровалась, причем известно, что часть письма А.Д. Меншикова Петру от 29 ноября 1709 года о поездке царевича в Саксонию была зашифрована [Соболева, 2002]. В связи с этими событиями были наложены жесточайшие ограничения на сношения с внешним миром первой жены Петра Евдокии Лопухиной (матери Алексея). Она приняла монашеский постриг и находилась в монастыре в Суздале. В 1718 г. она была переведена в монастырь в Старой Ладоге, расположенный на территории столичной губернии, которой руководил Меншиков. 20 мая 1718 г. он подписал инструкцию начальнику охраны бывшей царицы капитану Маслову, в которой говорилось, что Евдокия «должна была находиться в полной изоляции: запрещались переписка и общение не только с людьми, находящимися за монастырской стеной, но и с монахинями» [Павленко, 1989].

Подведем некоторые итоги. В Петровскую эпоху в России велась активная криптографическая деятельность. Шифрование стало основным видом защиты информации, хотя продолжали использоваться и другие методы: стеганография, физическая защита, условная сигнализация и др. При этом если в предыдущие времена практически вся шифрпереписка была посвящена дипломатическим вопросам, то при Петре также стала активно шифроваться военная и внутриполитическая информация. Шифрованная связь становится основным средством управления центральным государственным аппаратом и местными органами власти, армией и флотом.

Для организации связи были созданы ряд учреждений (кабинет его императорского величества, посольская канцелярия, коллегия иностранных дел и др.), со строгим распределением задач между ними. Деятельность данных учреждений была регламентирована законодательно. Широко практиковались организационно-административные методы защиты

информации, такие как особый подбор кадров, для осуществления криптографической деятельности и строгий контроль за их работой, организация пропускного режима в помещения, где производилось шифрование и расшифрование или хранились шифры, обеспечение охраны гонцов и курьеров и др. Из новшеств в области связи отметим, что для обеспечения управления флотом и прибрежными районами страны в качестве средства связи стали широко использоваться суда.

Именно в Петровскую эпоху свои первые шаги сделал российский криптоанализ, стали развиваться методы тайного перехвата информации, осуществлялась агентурная добыча криптографических секретов противника. В это время пришло понимание важности такого источника информации, как шифрованная переписка иностранных государств. Полученная информация могла быть весьма полезна российскому руководству, дипломатам, военным. Велся перехват сообщений и внутри России, совершенствовались методы перлюстрации, осуществлялась цензура, вводились ограничения на почтовое сообщения и здесь российские власти столкнулись с шифрами (дело царевича Алексея). Таким образом, можно отметить появление в России негосударственной криптографии.

В целом отметим, что Петр Великий был первым из российских правителей, кто предельно ясно осознал важность криптографической деятельности для обеспечения безопасности государства. Во время его правления впервые в истории отечественной криптографии к осуществлению криптографической деятельности привлеклось все высшее руководство России, включая царя.

Список рекомендуемой литературы

1. Буганов В.И. Пётр Великий и его время. – М.: Наука, 1989.
2. Бутырский Л.С., Гольев Ю.И., Ларин Д.А., Никонов Н.В., Шанкин Г.П. Криптографическая деятельность в Швеции. От викингов до Хагелина // Защита информации. INSIDE. – 2007. – №3. – с. 88-96.

3. Бутырский Л.С., Гольев Ю.И., Ларин Д.А., Никонов Н.В., Шанкин Г.П. Криптографическая деятельность в Швеции в первой половине XX века // Защита информации. INSIDE. – 2007. – №4. – с. 88-96.
4. Бутырский Л.С., Гольев Ю.И., Ларин Д.А., Никонов Н.В., Шанкин Г.П. Криптографическая деятельность в Швеции. Послевоенный период. // Защита информации. INSIDE. 2007. – №5. – с. 82–90.
5. Бутырский Л.С., Гольев Ю.И., Ларин Д.А., Никонов Н.В., Шанкин Г.П. Криптографическая деятельность в Швеции. От прошлого века к настоящему. // Защита информации. INSIDE. – 2007. – №6. – с. 76–85.
6. Вигилев А. История отечественной почты. – М., 1977.
7. Гладыш М. Псы войны // Независимое военное обозрение. – 2005. – №19. – с.8.
8. Голиков И.И. Деяния Петра Великого, мудрого преобразователя России, собранные из достоверных источников и расположенные по годам. – М., 1789.
9. Князьков С. Очерки из истории Петра Великого и его времени. Издательское объединение «Культура», 1990. Репринтное воспроизведение издания. – СПб.: Изданіе книжнаго магазина П.В. Луковникова, 1914.
10. Козлов В.П. Первые российские архивисты дипломатических бумаг // Российская дипломатия: История и современность. Материалы Научно-практической конференции, посвященной 450-летию создания Посольского приказа. – М.: РОССПЭН, 2001, с. 37-41.
11. Костомаров И.И. Царевич Алексей Петрович. – М., 1989.
12. Лурье Ф.М. Политический сыск в России 1649–1917. – М.-СПб., Центрполиграф, МиМ-Дельта, 2006.
13. Матвеев В.М. О трехсотлетии визита Петра I и Великого посольства в Англию // Российская дипломатия: История и современность. Материалы Научно-практической конференции, посвященной 450-летию создания Посольского приказа. – М.: РОССПЭН, 2001, – с. 90–92.
14. Материалы для истории Гангутской операции. Вып. I, Ч. I. Пг., – 1914.

15. Молчанов Н.Н. Дипломатия Петра Первого. – М., «Международные отношения», 1984.
16. Очерки истории внешней разведки. Том 1, под ред. Е.М. Примакова. – М.: Международные отношения, 1999.
17. Павленко Н.И. Александр Данилович Меншиков. – М.: Наука, 1989.
18. Письма и бумаги императора Петра Великого. Т. 1–12. – СПб., 1887–1912. – М.; Л., 1946–1977.
19. Подъяпольская Е.П., Шифрованная переписка России в первой четверти XVIII века. Проблемы источниковедения. – М., 1959.
20. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа. – М.: КРОН-ПРЕСС, 1999.
21. Пушкин А.С. Полтава // Полное собрание сочинений десяти томах. Т. 3. – М., 1956–1962.
22. Сборник Русского исторического общества. Т. XI. – СПб., 1873.
23. Трифанов М.А. Фельдъегерская связь России. Исторические очерки. – М.: АО «Панас-Аэро», 1994.
24. Тромонин К.Я. Достопамятности Москвы. Тетрадь 1. – М., 1843.
25. Турилова С.Л. Государственная коллегия иностранных дел (от Петра I к Екатерине II) // Российская дипломатия: история и современность. Материалы Научно-практической конференции, посвященной 450-летию создания Посольского приказа. – М.: РОССПЭН, 2001, с. 155-168.
26. Широкорад А.Б. Полтавская виктория породила великую державу – Россию // Независимое военное обозрение. – 2009. – №23. – с.14-15.
27. Юль Юст Записки. – М., 1899.
28. Kahn D. The codebreakers. – N-V: Macmillan Publ. Co., 1967.

Глава 3.

«Черные кабинеты» России

3.1. Рождение российского криптоанализа

270-летию создания отечественной дешифровальной службы посвящается

В начале 1742 г. в России была создана служба, в задачи которой входила организация перехвата и перлюстрации секретной шифрпереписки иностранных корреспондентов, организованы её дешифрование, перевод, докладывание сообщений в высшие инстанции. По аналогии с аналогичными европейскими службами, отечественная получила название «черный кабинет». Именно тогда началась регулярная работа по криптоанализу иностранных шифрованных сообщений, так что этот год можно с полным правом считать временем создания дешифровальной службы России.

Прежде чем перейти к рассказу о первых шагах отечественного криптоанализа, немного истории. XVII, XVIII и первая половина XIX вв. вошли в историю криптографии как эра «чёрных кабинетов» – специальных государственных органов по перехвату и дешифрованию переписки. В штат «чёрных кабинетов» входили криптографы-дешифровальщики, агенты по перехвату почты, специалисты по вскрытию пакетов, писцы-копировальщики, переводчики, граверы, специализировавшиеся на подделке печатей, химики, их наличие было необходимо из-за активного использования стеганографических методов защиты информации, так называемых невидимых чернил, специалисты по имитации почерков и так далее. Таким образом, чёрные кабинеты состояли из высококвалифицированных специалистов в различных областях деятельности. Первый «светский» «чёрный кабинет» (без криптоана-

литической составляющей) был организован по приказу императора Священной Римской империи Максимилиана I в первом десятилетии XVI века, это была одна из первых в Европе служб перлюстрации почтовой корреспонденции, которую можно считать прародительницей всех европейских «черных кабинетов» [Черняк, 1991]. Что касается Ватикана то подобные службы, работавшие на папский престол, в составе которых были и дешифровальщики, появились ещё ранее [Бабаш, 2002], [Kahn, 1967].

Во все времена дешифровальщики тесно сотрудничали со специалистами по перехвату и перлюстрации (тайное и безуликовое ознакомление с содержанием переписки), без перехвата нет дешифрования. До изобретения во второй половине XIX века электрических способов передачи информации (телеграф, телефон, радио) существовало два основных способа передачи сообщений – почта и специальные курьеры. Первый способ был дешевле и быстрее, но менее безопасным, «чёрные кабинеты» располагались, как правило, именно на почтамтах. Для защиты информации помимо шифрования использовались физические методы, конверты тщательно опечатывались сургучными и восковыми печатями, прошивались по контуру нитками, часто вместе с письмом в конверт вкладывался некий специальный знак (например, волос) при вскрытии целостность этого знака нарушалась (тот же волос выпадал из конверта) и адресат мог понять что с письмом уже кто-то ознакомился. С курьерами было ещё сложнее – их надо было подкупить, напоить, усыпить, а иногда даже убить, чтобы добыть секретную депешу.

О возможности перехвата тайных сообщений было известно ещё в Древней Руси, в связи с этим уже тогда принимались меры по защите информации, подробнее о них можно прочитать в статьях [Ларин, 2009], [Ларин, 2010]. Практический перехват сообщений внешних и внутренних противников российской власти осуществлялся во время правления Великого князя Московского Ивана III (XV в.) и первого русского царя Ивана IV Грозного (XVI в.) [Бабаш, 2002].

Огромная работа по перехвату внешней и внутренней переписки была организована во время правления Петра I. Вся иностранная почта доставлялась в Посольский приказ для вскрытия и досмотра. Кроме шифрованных сообщений врагов интересовала Петра и информация, содержащаяся в шифрпереписке руководителей и дипломатов, союзных России, и нейтральных государств. Такая переписка велась, Петр I не запрещал иностранным представителям использовать шифры, но требовал представление ему открытых текстов шифрованных посланий (речь, естественно, идет о тех посланиях, которые удавалось перехватить). Эти представители могли хранить свою тайну от кого угодно, но не от первого Императора России. Однако не всегда иностранные представители выполняли это указание, но в этом случае Петр I не шел на осложнение дипломатических отношений. Так, например 1710 г. Петр I потребовал, чтобы посол Дании Юст Юль представил зашифрованный документ с расшифрованным текстом на обороте (речь в документе шла о полномочиях посла). Юль заявил, что такой документ выдает шифр, на что Петр I ответил, что особенной беды в том не будет, так как между царем и королем датским не должно существовать никаких тайн.

Иностранные представители свой отказ мотивировали тем, что наличие открытого текста к перехваченному шифрованному раскроет ключ. Тем самым они косвенно подтверждали, что надеются на тайные каналы передачи своих сообщений. Среди способов тайной передачи секретных сообщений была и стеганография (использование невидимых чернил).

Петр I был первым в России криптоаналитиком. Кстати в этом году исполняется 340 лет со дня рождения первого русского императора. Напомним, что криптоанализ наука о дешифровании шифров, он применяется к «чужим» шифрам для получения информации и к собственным для оценки их стойкости и, соответственно, возможности использования для защиты своих секретов, Именно этим Петр и занимался. Сохранились его резолюции относительно ряда российских шифров: «А которую вы перво прислали, и та не годна, поне-

же так, как простое письмо, честь можно» [Соболева, 2002], «Сия цифирь зело к разобранию легка» [Бабаш, 2002]. При этом важно отметить, что занимался оценкой стойкости российских шифров не кто-нибудь, а сам царь!!!

В петровскую эпоху стали проявлять в России интерес и к шифрам иностранных государств, конечно о регулярном дешифровании иностранной переписки речь пока не шла, однако заинтересованность в получении информации таким методом уже была. Русским дипломатам, разведчикам и другим представителям за границей предписывалось добывать любую информацию, касающуюся шифров, организации связи, открытых текстов (против атаки «открытый текст – шифрованный текст» подавляющее большинство шифров того времени было не устойчиво). На этих лиц и их зарубежную агентуру также возлагалась задача организации перехвата иностранных сообщений за границами России. Подробнее о криптографической деятельности в России во времена правления Петра I можно прочитать в статье [Ларин, 2009].

Определенные меры по перехвату сообщений и добыче шифров предпринимались и после смерти Петра I, приведем ряд примеров, относящихся к концу 30-х гг. XVIII в.

При добыче информации российская сторона иногда применяла самые жесткие меры. В 1738 г. главными политическими противниками России были Швеция (с севера) и Турция (с юга). Российский двор, опасаясь создания их союза, был обеспокоен слухами о переговорах между ними. Императрица Анна Иоанновна повелела принять все возможные меры для получения соответствующей информации. Командующим русскими войсками на юге был фельдмаршал Б.К. Миних. Под его началом служил полковник русской армии Х. фон Манштейн. Приведем выдержку из его воспоминаний. «Предосторожности русского министерства, принимаемые против шведских интриг, доходили до самых насильственных мер и даже до смертоубийства на большой дороге... Ходили слухи о заключении между Швецией и Портою (Турцией – *авт*.) договора. Русский посол в Стокгольме Бестужев уведомил, что в

Константинополь послан майор Цинклер с тем, чтобы доставить оттуда ратификации договора. Тотчас после получения этого известия, граф Миних послал офицеров с несколькими унтер-офицерами в Польшу». По другим данным информация о Цинклере была получена от агентуры российской разведки в Швеции. Была поставлена задача любой ценой перехватить Цинклера и забрать имеющиеся у него документы. Русским военным удалось захватить необходимые документы, при этом Цинклер был убит. Однако в бумагах Цинклера не было обнаружено почти ничего интересного и после изучения их отправили по почте в Гамбург, откуда переслали в Швецию. В Швеции убийство Цинклера вызвало бурю негодования. По этому поводу Манштейн пишет: «Российская императрица (Анна Иоанновна – *авт*.) отреклась от этого ужасного дела, торжественно объясняя, что она об этом ничего не знала... А для того, чтобы сами убийцы не проговорились, их всех арестовали и сослали в Сибирь, где они несколько лет провели в остроге. Императрица Елизавета, вступив на престол, приказала их выпустить и приписать к гарнизонным полкам далеко во внутренность России... Это верно, что императрица не знала о распоряжении, сделанном относительно Цинклера, и что большую часть происшедшего от нее скрыли, даже по учинении убийства. Всем делом распоряжались герцог Курляндский, граф Остерман и фельдмаршал Миних» [Бабаш, 2002], [Соболева, 2002].

А вот примеры добычи криптографической информации. В середине XVIII в. русский посланник в Швеции барон Корф получил доступ к секретной информации, в том числе к открытым текстам дипломатической шифрованной переписки Швеции. Однако через некоторое время, почувствовав наличие канала утечки, шведы усилили защиту переписки своего МИДа. Правительству Швеции в 1747 г. пришлось изменить систему канцелярской переписки, потому что Корф имел возможность узнавать обо всех тайных государственных делах. Шведское правительство официально жаловалось в Санкт-Петербург на вмешательство русского посла во внут-

ренние дела Швеции страны и требовало его отзыва. Из Петербурга отвечали протестами на действия антирусской партии в Швеции. [Гольев, 2008], [Очерки, 1999].

Теперь же приведем пример добычи шифров оперативным путём. В 1739 г. герцогом Мекленбург-Шверинским Карлом Леопольдом[1] в Россию был направлен с секретным поручением французский генерал-майор Дюк де Фаллари. Однако российские спецслужбы получили информацию о неблаговидных намереньях посланца немецкого герцога: «российское министерство[2] заранее предуведомлено было о неблагоприятных предложениях, Фалларию[3] вверенных, и давно знало сего постыдными поступками обезглавленного негоциатора, то и предписало по приезде его в Россию арестовать» [Соболева, 2002].

Фаллари прибыл в Ригу 15 мая 1739 г. и на третий день пребывания на российской территории был арестован и отправлен в Санкт-Петербург под конвоем майора Астраханского полка Фёдора Воейкова. Во время обыска среди прочего представителями российских спецслужб был найден шифр многоалфавитной замены (буквы латинского алфавита заменялись на двух и трёхзначные числа, в основном применялись числа из второй сотни, каждой букве соответствовали 3 шифробозначения). Благодаря этой находке были прочитаны секретные инструкции, также конфискованные у Фаллари, в которых ему предписывалось «заботиться: 1) о возобновлении союза, заключённого Карлом Леопольдом в 1716 г. с Петром

[1] Карл Леопольд был мужем дочери брата Петра I царя Ивана Алексеевича, их дочь принцесса мекленбургская Анна Леопольдовна была правительницей России в 1740-1741 гг., как мать объявленного наследником престола Ивана VI Антоновича. Свергнуты в 1741 г. в результате дворцового переворота приведшего на российский престол дочь Петра I Елизавету [Словарь, 1984], [Соболева, 2002].

[2] Так в тексте документа [АВПРИ] процитированного в книге [Соболева Т.А., 2002], очевидно речь идет либо о коллегии иностранных дел или тайной канцелярии. Министерства в России появились лишь в начале XIX века.

[3] Так в тексте документа [АВПРИ].

Великим, 2) через посредничество русского двора и лично императрицы Анны Иоанновны ходатайствовать у германского цесаря, чтобы тот «уничтожил все изданные в предостережение герцогу декреты и ввёл бы его опять во владение мекленбург-шверинских земель» и главное 3) готовить почву для супружества дочери Карла Леопольда с сыном курляндского герцога Бирона» [Соболева, 2002]. Это не соответствовало планам российского двора, на этот престол имелись другие кандидатуры.

Императрица Анна Иоановна послала Карлу Леопольду грамоту с известием об аресте Фаллари, мекленбургский герцог поспешил отмежеваться от француза и в ответном послании заявил, что ни чего общего с Фаллари не имеет и «описав коварные замыслы сего аккредитованного им дипломата, назвал его злодеем и плутом, который старался у Папы[1] обратить его в католическую веру и даже попросил императрицу, чтобы Фаллари был предан по делам его наказанию» [Соболева, 2002]. Фаллари был посажен в тюрьму, а в последствии сослан в Сибирь.

Однако, несмотря на выше приведённые примеры какой-либо системы в осуществления перехвата и перлюстрации секретной переписки и специальной службы, выполняющей эти задачи в России на тот момент не было. Лишь с занятием российского престола императрицей Елизаветой Петровной вопросам криптографической деятельности в этом направлении стало уделяться регулярное должное внимание. К чести русской дипломатии следует отнести то, что она не только сумела закрепить успехи, достигнутые при Петре I, но стала играть решающую роль в делах Западной Европы. Русское правительство могло проводить, несмотря на смену лиц на престоле, более решительную политику. Международным успехам России способствовало и наличие в ее правящих кругах выдающихся дипломатов. При этом в руководстве Российской империи осознали, что ознакомление с иностранной перепиской является крайне важным источником информации и добыча её от случая к

[1] Речь здесь идёт о Папе Римском.

случаю является не продуктивной, пришло время поставить данные действия на регулярную основу.

Как мы уже отмечали выше первым барьером на пути к иностранным секретам были физические меры защиты, как и в Европе, их преодоление стало первой задачей отечественного «чёрного кабинета».

Организация службы перлюстрации в России во многом связана с именем выдающегося государственного деятеля Алексея Петровича Бестужева-Рюмина (1693–1766). Рассмотрим его биографию подробнее. Родился А.П. Бестужев-Рюмин 22 мая 1693 г. В 1708 г. он по приказу Петра I был отправлен вместе с братом Михаилом за границу «для науки». В 1712 году А.П. Бестужев становится дворянином посольства в Берлине, но, год спустя, поступает с разрешения Петра I на службу к ганноверскому курфюрсту, впоследствии английскому королю Георгу I. В 1717 г. он возвращается на русскую службу и направляется в качестве посланника в Данию и Гамбург. В 1740 г. он был вызван в Россию фаворитом Анны Иоанновны Бироном и назначен кабинет-министром. Бестужев принял деятельное участие в борьбе за назначение Бирона регентом после смерти Анны Иоанновны. Вместе с Бироном он был арестован в ночь с 8 на 9 ноября 1740 г. и приговорен к четвертованию. Однако казнь его была заменена ссылкой. В октябре 1741 г. Бестужев вновь был возвращен в Петербург и по вступлении на престол императрицы Елизаветы Петровны осыпан милостями и назначен главным директором почт. 25 апреля вместе с отцом и братом А.П. Бестужев-Рюмин получил графское достоинство. Занимая при дворе все более значительное положение, он начинает активно проводить свою политику, направленную на союз с Англией и Австрией против Франции и Пруссии. Французские дипломаты, аккредитованные в России, приложили немало стараний к тому, чтобы свергнуть Бестужева. Особую активность в этом проявлял французский посол маркиз Шетарди [Бабаш, 2002], [Соболева, 2002]. Об этом мы подробно расскажем далее.

Итак, перлюстрация переписки иностранных дипломатов была организована в России А.П. Бестужевым-Рюминым в

начале 1742 г., то есть как раз в тот период, когда он назначается главным директором почт. По распоряжению А.П. Бестужева-Рюмина почтовые службы должны были вскрывать и копировать все письма зарубежных послов (даже к дамам), уходящие и прибывающие из-за границы. Частные письма, пересекающие границу, также, по возможности, вскрывались все, но копировались наиболее интересные. В российских архивах сохранилось большое количество документов, отражающих деятельность «чёрного кабинета» в первые годы его существования. Например, сохранились русские копии писем, датированных 1742 г.: «от голштинского в Швеции министра Пехлина к находящемуся в Санкт-Петербурге обер-маршалу голштинскому Бриммеру», «голландского в Санкт-Петербурге резидента Шварца к Генеральным штатам, к графине Фагель в Гаагу, к пансионерному советнику фон дер Гейму и пр.», «австро-венгерского в Санкт-Петербурге резидента Гогенгольца к великому канцлеру графу Ульфреду и к графу Естергазию, а также секретаря его Бослера к маркизу Вотте», «английского в Санкт-Петербурге министра Вейча к милорду Картерсту в Ганновер и к герцогу Ньюкастлскому» и другие копии писем иностранных дипломатов [Соболева, 2002]. Все эти документы сшиты в толстые книги и переведены на русский язык (переводы прилагаются). На некоторых, в том числе самых первых перехваченных документов, есть пометки «Ея Императорское Величество слушать изволила» [Соболева, 2002].

Из данной цитаты следует, что уже в 1742–1743 гг. результаты работы «черного кабинета» докладывались высшему руководству страны в лице императрицы Елизаветы Петровны. По установленному порядку канцлер[1] или вице-канцлер несколько раз в месяц делали доклады императрице о международном положении и прочих государственных делах. При докладах, обязательно присутствующий секретарь (тогда им был Иван Пуговишников), вел подробный протокол, который впоследствии переписывался набело, скреплялся и подписы-

[1] В настоящее время должности канцлера соответствует должность премьер-министра.

вался канцлером или вице-канцлером и подшивался в дело. Таким образом, было запротоколировано всё о чём государыня «изволила рассуждать» [Соболева, 2002]. Среди «рассуждений» императрицы материалы перлюстрированной (а впоследствии дешифрованной) переписки занимали немалое место, при этом на совещаниях императрица довольно часто обсуждала вопросы работы «чёрного кабинета».

Работа перлюстраторам досталась нелёгкая, выше уже были приведены примеры способов физической защиты посланий которые надо было преодолеть, поэтому следует отметить, что безуликовая перлюстрация шифрованных сообщений была непростой задачей. Фактически главой российского «чёрного кабинета» в начальный период его работы стал, назначенный Бестужевым-Рюминым санкт-петербургским почтдиректором, Фридрих Аш. В его обязанности входило вскрытие и запечатывание посланий, вот как описывает этот процесс и трудности в ходе него возникающие в одном из писем Бестужеву-Рюмину сам первый российский профессиональный перлюстратор:

«… 29-го числа прошлого месяца купно (очевидно конверт или пакет – *Примеч. авт.)* с депешею от господина Мардефельда[1], вчерась пополудни с великим респектом получил. И не применул по силе данного мне милостивейшего приказа оную депешу распечатывать, а в ней находилось три пакета, а именно первый в придворный почтовый амт (отдел – *Примеч. авт*.) от г-на барона Мардефельда самого, второй к финанц-советнику Магирусу в Кенигсберг от секретаря Варендорфа, а третий от господина Латдорфа[2] к его брату в Ангальтбернбург. Последние два письма без трудности распечатать было можно чего ради и копии с них при сем прилагаются. Тако ж де куверт (конверт – *Примеч. авт*.) в придворный почтовый амт в Берлине легко бы было распечатать,

[1] Министр (по современному посол, в те времена для руководства важными дипломатическими миссиями назначались специальные министры) прусского двора в Санкт-Петербурге.

[2] Прусский дипломат, работавший в то время в Санкт-Петербурге.

однако ж два в оном письма, то есть к королю и в кабинет, такого состояния были, что хотя всякое удобовыполненное старание прилагалось, однако ж оных для следующих причин ответить невозможно было, а именно: куверты не только по углам, но и везде тем клеем обвязанная, под кувертом крестом на письмах нитка таким образом утверждена была, что оный клей от пара кипятка, над чем письма я несколько часов держал, никак распуститься и отстать не мог. Да и тот клей, который под печатями находился (кои я хотя искусно снял), однако ж не распустился. Следовательно же я к привеликому моему соболезнованию никакой возможности не нашел оных писем распечатать без совершенного разодрания кувертов. И таки я оные пакеты запечатал и стафету в ея дорогу отправить принужден был…» [Соболева, 2002].

Как видим, несмотря на то, что Аш к тому времени уже бывший первоклассным специалистом, мог справиться отнюдь не со всеми способами физической защиты посланий, существовавших в то время, однако всё же большинство писем удачно и безуликово перлюстрировалось.

Помимо Аша в штат «черного кабинета» входили особые секретари и переводчики в обязанности которых входило копирование иностранной дипломатической переписки и её перевод на русский язык для доклада российскому руководству (главным образом Бестужеву-Рюмину) или самой императрице.

Однако эффективная работа «черного кабинета» была бы вряд ли возможна без наличия в его штате человека очень редкой и оригинальной профессии. Как мы уже отмечали выше одним из распространенных методов физической защиты было опечатывание конвертов. В XVIII в. печати на конвертах были обычно сургучными, на которых ставился оттиск личной или государственной печати отправителя. В то время на подобные печати наносилась тонкая затейливая резьба обычно фамильный или государственный герб в сочетании с дополнительными рисунками и надписями для затруднения подделки. В ходе вскрытия конверта печати нередко повреждались и требовали восстановления. Эту задачу выполнял

«печатнорезчик», который по оттиску печати делал её копию, для опечатывания вновь закрытого конверта к отправителю. Это была тонкая и кропотливая работа, требующая аккуратности и высокого мастерства. Тем не менее Аш имел образцы печатей всех послов и других сотрудников дипмиссий, которые работали тогда в России.

В 1742–1744 гг. резчиком печатей в российском «черном кабинете» работал некий Купи, француз по национальности. Аш тщательнейшим образом проверял его работу, осматривая сделанные образцы, при необходимости делал замечания и после их устранения докладывал Бестужеву-Рюмину о результатах для окончательного утверждения работы. Вот пример подобного письма Аша, датированного февралем 1744 г.: «Печатнорезчик Купи от своей болезни отчасти оправился и уже начало подделыванием некоторых штемпелей учинил, из которых и сегодня два отдал, но один назад взять принужден был, дабы усмотренные мною в нем прогрешение поправить, а другой, которой барона Нейгауза[1] есть, я за нарочитой (правильной, подходящей – *Примеч. авт.*) нахожу и оной при чем полагаю … « [Соболева, 2002]. Но Бестужев-Рюмин был строже, он писал: «Из Государственной коллегии иностранных дел санкт-петербургскому почт-директору господину Ашу.

На рапорт Ваш от 29-февраля здесь в 6-е марта полученный в резолюцию объявляется … присланная от Вас печать барона Нейгауза при сем возвратно к Вам отправляю, дабы Вам, оную имев, столь меньшим трудом в рассматриваемом без формы исправлятся могли. Рекомендуя, впрочем, резчику Купи оные печати вырезывать с лучшим прилежанием, што ныняшняя нейгаузова не весьма хорошего мастерства» [Соболева, 2002].

Обратим внимание на заглавие этого документа, как видим деятельностью «черного кабинета» руководила Коллегия иностранных дел (предшественница МИД), в данном случае Россия пошла по пути стран Европы, имевших подобные службы. Эти службы подчинялись или непосредственно вхо-

[1] В то время австрийский посол в России.

дили в штат внешнеполитических ведомств, а территориально располагались на главном почтамте в столице страны, так продолжалось до середины XIX в., а в России несколько дольше. В последствии контроль за перепиской (перлюстрация) как правило осуществлялся органами внутренних дел, а дешифровальные подразделения включались в состав военных ведомств, разведок и спецслужб, иногда непосредственно для этих целей организованных (тут можно вспомнить АНБ США, образованное 60 лет назад (4 ноября 1952 г.).

Заметим также, что деятельность по созданию шифров в нашем Отечестве с 1549 по 1917 гг. велась также большей частью во внешнеполитическом ведомстве (Посольский приказ, Коллегия иностранных дел, Министерство иностранных дел).

Однако вернемся к подделке печатей. В феврале 1745 г. Бестужев-Рюмин доложил Елизавете Петровне о работе «черного кабинета». В частности, он упомянул о работе резчика Купи. В ответ императрица сказала (приведем цитату одного из «Протоколов докладов Ея Императорского Величества Елизавете»):

«В Санкт-Петербурге. 12 февраля 1745 г. пополудни при докладе происходило:

… 20. При сих докладах Ея Императорское Величество о потребности в сделании печатей для известного открывания писем рассуждать изволила: что для лучшего содержания сего в секрете весьма надежного человека и ежели возможно было, то лучше из российских такого мастера или резчика приискать, и оного такие печати делать заставить не здесь в Санкт-Петербурге, но разве в Москве или около Петербурга, где в отдаленном месте, и к нему особливый караул приставить, а по окончании того дела все инструменты и образцы у того мастера обыскать и отобрать, чтобы ничего у него не осталось, и сверх того присягою его утвердить надобно, дабы никому о том не разглашал» [Соболева, 2002].

Как видим Елизавета стремилась содержать службу перлюстрации в особом секрете и была озабочена «засильем» там иностранных специалистов. По некоторым сведениям впоследствии печати изготавливались гравером Академии наук.

При этом справедливости ради надо отметить, что перешедшие на русскую службу иностранцы в XVIII–XIX вв. внесли значительный вклад в развитие российской криптографии о некоторых из них мы расскажем далее.

Итак, хоть и с трудом, физическую защиту иностранных корреспондентов в российском «черном кабинете» преодолевать научились. Однако как показывал почти 200-летний опыт работы отечественной криптографической службы самые интересные и важные сведения содержатся именно в зашифрованных частях писем. Хотя в самом начале работы российского «черного кабинета» шифрованные тексты даже не копировались. В сохранившихся в российских архивах переводов иностранной переписки тех времен часто можно видеть такие пометки в тексте: «Далее... страниц цифрами писано было...» [Соболева, 2002]. Затем переводчик делает пропуск и дает следующий далее текст письма. Однако российскому руководству, прежде всего в лице Бестужева-Рюмина, было понятно, что дальше так продолжаться не может. Пришло время сделать следующий шаг – начать дешифрование иностранной шифрпереписки. И вскоре Бестужеву-Рюмину удалось найти для отечественного «черного кабинета» такого специалиста. Прежде чем подробно рассказать о нем сделаем небольшое отступление.

В настоящее время благодаря работам К. Шеннона [Шеннон, 1963] и В.А. Котельникова[1] криптоанализ стал строгой математической наукой. В описываемые же времена это было ис-

[1] Владимир Александрович Котельников (1908–2005) знаменитый русский ученый, академик АН СССР, дважды Герой Социалистического Труда, лауреат многочисленных премий. В.А. Котельников опубликовал фундаментальные труды в области радиотехники, теории помехоустойчивой связи, радиолокации, радиоастрономии. Впервые в мире сформулировал и доказал фундаментальную теорему дискретизации, на которой основана вся цифровая обработка сигналов. Под его руководством в 1930 гг. были созданы первые отечественные аппараты для шифрования речевого сигнала. Эта работа продолжалась и в годы Великой отечественной войны Подробнее об этом можно прочитать в стае [Бабиевский, 2010]. Параллельно с К. Шенноном В.А. Котельников математически формализовал требования к стойкости шифров.

кусство ну или в крайнем случае редкое ремесло – удел талантливых одиночек. Однако уже с древних времен криптография вообще и криптоанализ в частности, вызывали большой интерес у математиков. Здесь же заметим, что наиболее известными математиками-криптоаналитиками были француз Франсуа Виет и англичанин Джон Валлис. Сейчас неизвестно знал ли об этом Бестужев-Рюмин, но интуитивно он правильно определил профессию первого российского дешифровальщика – им стал тогда уже известный математик Христиан Гольдбах (1690–1764). Рассмотрим его биографию подробнее.

Родился Х. Гольдбах в Кенигсберге. История его приезда в Россию напрямую связана с организации Петром I в России Академии наук. Как известно Петр Великий (1672–1725) вошел в историю России как великий реформатор. Главным итогом петровских реформ стало преодоление серьезного отставания России от европейских держав в военной, экономической, политической областях. Петр I коренным образом изменил структуру государственного управления и исполнительной власти русского государства, создал боеспособные армию и флот, сумевшие в ходе Северной войны одержать победу над Швецией, имевшей одну из лучших армий в Европе. Во время правления Петра произошел существенный прорыв в экономике России, было создано множество предприятий, мануфактуры, оружейные заводы, металлургические и горнодобывающие предприятия, верфи для строительства кораблей и др. Серьезный импульс получило развитие торговли, в том числе и международной. Огромное значение Петр придавал повышению образовательного уровня населения России. По его инициативе открывались учебные заведения сотни молодых людей отправились учиться за границу, с другой стороны в Россию было приглашены для работы и преподавательской деятельности многие иностранные специалисты. Уже в первые годы своего царствования Петр ощутил огромную потребность России в большом числе образованных людей, способных осуществлять его планы, руководить вновь создаваемыми учреждениями, работать в промышленности и служить

в преобразованной армии. Эта потребность вызвала к жизни «цифирные» (математические), а также специальные технические и военные школы. Петр также понимал, что для основательного развития его начинаний России нужна своя развитая наука, нужны ученые. Это понимание привело к созданию в России Академии наук [Соболева, 2002].

Кстати следует отметить, что в 1712 г. Петр встречался с великим немецким математиком Лейбницем, чтобы уговорить его разработать проекты развития образования и государственного устройства в России. Интересовался Лейбниц и криптографией, так курфюрст Ганновера, через этого великого математика попытался выведать методы, которые упомянутый выше английский дешифровальщик Валлис использовал при криптоанализе французских шифров, а также попросил обучить криптоанализу нескольких молодых людей из числа своих подданных. К сожалению, для курфюрста Валлис заявил, что в случае необходимости он рад будет оказывать ему услуги, но делиться своими знаниями без разрешения короля Англии не может. Лейбниц придавал в своих проектах развитию шифрования и криптоанализа большое значение. Если бы не смерть Лейбница то первый немецкий математик-криптограф мог бы появиться в России ещё раньше чем Гольдбах. [Бабаш, 2002].

24 января 1724 г. последовал императорский указ об организации Академии наук, а при ней университета и гимназии. Через немецкого философа и математика Вольфа, с которым Петр длительное время вел переписку относительно развития науки, в Россию был приглашен ряд ученых из Европы. Среди них были и математики, подбор которых оказался поразительно удачным. Приехали Герман, ученик Якова Бернулли, два сына знаменитого Иоганна Бернулли – Николай и Даниил и, наконец, наш герой Христиан Гольдбах. В 1727 г. по приглашению Гольдбаха в Россию прибыл один из самых замечательных математиков всех времен Леонард Эйлер. По приезде в Россию Х. Гольдбах в течение 15 лет (1726–1740) исполнял обязанности конференц-секретаря Академии наук.

Как математик, Гольдбах известен классическими трудами по теории чисел и математическому анализу. В первых томах «Комментариев Петербургской Академии наук» – первом научном российском журнале – Гольдбах напечатал ряд статей об интегрировании дифференциального уравнения Риккати, о превращении расходящихся рядов в сходящиеся и др. Как известно, с 1729 г. и до конца своих дней Гольдбах работал в тесном контакте с Леонардом Эйлером и вел с ним регулярную переписку. В одном из писем (1742 г.) Гольдбах высказал Эйлеру гипотезу, вошедшую в историю под названием «проблемы Гольдбаха», которая сводится к тому, что всякое число, большее или равное шести, может быть представлено в виде суммы трех простых чисел [Бабаш, 2002], [Соболева, 2002].

Итак, А.П. Бестужев-Рюмин решил привлечь к дешифровальной работе в Коллегии иностранных дел математика, специалиста по теории чисел Х. Гольдбаха, кстати одним из аргументов в при выборе его кандидатуры может быть то, что при дворе Гольдбах исполнял обязанности одного из воспитателей Петра II, а к воспитанию коронованных особ всегда привлекались наиболее доверенные люди. Дешифровальная деятельность разумеется не могла быть поручена кому попало.

И вот 18 марта 1742 г. императрица Елизавета Петровна подписала именной указ о назначении Гольдбаха на «особливую должность», а дело об этом в архивах российского внешнеполитического ведомства озаглавлено «Об определении в Коллегию иностранных дел бывшего при Академии наук профессора юстиц-рата Христиана Гольдбаха статским советником с жалованьем 1500 руб. (очень крупная по тем временам сумма – *Примеч. авт.*), о выдаче недоданного ему в Академии наук жалованья и о выдаче ему вперед жалованья» [Соболева, 2002]. С этого времени вся дальнейшая жизнь Гольдбаха была связана с дешифровальной службой и именно эту дату следует считать началом отчёта регулярной работы по дешифрованию иностранной переписке в России.

Однако успех пришёл к первому российскому профессиональному дешифровальщику далеко не сразу, последовало

более года напряжённой работы прежде чем на полях копии одного из писем австрийского посла барона Нейгауза (о проблемах с подделкой печати которого было сказано выше) из тех, что датированы июлем 1743 г., появилась пометка: «Разобраны с цифр (имеется ввиду шифр, возможно шифртекст этого письма представлял собой набор цифр – *Примеч. авт.*) искусством статского советника Гольдбаха; в цифрах имевшиеся места внесены, для знака линиями подчеркнуты и прочее малое число еще не разобранных цифров каждая тремя пунктами означены» [Соболева, 2002].

Из этого документа следует, что в представляемых вице-канцлеру Бестужеву-Рюмину переводах перлюстрированных писем те места, которые дешифрованы, подчеркнуты, чтобы было ясно, какую именно информацию зашифровали. Далее как говорится дело пошло 30 июля 1743 г. Гольдбах представил Бестужеву-Рюмину пять дешифрованных писем, 2 августа – также пять, 10 августа – два, 20-го – снова пять, 27-го и 30 августа – по два письма. Всего с июля по декабрь 1743 г. им было дешифровано 61 письмо «министров прусского и французского дворов» [Соболева, 2002]. Как видим, Гольдбах работал и против своих соотечественников, отдавая без остатка свой талант служению России.

Результаты работы по криптоанализу иностранных шифров сразу привлекли внимание императрицы. Елизавета Петровна уделяла вопросам криптографической деятельности большое внимание. Как указывалось выше, с самого начала работы по перлюстрации корреспонденции иностранных дипломатов канцлер и вице-канцлер докладывали ее содержание Елизавете, как только появился новый источник информации – дешифрованные фрагменты иностранной переписки Елизавета сразу обратила на это внимание. Заслуги Гольдбаха были высочайше оценены, в том числе и материально. В начале январе 1744 г. с Гольдбахом был перезаключен договор о службе в России, из протокола докладов Елизавете от 3 января 1744 г. следует: «...18. Слушать же и всемилостивейше апробовать соизволила проект заключаемого статским

советником Гольдбахом о вступлении его в российскую службу контракта. И при том по всеподданнейшему докладу, не соизволено ль будет ему, Гольдбаху, за прилежные его труды и особливое искусство в разбирании цифирных секретных писем вознаграждение до 1000 рублей пожаловать, Ея Императорское Величество на сие всемилостивейше соизволила» [Соболева, 2002].

Одним из важнейших результатов работы Х. Гольдбаха стало дешифрование переписки французского посланника в России маркиза Шетарди, хотя это не был первый (а точнее четвёртый) взломанный в России иностранный шифр, ознакомление российского руководства с этой перепиской имело далеко идущие дипломатические последствия.

Однако обо всем попорядку. Одним из первых документов где упоминается о дешифровании переписки Шетарди была записка следующего содержания:

«Переводы корреспонденции маркиза Шетарди с французскими министрами при иностранных дворах и ответы к нему.

Сие почти все в цифрах писано было, но которые статский советник Гольдбах особливым искусством и неусыпным трудом, кроме некоторого малого числа, соизволил разобрать и ключ сочинить, как о том следующей пиесы (сообщения – *Примеч. авт.*) перевод с его письма гласит… Итако сие уже четвертая цифирь, которую помянутый статский советник разобрал, а именно сперва нейгаузову, потом далионову[1] с французскими министрами при иностранных дворах, да его же с статским секретарем Амелотом и сие, шетардиеву. По неже он уповает в кратком времени употребляемую и статским секретарем Амелотом и придворную цифирь маркиза Шетардия разобрать...».

На полях же рядом с этим текстом написано:

«Сии пиесы поданы Ея Императорскому Величеству самим государственным вице-канцлером в 3 апреля 1744 года» [Соболева, 2002].

[1] Далион – французский министр, участвовавший в политических интригах в России в описываемый период времени.

Посол Франции маркиз Шетарди определенно знал, что русские вскрывают его корреспонденцию. Однако текст его писем был зашифрован, и Шетарди чувствовал себя в полной безопасности, так как был уверен, что русские недостаточно образованны, чтобы вскрыть его шифр. Неизвестно, насколько он был прав в отношении русских, но для трех немцев, работавших в русском «черном кабинете», это был отнюдь не крепкий орешек. Шетарди допустил ошибку, когда в письме домой неуважительно отозвался о русской императрице, написав, что она «полностью находится во власти своих прихотей» и является «довольно фривольной и распутной женщиной». Это письмо попало в руки канцлера императорского двора графа Алексея Бестужева-Рюмина, который только и ждал случая, чтобы отомстить Шетарди, который сплел вокруг Бестужева сеть интриг в связи с англофильскими настроениями графа. Письмо было показано Елизавете, которая, будучи ослепленной своими симпатиями к Франции, отказалась ему поверить до тех пор, пока оно не было дешифровано в ее присутствии. На следующий день. 17 июня 1744 г., когда Шетарди прибыл в свою резиденцию, ему была вручена нота, в соответствии с которой в течение 24 часов французский посол должен был покинуть пределы России. Шетарди заявил протест. Тогда русские начали зачитывать ему его же собственные письма. «Достаточно», – сказал он и отправился упаковывать вещи [Кан, 2004].

Таковы были первые шаги отечественного криптоанализа. Научный подход и активное заинтересованное внимание руководителей государства к специальной службе позволили России добиться быстрых и важных успехов в дешифровании корреспонденции Франции, Англии, Германии.

3.2. О русской криптографии в период войны Наполеона против России

В 1812 г. Наполеон начал войну против России. Русские дешифровальщики сыграли значительную роль в получении информации о его войске, что способствовало разгрому его

армии. В России достойное внимание службам перехвата и дешифрования уделял еще Петр I, были заметные успехи во времена Елизаветы и Екатерины II. Регулярное чтение французской дипломатической переписки началось с середины XVIII в. В конце XVIII – начале XIX вв. российские спецслужбы активно проводили мероприятия по добыванию шифров противника и защите своих собственных секретов. Вот несколько примеров.

В конце XVIII в. секретарь российского посольства в Париже Мешков завербовал одного из чиновников МИД Франции. Были получены шифры и ключи к ним, которыми пользовался министр иностранных дел Франции граф Монморси и французский поверенный в делах в России Жене. В результате Россия получала секретную информацию длительное время.

Большое внимание уделялось вопросам защиты собственной информации. Так, в январе 1800 г. канцлер России граф И.Остерман приказал русскому послу в Берлине вывести из действия шифр («генеральную цифирь») 1799 г., поскольку возникло подозрение в его компрометации. Этот шифр мог быть утрачен вместе с багажом одного русского генерала во время революции во Франции. Аналогичное подозрение вынудило вывести из действия шифры послов России в Мадриде и Лиссабоне. Одновременно были высланы новые шифры [Кан, 2004], [Соболева, 2002].

В том же году русская разведка продемонстрировала возможность использования контролируемых каналов связи не только для «пассивного дешифрования» но и для активного навязывания сообщений, содержащих нужную руководству страны информацию. В марте 1800 г. министр иностранных дел Панин писал из Петербурга русскому послу в Берлине: «В нашем распоряжении есть шифры, с помощью которых переписывается король Пруссии со своим поверенным в делах в России. В случае, если у Вас возникнут подозрения в вероломстве министра иностранных дел Пруссии графа Кристиана фон Хаунвитца, то ваша задача будет состоять в том, чтобы под каким-то предлогом заставить его написать сюда письмо по ин-

тересующему нас вопросу. И сразу же как только будет дешифровано его письмо или письмо его короля, я проинформирую Вас о содержании» [Кан, 2004].

Криптографической службы Российской империи накануне Отечественной войны 1812 г. была организована следующим образом. В начале XIX в. в России была произведена реорганизация органов управления страной. Манифестом императора Александра I от 8 сентября 1802 г. вместо коллегий (созданных еще Петром I) учреждались министерства. Были учреждены и новые высшие органы управления страной – Государственный совет и Комитет министров. В частности, было организовано министерство иностранных дел (МИД), руководителем которого был назначен граф А.Р. Воронцов (одновременно он был назначен государственным канцлером, т.е. премьер-министром по современному). Канцелярия МИД содержала четыре основные экспедиции и три секретные. Первая секретная – цифирная (шифровальная), вторая – цифирная (дешифровальная), третья – газетная (служба перлюстрации). Позднее экспедиции стали называться отделениями. Управляющий канцелярией МИД фактически руководил криптографической службой, он «назидает вообще, ко всем экспедициям; за порядком архива и регистрацией; ему поручается хранение цифирных ключей и весь внутренний порядок канцелярии, а также сношение с директором почт, переписка с нашими министрами вне государства» [Соболева, 2002]. С 1808 года канцелярией МИД руководит А.А. Жерве. Шифровальным отделением руководит Х.И. Миллер, дешифровальное отделение возглавляет Христиан Бек. Напряженная политическая обстановка требовала составления и ввода в действие новых шифров и такая работа проводилась. Вот письмо управляющего канцелярией начальнику первого цифирного отделения от 8 марта 1812 г. [Соболева, 2002]:

«Г. Канцлеру угодно, чтобы Вы, милостливый государь мой, Христиан Иванович, немедленно занялись составлением двух совершенно полных лексиконов как для шифрования, равно как и дешифрования (в данном случае правильно применять

термин «расшифрование» – *авт.*) на российском и французском языках, и чтобы Вы снеслись по сему предмету с Александром Федоровичем Крейдеманом, стараясь соединенными силами работу сию к скорейшему и успешнейшему окончанию.

А. Жерве».

Речь в письме идет о требовании составления двух новых кодов. Этой работой занимались в отделении, кроме упомянутых в письме Х.И. Миллера и А.Ф. Крейдемана, еще ряд сотрудников. В XIX в. российская шифровальная служба использовала достижения технического прогресса. Составленные специалистами шифры не переписывались как ранее, а печатались, для чего в первом цифирном отделении имелась литография. Обычно шифры классифицировались на общие и индивидуальные. Общие шифры предназначались для нескольких корреспондентов, как правило, расположенных в одном географическом регионе. Они обеспечивали им связь между собой и с «центром». Индивидуальный шифр предназначался исключительно для связи с центром. Идея такого разделения получилась еще при Екатерине II. Несколько позже в МИД был организован цифирный комитет, в состав которого вошли наиболее опытные и квалифицированные специалисты-криптографы. В задачи комитета входили разработка, анализ стойкости и введение новых систем шифрования, контроль за правильным использованием и хранением криптографических документов; вывод из действия устаревших или скомпрометированных шифров; составление заключений, отчетов и докладных для руководителей МИД и императора по вопросам деятельности шифровальной и дешифровальной служб. Комитет подчинялся непосредственно министру, а возглавлял его «главный член цифирного комитета» [Соболева, 2002].

Большое значение руководство Российской Империи придавало организации быстрой и надежной связи. В 1781 г. управление всей внутригосударственной почтой России сосредоточилось в одном ведомстве – Санкт-Петербургском почтамте, или почтовом департаменте, подчинявшемся кол-

легии иностранных дел, а в 1802 г., причисленном к министерству внутренних дел. Передача информации осуществлялась по почтовым трактам (к концу XVIII в. их общая протяженность составляла 33 тысячи верст). При этом правительственная корреспонденция перевозилась специальными курьерами, а ведомственная и частная – почтальонами. Для повышения эффективности доставки правительственной, дипломатической и военной корреспонденции 17 декабря 1796 г. указом императора Павла I был создан фельдъегерский корпус. Корпус стал специальной воинской частью, предназначенной для несения службы связи и выполнения особых поручений императора.

Штат корпуса, в соответствии с императорским указом, состоял из 1 офицера и 13 фельдъегерей. В дальнейшем он неоднократно увеличивался. Учитывая особенности выполняемых задач (доставка наиболее важных и срочных документов, исходящих от императора, членам правительства, военачальникам и другим должностным лицам в столице и на регионах и от них – в его адрес; сопровождение при поездках по стране и за границу императора, членов императорской фамилии и их зарубежных гостей; перевозка денежных сумм и государственных ценностей и др.), Фельдъегерский корпус был укомплектован в основном за счет личного состава особой кавалерийской части придворного назначения – кавалергардов, а также унтер-офицеров гвардейских Измайловского, Преображенского и Семеновского полков. При первом комплектовании корпуса особое внимание уделялось внешнему виду и физическим данным зачисляемых на фельдъегерские должности, а впоследствии от них стали требовать также знания иностранных языков.

К началу XIX в. корпус состоял из 4 офицеров и 80 фельдъегерей. Все они подчинялись дежурному генералу главного штаба. Благодаря высокой скорости передвижения (по хорошим дорогам 400 верст в сутки) доставка документов с помощью фельдъегерской связи была наиболее быстрой и надежной. Для охраны фельдъегерей обычно назначался один солдат, а при доставке особо важных депеш и грузов – специальный конвой.

Александр I

26 января 1808 г. Фельдъегерский корпус, указом императора Александра I был переведен в подчинение военному министру. Это способствовало более четкой организации его служебной деятельности, установлению воинского порядка и укреплению дисциплины среди личного состава. Передача корпуса в Военное ведомство сыграла положительную роль в установлении единообразия требований при работе с корреспонденцией и исполнения служебных обязанностей фельдъегерями в поездках за границу. Именно фельдъегери выезжали с различными поручениями императора и правительства во многие страны не только к российским дипломатам, но и к главам иностранных государств. Фельдъегери обеспечивали доставку правительственной корреспонденции и внутри страны. Для обеспечения оперативности связи чины корпуса несли дежурство в резиденции императора – Зимнем дворце, в военном министерстве, главном штабе, министерстве иностранных дел, кабинете его императорского величества, государственном совете, сенате, комитете министров. Чтобы правительство своевременно получало информацию о положении в армии, широко практиковалось прикрепление офицеров и фельдъегерей корпуса к командующим войсками во время военных действий. Особо важные документы, адресованные в действующую армию, срочно доставляли фельдъегери, которые постоянно дежурили в главной квартире императора. Так, перед войной 1812 г. фельдъегери из Санкт-Петербурга преодолевали расстояние до Вильно за 3 суток, доставляя пакеты фельдмаршалу М.Б. Барклаю-де-Толли и от него с такой же скоростью в столицу.

27 января 1812 г. было введено в действие «Учреждение для управления большой действующей армией». Это был первый в истории отечественного военного искусства устав для

управления армиями в военное время, утверждавший схему полевого управления русской армии. Согласно этому документу фельдъегери подчинялись лично главнокомандующему, им предписывалось действовать совместно с генеральскими адъютантами в случаях передачи важнейших приказаний (о выступлении, движении или передислокации и т.п.). Чины корпуса также осуществляли связь со столицей. В сложных условиях войны фельдъегери, прикомандированные к М.И. Кутузову, доставляли исходящую от него корреспонденцию командующим армиями (П.И. Багратиону и М.Б. Барклаю-де-Толли), командирам корпусов, начальникам партизанских отрядов, губернаторам Московской, Калужской, Смоленской и других губерний, министрам и другим корреспондентам, обеспечивая тем самым связь в оперативно-стратегическом звене руководства действующей армии.

Специальные поручения, которые возлагались на офицеров и фельдъегерей корпуса в период войны и первые послевоенные годы, носили самый разносторонний характер. Так, именно русскому фельдъегерю И.В. Лицынскому было поручено сопровождать Наполеона в ссылку. После доставки бывшего императора Франции на остров Эльба был Лицынский послан с известием об этом к Александру I и к монархам ряда европейских государств.

В описываемый период времени активно велась дешифровальная работа. «Черный кабинет» России, сосредоточенный в МИД, совершенствовал методы, технику перехвата и перлюстрации сообщений иностранных государств. На почтамтах были созданы профессиональные службы по перехвату и перлюстрации дипломатической переписки, разрабатывались методы быстрого копирования, перлюстрации без улик (подделка печатей и др.), оперативного ознакомления с содержанием сообщений и передачи их дешифровальным органам.

Можно сказать, что русская криптографическая служба была готова к войне, и с ее началом появились значительные успехи. В ходе военных действий русские дешифровальщики вскрыли не только простейшие шифры для связи с небольшими подразделениями, но и Большой и Малый шифры

Денис Давыдов

Наполеона. Несмотря на то, что эти шифры являлись недостаточно стойкими, французы им полностью доверяли. Они не верили в интеллектуальные способности российских дешифровальщиков и считали, что в России даже слабые шифры будут обеспечивать тайну переписки. История показала, что они сильно ошиблись.

Российский император Александр I обильно цитировал переписку Наполеона и его генералов. В частности, в одной из своих работ американский историк Флетчер Пратт приводит выдержку из разговора, состоявшегося между Александром I и командующим одного из корпусов армии Наполеона – маршалом Макдональдом: «Конечно, – сказал император России Александр, – нам очень много помогало то, что мы всегда знали намерения вашего императора из его собственных депеш. Во время последних операций в стране были большие недовольства, и нам удалось захватить много депеш». «Я считаю очень странным, что Вы смогли их прочесть, – заметил Макдональд, – кто-нибудь, наверное, выдал вам ключ?» Александр возмутился: «Отнюдь нет! Я даю вам честное слово, что ничего подобного не имело места. Мы дешифровали их». Наши криптоаналитики могли гордиться тем, что их достижения пропагандировал сам император.

Ни в коей мере не умаляя заслуг отечественных дешифровальщиков, следует отметить, что в некоторых случаях в их руки действительно могли попадать ключевые документы. Такая возможность объясняется тем, что в тылу у французов шла широкомасштабная партизанская война. В боевых действиях в тылу противника принимали участие не только отряды вооружившегося гражданского населения, но и регулярные воинские подразделения, состоящие из гусар (здесь, безусловно, следует упомянуть легендарного партизана и знаменитого поэта Дениса Давыдова) и казаков. Эти подразделения, фактически, явились

предшественниками современного спецназа. Они нападали не только на фуражиров и небольшие отряды противника, но и совершали лихие рейды по тылам французов. Нередко они захватывали высокопоставленных офицеров и даже целые штабы и добывали таким образом ключи к французским шифрам.

М.И. Кутузов

Нельзя не отметить еще один крайне важный аспект деятельности партизан, оказавший существенную помощь российским криптоаналитикам. Именно «эскадроны гусар летучих» занимались перехватом курьеров, осуществлявших связь между подразделениями наполеоновской армии, и поставляли материал для работы дешифровальщиков.

Великий русский полководец М.И. Кутузов отдавал должное перехвату и криптоанализу сообщений противника еще до нападения Наполеона на Россию. Так, находясь вместе с русской армией, действующей за пределами России (ноябрь 1805 г.), Кутузов получил перехваченные и дешифрованные письма Наполеона и его маршала Л.Бертье к австрийскому императору Францу I. В это время Австрия, напуганная победой Наполеона под Аустерлицем, пыталась тайно войти в сговор с Францией. Если бы это случилось, то Россия лишилась бы мощного союзника и должна была пересмотреть свою стратегию в войне. Но были нужны доказательства тайного сговора. Изучив полученные письма, Кутузов сообщал Александру I: «Теперь я имею все основания считать, что существуют переговоры между Австрией и Францией» [Жилин, 1974]. Факт предательства Австрии был подтвержден.

О важности перехваченной и дешифрованной переписки французов указывает следующее сообщение М.Кутузова к командующему одной из русских армий адмиралу П. Чичаго-

ву (от 30 октября 1812 г.): «Господин адмирал! Для большей уверенности посылаю еще раз вашему превосходительству достоверные подробности, почерпнутые из переписки, вплоть до писем самого Наполеона, копии с которых я вам уже отослал. Из этих выдержек Вы увидите, господин адмирал, как в действительности ничтожны те средства, коими располагает противник в своем тылу в части продовольствия и обмундирования…» [Кутузов, 1989].

Приведем еще один пример важности перехваченной депеши противника. 5 октября 1812 г. отряд полковника М. Кудашева во время боя у Тарутино захватил предписание маршала Франции Бертье одному из французских генералов. В нем говорилось об отправлении всего тяжелого снаряжения французской армии на Можайскую дорогу. Это позволило Кутузову принять правильное решение. Он отказался от преследования разбитого авангарда маршала Мюрата и сосредоточил основные силы на Калужской дороге, перекрыв тем самым путь французов на юг. Французы были вынуждены отступать по Смоленской дороге, местность вокруг которой была разграблена ими ранее. Тем самым, французы были лишены продовольственного снабжения в ходе отступления.

Действие российских конных отрядов в тылу французов очень беспокоили Наполеона. Французский генерал А. Коленкур, постоянно находившийся рядом с Наполеоном, вспоминал: «Император был очень озабочен и начинал, без сомнения, сознавать затруднительность положения, тогда как до сих пор он старался скрыть это даже от себя. Ни потери, понесенные в бою, ни состояние кавалерии и ничего вообще не беспокоило его в такой мере, как появление казаков в нашем тылу» [Кудрявцев, 2002].

Сам Наполеон неоднократно высказывал сожаление о том, что ему не удается создать разведывательную сеть в тылу русской армии. Конные французские отряды в тылу у русских были бы мгновенно выявлены и уничтожены. Поэтому нужно было вербовать русских на службу Наполеона, что было связано с большими трудностями. Приведем один из примеров неудач-

ной вербовки. В период пребывания Наполеона в Москве был захвачен купец Жданов, не успевший выехать из Москвы. Под угрозой смертной казни ему предложили проникнуть в расположение Русской армии и собрать нужные французам сведения. За выполнение задания Жданову было обещано большое вознаграждение, он «согласился». Прибыв в расположение русских войск Жданов обратился к генералу М. Милорадовичу и передал ему список вопросов на которые французы хотели бы получить ответы. Этот список содержал существенную военно-тактическую информацию, и Кутузов, узнав об этом, наградил Жданова медалью. Таких примеров было немало.

Эффективность криптографических усилий наполеоновской Франции против России оценивается так. Использовавшиеся в военных сетях связи российские шифры по сложности их дешифрования были аналогичны французским, однако российское руководство уделяло гораздо большее внимание правильному их использованию. Значительные усилия были направлены на развитие службы перехвата и дешифрования. Полученные из дешифрованных сообщений сведения своевременно передавались командованию армии и высшему политическому руководству, включая царя. Наполеон же находился на захваченной территории и не имел возможности «партизанского» перехвата сообщений российских военачальников. Вообще, как отмечает Д. Кан, французский полководец определенно не придавал большого значения криптографии. Он целиком полагался на мощь своей «непобедимой» армии и не имел дешифровальной службы в войсках. Она казалась ему бесполезной. Поэтому сведения об эффективном дешифровании французами российских военных депеш в истории отсутствуют. Таким образом, можно утверждать, что российская криптография победила в борьбе с французской.

В заключении отметим, что в середине XIX в. под давлением общественности были официально запрещены «чёрные кабинеты» в ведущих странах Европы. Бурные политические события середины XIX в. привели к ограничению абсолютной власти европейских монархов и их полицейских ведомств. Провозглашенные принципы свободы и равенства были несо-

вместимы с цензурой переписки. Подглядывание и подслушивание якобы противоречили нравственным нормам поведения государств в отношении друг с другом. И эти «кабинеты» везде были закрыты. В июне 1844 г. волна протестов со стороны общественности по поводу перлюстрации писем вынудила английское правительство прекратить перехват дипломатической переписки. В Австрии двери венского «черного кабинета» закрылись в 1848 г. А во Франции «черный кабинет», который уже со времен Великой французской революции дышал на ладан, в этот год также прекратил свое существование. Но это была только видимость. Очень скоро руководители государств поняли, что отказ от информационно-криптографической поддержки наносит серьёзный ущерб в плане принятия и реализации эффективных государственных решений. «Чёрные кабинеты» ушли в «подполье» и получили ещё большее распространение. Хотя они действовали неофициально, но очень скоро получили полную, хотя и секретную моральную и материальную поддержку со стороны государства.

3.3. Криптографическая деятельность в период наполеоновских войн

Следует отметить, что нередко криптография оказывала серьезное влияние на ход войн, революций, внешнюю и внутреннюю политику, проводимую различными государствами. Напомним, что под криптографической деятельностью понимается не только шифрование и дешифрование, но и физическая защита собственных линий связи и перехват шифрованной информации противника. Дешифрование без перехвата невозможно. Разумеется, сюда входят меры по добыванию информации, облегчающей дешифрование (добывание ключей, описания шифрсистем и др.).

В данном подразделе рассмотрены наиболее яркие для Европы события начала XIX в. – наполеоновские войны. Отдельные эпизоды истории, иллюстрирующие удачные способы защиты и нападения, объединены в работе в хронологиче-

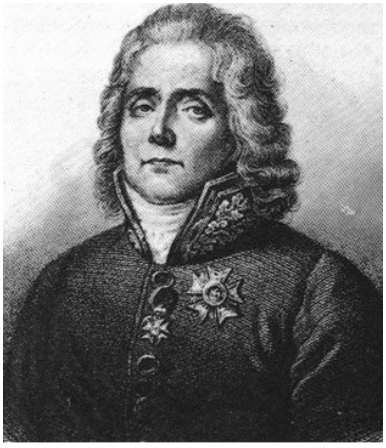
скую последовательность. В целях удобства и целостности изложения допускаются некоторые отступления от хронологии.

Все приводимые факты основаны на информации, опубликованной в открытой печати.

Наполеон Бонапарт

Напомним, что Наполеон Бонапарт родился в 1769 г. на острове Корсика. Начал службу во французской армии в 1785 г. в чине младшего лейтенанта артиллерии. Наполеон проявил себя в качестве талантливого полководца во время Французской революции (получил чин бригадного генерала) и Директории (стал командующим армией). В ноябре 1799 г. совершил государственный переворот и стал первым консулом, фактически сосредоточив в своих руках всю полноту власти. В 1804 г. провозгласил себя Императором Франции Наполеоном I. В период своего правления практически непрерывно вел войны. К 1812 г. территория империи, включала в себя большую часть Западной и Восточной Европы, а также ряд территорий в Азии и Северной Африке. Летом 1812 г. Наполеон начал войну против России, которая закончилась для него тяжелым поражением. В 1814 г. войска антифранцузской коалиции вступили в Париж. Наполеон отрекся от престола и был сослан на остров Эльба. В марте 1815 г. вновь занял французский престол. Период возвращения Наполеона к власти получил название «сто дней». После поражения в битве при Ватерлоо он вновь отрекся от престола и был сослан на остов Святой Елены, где и умер в 1821 г. По числу участвовавших в боевых действиях стран и количеству задействованных войск наполеоновские войны являются одним из крупнейших конфликтов в Европе до начала XX в.

Наполеон I существенно реорганизовал французскую разведку. Агенты Наполеона появились во всех европейских дворах. Значительно укрепился «черный кабинет» Франции. В 1811 г.



Шарль-Морис Талейран

Наполеон создал филиалы «черного кабинета» по всей своей огромной империи: в Турции и Генуе, Флоренции и Риме, Амстердаме и Гамбурге. Эти кабинеты работали весьма эффективно. Перлюстрация дипломатической переписки приняла огромные размеры. Эта деятельность находилась под контролем министра иностранных дел Талейрана. Не обходилось здесь и без курьёзов. Так, один из иностранных послов пожаловался министру: «Черный кабинет» Франции перлюстрирует мою корреспонденцию». Тайлеран скромно ответил: «Господин посол! Я уверен только в одном: ваши депеши вскрывает кто-то, интересующийся тем, что содержится внутри пакетов». Другими словами, прямых улик против «черного кабинета» нет. Отметим, что в основном речь здесь идет лишь о перехвате и перлюстрации сообщений. Успехи в дешифровании были гораздо скромнее.

Примером успехов криптографической службы Франции может служить следующий эпизод. 26 сентября 1812 г. американский посланник в Париже в письме президенту США Мэдисону тщательно зашифровал имена двух французских чиновников, которые поддерживали претензии США к Наполеону и особо просили, чтобы этот факт оставался в секрете, но французская дешифровальная служба прочитала послание и выяснилось, что это были Камбасере и Талейран.

Талейран долгое время находился на высоких должностях в правительстве Наполеона (вплоть до министра иностранных дел). В 1808 г. Талейран при личной встрече предложил себя в качестве платного информатора русскому императору Александру I. Им двигали меркантильные соображения и обида на Наполеона. Отношения между Императором Франции и его министром иностранных дел были далеки от идеала. Нередко

при большом скоплении людей Наполеон называл Талейрана вором, мерзавцем и другими оскорбительными словами, а иногда обещал и вовсе повесить. После недолгих раздумий о том, не является ли предложение Талейрана провокацией, российский император принял предложение о сотрудничестве и стал весьма щедро оплачивать поставляемую информацию. Так Талейран стал платным агентом русской разведки. Предоставляемая им информация была весьма важной для российского двора. Он сообщал сведения о состоянии французской армии, внешнеполитических инициативах Франции, внутриполитической обстановке. Одним из важнейших сообщений Талейрана была дата вторжения Наполеона в Россию. Поскольку Талейран имел прямое отношение к деятельности французского «черного кабинета», то вполне возможно, что он продавал и криптографические секреты Франции. Александр I очень ценил этот источник информации и тщательно оберегал его от разоблачения. Талейран проходил под несколькими псевдонимами: «Мой кузен Анри», «Анна Ивановна», «Красавец Леандр», «наш книготорговец», «юрисконсульт». Все сообщения, передаваемые от Талейрана российским послом в Париже К.В. Нессельроде, тщательно зашифровывались. При этом Талейран сам нередко высказывал весьма конструктивные предложения по организации конспирации и обеспечению секретности переписки.

Интересно отметить, что Талейран предложил подобные услуги и Австрии. Его предложение было принято, о чем из агентурных источников узнал Александр I. Это привело к постепенному сворачиванию контактов с Талейраном, который к тому же стал требовать за свои услуги огромные суммы. Таким образом, Талейран одновременно укреплял безопасность Франции, фактически руководя криптографической службой, и наносил ей ощутимый вред. Моральный облик Талейрана очень хорошо характеризует его фраза: «Главное качество денег – это их количество».

Несмотря на некоторые успехи в дешифровании чужих шифров, защита собственной информации, особенно в действующей французской армии, осуществлялась с помощью

весьма простых шифров. Наполеон и его генералы использовали шифры Россиньоля, книжные шифры, шифры простой замены, в том числе и типа «масонский ключ», который был переименован в «алфавит Наполеона».

Во время походов у Императора было две системы шифров. «Большой шифр» Наполеон использовал для связи со своими командующими. Эта система была подобна «великому шифру» Россиньоля, однако представляла собой код на 200 величин вместо 600, предложенных Россиньолем. Это делалось для простоты шифрования и расшифрования в полевых условиях. «Малый шифр» был предназначен для связи с небольшими воинскими подразделениями.

Но даже эти не очень стойкие шифры использовались с серьезными ошибками. Ключи не менялись длительное время, в шифртекстах сохранялось разбиение на слова (в соответствии с открытым текстом), использовались стандартные обращения и подписи, значительная часть сообщения не шифровалась (она считалась несекретной) и др. Все это, безусловно, облегчало дешифрование. Кроме того, в экстренных случаях секретные сообщения вообще не шифровались и в открытом виде попадали к противнику.

Следует отметить, что криптография во Франции отнюдь не находилась в застое. В начале XIX века была издана Французская Энциклопедия. В ней были описаны все известные к тому времени исторические шифры и способы их дешифрования. Это способствовало широкому распространению криптографических знаний в Европе. Энциклопедия сыграла роль учебника по криптографии для широкого круга заинтересованных лиц в различных странах (в том числе и в России). Особенно это относится к революционным подпольным организациям, которые не имели доступа к секретам государственных криптографических служб. Как уже отмечалось в работе [Бабаш А.В., 2004–3], опыт революционного подполья в России показывает, что революционеры использовали исторически сложившиеся шифры, модернизируя и усиливая их. Оригинальных идей практически не появлялось.

Генерал Джордж Сковелл

При Наполеоне не были изобретены новые специальные шифры. Французская армия пользовалась известными к тому времени способами шифрования. Поэтому противники Наполеона достигли весьма серьезных успехов в дешифровании его переписки.

Одним из первых добился успехов Джордж Сковелл (George Scovell). Он был шефом шифровальщиков при командующем английской армией герцоге Веллингтоне. Во время войны с французами в Испании (1808–1814) он развил систему сбора развединформации, с помощью которой осуществлялся перехват почты и фронтовых донесений французов и производилось дешифрование.

В 1808 г. внимание Наполеона привлекла Португалия и Испания. Его войска заняли Лиссабон и Мадрид. Наполеон посадил своего брата Жозефа на испанский трон. Не смирившиеся с поражением португальцы и испанцы стали вести партизанскую войну против оккупантов. Они попросили помощи у англичан. Первые подразделения британцев высадились в Португалии летом 1808 г. Следующие 6 лет португальцы и испанцы сражались против врага вместе с англичанами.

В этой войне отличилась команда дешифровальщиков и агентов по сбору развединформации, работу которой контролировал Дж. Сковелл. По мнению англичан, она сыграла огромную роль в победах британцев при Опорто (1809), Саламанке (1812) и Витториа (1813). Сковелл служил офицером Разведывательного отдела Управления генерал-квартирмейстера. Талантливый лингвист, он отвечал за группы испанских, португальских, итальянских, швейцарских и ирландских солдат и дезертиров из французской армии. Эти люди хорошо знали местные и французский языки, географию театра военных

действий. Сковелл называл эти отряды «армией проводников». Эта армия и начала развивать систему перехвата и дешифровки кодов, которыми пользовались французы.

До 1811 г. французы для передачи сообщений использовали простые шифры, получившие известность как *petits chiffres*. Они были рукописными и расшифровывались в спешке на боле боя. Как правило, это были короткие сообщения, инструкции или приказы, зашифрованные кодом на основе 50 величин. Английские дешифровальщики под руководством Сковелла довольно легко справлялись с этими кодами. Весной 1811 г. французы стали использовать более сложный код, известный как код португальской армии, который состоял из комбинаций 150 чисел. Сковелл взломал этот код за 2 дня. В 1811 г. Джордж Сковелл получил книгу «Криптография, или искусство расшифровки», написанную Дэвидом Арнольдом Конрадусом. В книге излагались правила и принципы создания и взламывания кодов и шифров. Она также описывала особенности английских, немецких, датских, латинских, французских и итальянских шифров. Эксперименты Сковелла с различными методами шифрования и кодирования информации основывались на принципах, изложенных в этой книге. Он придумал принцип, гарантирующий, что общий для Британии шифр, защищавший донесения, не будет взломан. По этой системе, обозначение 56С2 направляет получателя к странице 56 некоторой книги, колонке С, второму слову снизу. Это был хоть и очень простой, но довольно надежный код. Вопрос был в том, чтобы узнать, в какой именно книге надо искать нужную страницу. Фактически, это был один из вариантов книжного шифра.

В конце 1811 г. новые таблицы кодов были разосланы из Парижа всем ведущим французским военным. Они были основаны на дипломатическом коде середины XVIII в., и в них использовалось 1400 кодвеличин. Такие таблицы отправлялись вместе с инструкциями по их использованию, призванными устранить некоторые недостатки в использовании шифров, описанные ранее. Например, в конце сообщения рекомендовалось приписывать цифры, лишенные всякого смысла. Это было сделано для того, чтобы затруднить работу де-

шифровальщика, так как была высока вероятность наличия в конце сообщения стандартных фраз, которыми обычно заканчивается корреспонденция (например, звание и фамилия лица отправившего документ). Знание отрытого и шифрованного текста, разумеется, облегчает дешифрование.

В течение следующего года Сковелл изучал перехваченные документы французов. Он добился успеха, работая с сообщениями, которые содержали незакодированные слова и фразы (как уже упоминалось, для ускорения процесса шифрования/расшифрования французы часто шифровали не все сообщение, а только «наиболее секретные» его части). В таких сообщениях значение зашифрованных кусков текста становилось ясным из контекста. Информация о передвижениях войск, собранная «армией проводников» Сковелла помогала идентифицировать конкретных людей и определять населенные пункты, упоминаемые в зашифрованных письмах.

В 1812 г. в руках Сковелла оказалось перехваченное письмо Жозефа, адресованное его брату – Наполеону Бонапарту. Сковеллу удалось расшифровать большую часть закодированной информации, касающейся плана военной операции. Это позволило Веллингтону подготовиться к битве, от исхода которой зависело, будут ли французы контролировать Испанию (битва при Виттория 21 июня 1813 г.). Той ночью британские отряды захватили экипаж Жозефа Бонапарта и завладели копией великого французского шифра. В результате этот код был раскрыт окончательно.

В 1812 г. Наполеон начал войну против России. Русские дешифровальщики сыграли значительную роль в разгроме его армии. В России достойное внимание службам перехвата и дешифрования уделял еще Петр I, были заметные успехи во времена Елизаветы и Екатерины II. В конце XVIII – начале XIX вв. российские спецслужбы активно проводили мероприятия по добыванию шифров противника и защите своих собственных секретов. Вот несколько примеров.

В конце XVIII в. Российское посольство в Париже через своего секретаря Мешкова завербовало одного из чиновников МИД Франции. Были получены шифры и ключи к ним, кото-

рыми пользовался министр иностранных дел Франции граф Монморси и французский поверенный в делах в России Жене. В результате Россия получала секретную информацию длительное время.

В январе 1800 г. канцлер России граф И. Остерман приказал русскому послу в Берлине вывести из действия шифр («генеральную цифирь») 1799 г., поскольку возникло подозрение в его компроментации. Этот шифр мог быть утрачен вместе с багажом одного русского генерала во время революции во Франции. Аналогичное подозрение вынудило вывести из действия шифры послов России в Мадриде и Лиссабоне. Одновременно были высланы новые шифры.

В том же году русская разведка продемонстрировала возможность использования контролируемых каналов связи не только для «пассивного дешифрования» но и для активного навязывания сообщений, содержащих нужную руководству страны информацию. В марте 1800 г. министр иностранных дел Панин писал из Петербурга русскому послу в Берлине: «В нашем распоряжении есть шифры, с помощью которых переписывается король Пруссии со своим поверенным в делах в России. В случае, если у Вас возникнут подозрения в вероломстве министра иностранных дел Пруссии графа Кристиана фон Хаугвитца, то ваша задача будет состоять в том, чтобы под каким-то предлогом заставить его написать сюда письмо по интересующему нас вопросу. И сразу же как только будет дешифровано его письмо или письмо его короля, я проинформирую Вас о содержании».

Подводя итог данного подраздела, приведем оценку деятельности российских спецслужб в период Отечественной Войны 1812 года из книги [Кутузов, 1989]: «К чести российской внешней разведки и ее руководителей нужно сказать, что на сей раз были приняты солидные упреждающие меры, позволившие своевременно добыть необходимую секретную информацию о планах и замыслах противника. Это позволило избрать правильную стратегию военных действий, закончившуюся сокрушительным поражением противника».

Список рекомендуемой литературы

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: учеб. пособие. – М.: Гелиос АРВ, 2001
2. Бабаш А.В., Шанкин Г.П. Криптография. Аспекты защиты. – М.: Солон-Р, 2002.
3. Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П. О развитии криптографии в XIX веке // Защита информации. Конфидент. – 2003. – №5. – с. 90–96.
4. Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптографические идеи XIX века // Защита информации. Конфидент. – 2004. – №1. – с. 88-95; 2004. – №2. – с. 92–96.
5. Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптографические идеи XIX века. Русская криптография // Защита информации. Конфидент. – 2004. – №3. – с. 90–96.
6. Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Шифры революционного подполья России XIX века // Защита информации. Конфидент. – 2004. – №4. – с. 82–87.
7. Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Криптография: страницы истории тайных операций. – М.: Гелиос АРВ, 2008.
8. Дамасскин И.А. Сто великих разведчиков. – М., 2002.
9. Жилин П.А. Гибель наполеоновской армии в России. – М., 1974.
10. Кан Д. Взломщики кодов. – М.: Центрполиграф, 2004.
11. Кукридж Е.Х. Тайны английской секретной службы. – М., 1959.
12. Кутузов М.И. Письма, записки. – М.,1989.
13. Ларин Д.А. О вкладе советских криптографов в Великую Победу // Проблемы отечественной истории. Сборник научных статей. Выпуск 13. – М.: Издательство РАГС, 2010. – с. 76–85.
14. Ларин Д.А. Защита информации в эпоху Наполеона // Вестник РГГУ №10/09, Научный журнал. – М.: РГГУ, 2009. – с. 10–32.

15. Ларин Д.А. Криптографическая деятельность в России при Петре Великом. // Защита информации. INSIDE, – СПб., 2009. №5, с. 76–88, №6, с. 73–86.
16. Очерки истории внешней разведки т.1 ред. Е.М. Примакова. – М.,1999.
17. Ронге М. Разведка и контрразведка. – Киев, 1993.
18. Роуан Р. Очерки секретной службы. – СПБ., 1992.
19. Соболева Т.А. Тайнопись в истории России. – М., 1994.
20. Тайные операции российских спецслужб. – М., 2000.
21. Тайные страницы истории. – М., 2000.
22. Тарле Е.В. Талейран. Из мемуаров Талейрана. – М.,1993.
23. Шеннон К. Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963.
24. Kahn D. The codebreakers. – N-Y: Macmillan Publ. Co., 1967.

Глава 4.

Русские криптографические идеи в России XIX в.

4.1. Методы криптографической защиты информации России в XIX в.

Методы криптографической защиты информации в России в XIX в., в основном, воспроизводили аналогичные методы западных стран с учетом собственного криптографического опыта XVIII века. Однако появлялись и оригинальные идеи их усложнения для усиления стойкости, а также и новые шифры. Одновременно уделялось значительное внимание вопросам перехвата и дешифрования иностранных посланий и переписки антигосударственных организаций в самой России. Этим вопросам придавалось огромное значение на высшем государственном уровне, так, например, Николай I и Александр II охотно читали выписки из перлюстрированных писем и, используя эту информацию, принимали важные решения.

В начале XIX в. в России была произведена реорганизация органов управления страной. Манифестом Александра I вместо коллегий учреждались министерства. В частности, было организовано МИД, руководителем которого был назначен граф А.Р. Воронцов. Канцелярия МИД содержала четыре основные экспедиции и три секретные. Первая секретная – цифирная (шифровальная), вторая – цифирная (дешифровальная), третья – газетная (служба перлюстрации). Позднее экспедиции стали называться отделениями.

«Черный кабинет» России, сосредоточенный в основном в МИД, совершенствовал методы, технику перехвата и перлюстрации сообщений иностранных государств. На почтамтах были созданы профессиональные службы по перехвату и перлюстрации дипломатической переписки, разрабатывались методы

Барон Шиллинг фон Канштадт

быстрого копирования, перлюстрации без улик (подделка печатей и др.), оперативного ознакомления с содержанием сообщений и передачи их дешифровальным органам. За успехи в этой работе императоры щедро награждали подчиненных, так, например, один из чиновников «черного кабинета», который изобрел новый эффективный метод подделки печатей и аппарат для вскрытия конвертов паром, высочайшим указом был награжден орденом Святого Владимира 4-й степени «за полезные и применимые в деле открытия».

Обычно шифры классифицировались на общие и индивидуальные. Общие шифры предназначались для нескольких корреспондентов, как правило, расположенных в одном географическом регионе. Они обеспечивали им связь между собой и с «центром». Индивидуальный шифр предназначался исключительно для связи с центром. Идея такого разделения возникла еще при Екатерине II.

Одной из ярких личностей, связанных с российской криптографией начала XIX в., был барон П.Л. Шиллинг фон Канштадт. Он родился в 1786 г. в городе Ревель (ныне город Таллин). Разносторонняя и одаренная личность, полковник российской армии, ученый-востоковед, член-корреспондент Российской Академии наук, друг А.С. Пушкина, К.Н. Батюшкова, А. Мицкевича, А.И. Тургенева и др., заведующий цифирной (криптографической) частью МИД – таковы наиболее яркие моменты его биографии. Ранее он уже упоминался как изобретатель электромагнитного телеграфа, он также изобрел и внедрил электрический способ подрыва минных зарядов, ввел в России литографию, положил начало изучению языка и культуры народов Дальнего Востока.

В историю криптографии Шиллинг вошел, прежде всего, как изобретатель так называемого биграммного шифра. По сути дела его шифр был комбинацией шифра перестановки с шифром многозначной замены на биграммах (двухбуквенных сочетаниях). Соответственно шифрвеличинами были не буквы, а биграммы. Шифробозначениями являлись числа, по два на каждую биграмму. Важно при этом заметить, что шифровались не две рядом стоящие в открытом тексте буквы, а пара букв, разделенных некоторым заранее оговоренным расстоянием Т друг от друга.

Открытый текст сначала переписывался в биграммы букв находящихся на расстоянии Т. Если длина открытого сообщения была не кратна Т, то она дополнялось произвольными знаками алфавита. Таким образом сообщение a_1, a_2, …, a_i, … преобразовывалась к следующему виду: a_1 a_{T+1}, a_2 a_{T+2}, …, a_i, a_{T+i}… По сути это было предварительное шифрование – перестановка букв исходного сообщения.

Табличное задание правила шифрования биграмм напоминает биграммный шифр Порта, однако вместо замысловатых знаков для замены биграмм использовались числа. При этом вводились и «пустышки». Предусматривалось шифрование отдельных знаков, дополнение открытого текста хаотическим набором знаков и др. Для реализации такого способа шифрования Шиллинг предложил механическое устройство – наборно-разборную таблицу, наклеенную на коленкор. Срок действия шифра был определен в 6 лет (позднее снижен до 3 лет). С современных позиций этот шифр нельзя признать стойким.

В XIX в. в связи с развитием внешних и внутренних связей России существенно увеличился объем шифрованной переписки. Это повлекло за собой необходимость увеличения количества вводимых в действие шифров и кодов. Поэтому во второй половине XIX в. криптографическая служба России была вновь реорганизована. Она была создана (кроме МИД) еще в двух ведомствах – военном и внутренних дел (в департаменте полиции). Сфера использования криптографии существенно расширилась. Стали прибегать к шифрованию переписки жандарме-

рия и гражданские ведомства (Министерство финансов и др.). Разрабатывались специальные агентурные шифры. Шифровались и несекретные документы (на так называемых ключах «специального назначения») в целях недопущения утечки информации к «третьим лицам» (журналистам и др.). Особые шифры разрабатывались для разведчиков и агентов.

Появилось разделение шифров по степени секретности защищаемой информации. Соответственно менялись и требования к шифрам. Шифры стали делиться и по языковому принципу: русские, французские, английские, немецкие и др. Таким образом, разработка шифров опиралась на язык, на котором велась переписка.

Потребность в шифрах постоянно возрастала. Достаточно напомнить, что только количество посольств и консульств за рубежом приближалось к 150.

Рассмотрим некоторые наиболее типичные шифры России в конце XIX века.

Шифры П.Л. Шиллинга использовались вплоть до начала XX в. В основном они были ориентированы на французский язык. В нарушение существовавших правил, эти шифры в неизменном виде использовались на протяжении около 20 лет, что естественно, не могло не сказаться на их стойкости. Предлагались усовершенствования этого шифра. Так, в частности, рекомендовалось уменьшить число букв латинского алфавита, используемых при написании секретного текста, а также знаков препинания (без потери его смысла при их пропуске или замене на оставшиеся буквы). В этом случае появлялась возможность заменять числовые шифробозначения на буквы и биграммы латинского алфавита (биграммы образовывались за счет наличия исключенных – «запретных» букв в шифрованном тексте). Аналогичным изменениям подвергался и русский биграммный шифр. Нередко в качестве его усложнения использовались дополнительно вариации шифра перестановки.

Управляющий первой секретной (цифирной) канцелярией МИД, после смерти П.Л. Шиллинга (1837 г.), барон Н.Ф. Дризен разработал шифр так называемой «биклавной системы».

Этот шифр, наряду с шифром Шиллинга, активно использовался МИД России в XIX веке. Его идея заключалась в следующем. Шифр был ориентирован на использование французского языка, то есть на латинский алфавит. Основной элемент шифра (долговременный ключ) представлял собой таблицу размером 26 × 26. Столбцы таблицы обозначались буквами латинского алфавита *A, B, C, …, Z*. В столбцах буквы алфавита располагались в порядке, определяемом ключом. Строки таблицы обозначались 23 буквами алфавита (исключались *K*, *W*, *Y*) и трех знаков препинания: точка, запятая, тире. Буквы открытого текста *K*, *W*, *Y* заменялись на двухбуквенные сочетания по следующему правилу *K=qq*, *W=vv*, *Y=ii*, знак « ; » заменялся на знак « . , » и т.д.

Вторая часть шифра были так называемые «полоски». В комплекте их было 24. На каждые сутки из комплекта в строго определенном порядке извлекалось по 8 полосок. Полоска представляла собой набор 20 букв латинского алфавита. Здесь допускалось и повторение букв.

При шифровании открытый текст разбивался на отрезки по 20 знаков. Если длина текста не была кратна 20, то он дополнялся произвольным набором знаков алфавита. Каждый отрезок шифровался по своей полоске. Если открытый текст превышал по длине 20 × 8 = 160 знаков, то процесс шифрования повторялся циклически. Шифрование осуществлялось по следующему правилу. Буквы полоски определяли столбец таблицы, а строки этой таблицы соответствовали буквам и знакам открытого текста, на пересечении которых и находился знак шифрованного текста. Расшифрование производилось очевидным образом.

Нетрудно заметить аналогию этого шифра с шифром Виженера. При этом ключ – лозунг реализовывался в виде последовательности используемых полосок, а в самой таблице шифра допускались повторения букв в строке.

Полоски обычно менялись 2 раза в год. Суточные ключи у разных корреспондентов были различными. Главная слабость шифра – сравнительно короткий период шифрующей гаммы (160 знаков).

Предпринимались меры по защите от компрометации в сети засекреченной связи (СЗС). Каждый абонент СЗС имел свои собственные ключи, известные лишь в центре связи (МИД), поэтому даже если ключи одного из абонентов СЗС оказывались в руках противника, остальные абоненты сети сохраняли секретную связь с центром.

В МИД России и других министерствах и ведомствах продолжали активно использоваться коды. Коды получили распространение в России с XVIII века и являлись основным способом шифрования весьма длительное время. Объем кодов лежал в пределах от 300 до 10 000 словарных величин.

Коды были «привязаны» к словарному языку переписки (дипломатическая, военная, торговая и др.). При этом наиболее часто употребляемым словам и фразам придавалось несколько кодобозначений, чем чаще встречалась кодвеличина, тем большее количество кодобозначений ей присваивалось. Стойкость такой системы значительно возрастала за счет «выравнивания» частотной характеристики встречаемости кодобозначений в шифртексте. Таким образом, здесь имело место применение шифра омофонной (многозначной) замены по отношению не к отдельным буквам, а к целым кодвеличинам (слова, фразы и др.). В кодах также предусматривались буквенно–слоговые единицы текста. Характерная особенность российских кодов – наличие значительного количества «пустышек», т.е. кодобозначений, не несущих никакого смысла. Коды в основном были алфавитными, в них кодвеличины (буквы, слоги, слова, словосочетания) располагаются в алфавитном порядке. Кодобозначения в основном были цифровые, от 3 до 5 десятичных цифр. Они располагались в порядке возрастания чисел. Практическое удобство такой системы шифрования заключалось в том, что при шифровании и расшифровании применялась одна и та же кодовая книга, в которой и кодвелечины, и кодобозначения располагались в естественном порядке. Однако это являлось одновременно и слабостью кодирования, поскольку позволяло противнику, узнавшему хотя бы одно кодобозначение, выдвигать правдоподобные гипотезы о следующих.

Реже применялись неалфавитные коды, а также коды многозначного кодирования. В последнем случае одной кодвеличине могли соответствовать несколько кодобозначений. Практическое неудобство этих гораздо более стойких систем заключалось в том, что для повышения оперативности работы шифровальщика были необходимы две книги (кодирования и декодирования), причем в книге декодирования кодобозначения (числа) располагались в порядке их возрастания в книге кодирования кодвеличины располагались в лексикографическом порядке, а кодобозначения были произвольными.

Иногда применялось и двойное кодирование на разных кодах. При этом первый код не был секретным и использовался для «сжатия» открытого текста (уменьшения его длины). Второй код непосредственно обеспечивал его защиту.

Довольно часто кодированные тексты дополнительно перешифровывались, Наряду с простыми шифрами (типа простой замены) использовались и достаточно сложные шифры. В качестве примера приведем шифр «Лямбда» (МИД). После кодирования текст принимал вид последовательности, состоящей из десятичных знаков, т.е. кодированный текст имел вид:

$$a_1, a_2, \ldots, a_i, \ldots, a_n,$$

где $a_i \in \{0, 1, 2, \ldots, 9\}$, $i = 1, 2, \ldots$

Для зашифрования каждой цифры a_i создавалась некоторая подстановка вида:

$$\Pi_i = \begin{pmatrix} 7 & 5 & 0 & 4 & 9 & 1 & 2 & 3 & 6 & 8 \\ 5 & 4 & 0 & 2 & 1 & 3 & 6 & 8 & 9 & 7 \end{pmatrix}$$

Если, например, $a_i = 5$, то знак шифртекста $b_i = 4$. Шифртекст представляет собой последовательность:

$$b_1, b_2, \ldots, b_i, \ldots, b_n,$$

где $b_i \in \{0, 1, 2, \ldots 9\}$, i = 1, 2, …

Отметим следующий факт. Обычно подстановки представляются в естественном виде, где верхняя строка является последовательностью натуральных чисел: 0, 1, 2, … , 9. Тогда приведенная подстановка эквивалента следующей.

$$П^*_i = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 3 & 6 & 8 & 2 & 4 & 9 & 5 & 7 & 1 \end{pmatrix}$$

Результат при шифровании остается тем же.

Начальная запись подстановки приведена здесь потому, что верхняя строка подстановки являлась ключевым элементом шифра. При зашифровании менялась не только нижняя строка, но и верхняя. Сам процесс шифрования можно представить в следующем виде: $b_i=П_i a_i$, i=1,2,…, это означает, b_i получен в результате замены a_i по подстановке $П_i$. Подчеркнем, что в общем случае эта замена не может быть представлена в виде уравнений Виари (сложение и вычитание по модулю 10 чисел a_i и знаков гаммы). Этот шифр – более стойкий.

Теперь рассмотрим способ создания подстановок $П_i$. Основу шифра представляли две секретные книги объемом более 600 страниц каждая, они являлись долговременным ключом шифра. В этих двух книгах располагались 10000 произвольно выбранных перестановок цифр от 0 до 9. Все эти перестановки нумеровались числами от 0000 до 9999. Книги использовались при формировании подстановок $П_i$.

Выбор верхней строки подстановок $П_i$ был ключом, и он определялся особым номером в книгах шифрования. Этот ключ действовал достаточно долго (от 1 до 2 месяцев). На протяжении этого срока верхняя строка подстановок $П_i$ не менялось. Корреспонденты сети связи знали указанный номер (по ключевым книгам) и меняли верхнюю строку по установленному расписанию.

Нижняя строка подстановки $П_i$ менялась с каждым тактом шифрования. Таким образом, подстановки $П_i$ и $П_{i+1}$ являлись разными.

Шифровальщик выбирал произвольно строку из одной из шифровальных книг. Она являлась нижней строкой под-

становки $П_1$. Последующие нижние строки выбирались в естественном порядке их нумерации после первой строки. Выбор первой строки являлся так называемым «разовым ключом» – ключом, изменяемым при каждом послании. Поскольку шифровальщик пользовался произвольным выбором разового ключа, то этот выбор по необходимости следовало передавать в посылаемой криптограмме. Открытая пересылка номера первой нижней строки таила в себе опасность. Поэтому этот номер зашифровывался по особому правилу. При его зашифровании он выписывался трижды (получалось 3 × 4 = 12 цифр). К ним добавлялся (для контроля на приемном конце) дважды выписанный номер последней замены (2 × 4 = 8). Таким образом, появлялось контрольная группа из 20 цифр. Эта группа была маркантом, вставляемым после перешифровки в текст криптограммы на заранее обусловленном месте.

Далее выбиралась верхняя строка подстановки, определяемая по правилу шифрования отрытого текста (из ключевой книги). Нижней строкой подстановки являлась следующая по книге строка. По этой подстановке зашифровывался маркант. После этого шифровался открытый текст.

Для удобства практического использования довольно сложного алгоритма шифрования был разработан простой механический прибор, который назвали «Скала». Основная часть прибора – это так называемая «лама», она представляет собой линейку с 10 прорезями, в которые записывается верхний ряд подстановок. Линейка, перемещаясь по страницам шифровальной книги, давала удобное представление подстановок $П_i$. Подводя итог, описанию данной шифровальной системы следует отметить, что она имеет три ключевых элемента:

1. Долговременный ключ (кодовая книга и книги шифров).
2. Средневременный ключ (выбор верхней строки подстановок $П_i$).
3. Разовый ключ – выбор нижней строки подстановки $П_1$.

Этот шифр был достаточно стоек, но он имел и серьезные недостатки:

– «громоздкость» шифра. Смена долговременного ключа была весьма трудоемка – всем корреспондентам сети необходимо было разослать по три новых книги весьма большого объема;

– большая трудоемкость операции зашифрования и расшифрования, из-за этого оперативность связи существенно снижалась.

Однако сам принцип выработки подстановок при шифровании являлся весьма прогрессивным, он активно используется и в наши дни.

Разрабатывались и другие менее сложные шифры. Например, в начале XX в. был предложен код объемом в 1000 словарных величин, кодобозначения – трехзначные десятичные числа. После кодирования осуществлялась перешифровка гаммой короткого периода по правилу Бофора – вычитание текста из гаммы по модулю 10. Период гаммы был равен 3, исходное трехзначное число – разовый ключ шифра.

Само сочетание кода и гаммы вполне оправданно, но в данном случае оно заметно ослаблялось очень коротким периодом гаммы.

Перечисленные шифры использовались министерством иностранных дел.

Примерно до середины XIX в. шифры для Военного министерства разрабатывал МИД. Затем в этом министерстве была создана «цифирная экспедиция», которая начала разрабатывать собственные шифры. Этими шифрами пользовался российский император и члены императорской фамилии, занимающие высшие военные посты.

Шифры первоначально представляли собой коды достаточно малого объема (до 1000 словарных величин). Кодобозначениями являлись трех- четырехзначные числа. Кодовые книги периодически сменялись, однако они действовали достаточно длительное время. Коды обычно использовались без перешифровки, в них вводились и пустышки, их рекомендовалось использовать по две-три в каждой строке.

Следующее усложнение заключалось в «запрятывании» начала сообщения. Это было связано с тем обстоятельством, что именно в начале сообщения использовались стандартные выражения типа: «Сообщаю Вам…», «Докладываю, что …» и др.

С этой целью цифровой шифртекст разбивался справа налево (с конца телеграммы) на группы по пять цифр, однако

в первой группе оставляли четыре цифры. Если в последней группе окажется менее пяти цифр, то эта группа дополнялась произвольными цифрами. Количество произвольно добавленных цифр (от 0 до 4) указывалось в конце начальной четырехзначной группы. Таким образом, весь текст превращался в пятизначные группы цифр, записанных справа налево и разделенных знаком «тире». Это усложнение незначительно увеличивало стойкость шифра, но заметно усложняло работу дешифровальщика (как, впрочем, и самого шифровальщика).

Предусматривалось и такое усложнение как перемена мест второй и четвертой цифр в пятизначных группах (остальные цифры оставались на своих местах). Это усложнение достаточно эффективно при применении алфавитных кодов, нарушая алфавитный порядок шифробозначений.

При этом нередко в шифрованном тексте оставлялся «клер» – незашифрованные «малоинформативные» слова и словосочетания. Это делалось для повышения оперативности зашифрования, но одновременно являлось заметной слабостью засекречивания.

Иногда для кодирования применялась не одна кодовая книга, а несколько. Например, шифр императора Николая II состоял из 13 кодов на 100 кодвеличин каждый. При шифровании использовались все 13 кодов. Номер используемого кода указывался в марканте. При зашифровании даже одного сообщения применялись различные коды. Порядок шифрования тем или иным кодом определялся ключевой книгой. Период использования кодов равнялся 5, поскольку маркант состоял из 5 цифр, определяющих эту последовательность. В последующем этот код перешифровывался. Перешифрование по принципу Виженера-Бофора проводилось с помощью закономерной гаммы шифра Виженера-Бофорта.

При зашифровании открытый текст разбивался на группы по 19 букв в каждой. В последней группе могло оказаться менее 19 букв. Группы разделялись чертой. Для шифрования произвольно выбирался один из 13 кодов, и его номер ставился в начале первой 19-буквенной группы. После

набора первой буквы к каждому последующему кодобозначению прибавлялось одно и тоже число ("ключ телеграммы»). Этот ключ определялся датой отправки телеграммы. Так, если, например, дата была «13 июня» (13 + 6 = 19), то это число (19) и прибавлялось ко всем цифрам кодобозначений по модулю 100. При переходе к шифрованию другой последовательности из 19 цифр, шифровальщик произвольно выбирал номер следующего кода и отражал его в марканте. При этом перешифрование производилось по числу меньшему на 1 исходного числа (19 – 1 = 18). Далее процесс шифрования повторялся таким же образом.

Помимо шифра Николай II пользовался и кодом. Объем кода составлял 10000 словарных величин. В нем кодобозначения были многозначными (наиболее частым кодвеличинам соответствовало наибольшее количество кодобозначений). Таким образом, в данном случае имел место шифр пропорциональной замены на уровне кодобозначений (слов, слогов, букв). Эти обозначения были цифровые, 3–4 значные.

Теперь рассмотрим шифры МВД, которые существенно отличались от шифров МИД и военного ведомства. Например, шифр жандармерии начала XX в. представлял собой набор из 30 простых замен. Букве открытого текста соответствовало двухзначное число. Номер применяемой замены проставлялся в открытом виде в начале сообщения (сама нумерация была произвольной). Адрес и подпись не шифровались. Разумеется, это был простой, но ненадежный шифр. Другой используемый шифр представлял собой кодовую книгу на 110 величин, кодобозначения – цифры и двузначные числа. Этот шифр также являлся весьма слабым. Следует отметить, что даже такие слабые шифры часто применялись для шифрования не всего документа, а его отдельных «наиболее секретных» мест, например, имени и фамилии подозреваемого, а большая часть информации оставалась открытой.

Агентурные шифры России занимали особое положение. Эти шифры отличались следующими особенностями.

1. Простота использования. Агент, даже малообразованный, должен был легко шифровать и расшифровывать.

2. «Безуликовость», т.е. вся необходимая документация (ключи, правила использования) не должны были вызывать подозрения в ходе обыска (гласного или негласного). Наилучший вариант – эти шифры должны легко запоминаться (перестановка по лозунгу и др.).

Разумеется, эти требования входили в противоречие с требованием высокой криптографической стойкости. Приведем примеры русских агентурных шифров.

Шифры простой замены типа шифра Цезаря. Такой шифр легко запомнить. Ключ (сдвиг нижней строки подстановки) обычно определялся датой зашифрования, проставленной в начале шифрованного текста. Усложнением этого шифра являлся шифр с изменяемым в процессе шифрования сдвигом (через заранее оговоренное количество знаков от 5 до 9). Но такой шифр оказался слишком сложным для некоторых агентов, тем более, что нижняя строка подстановки часто не являлась алфавитной.

Книжные шифры. В этих шифрах буква открытого текста заменялась на ее координаты на определенной странице в книге не вызывающей подозрений, которая служила ключом.

Шифры перестановки. В конце XIX в. получили широкое распространение в качестве агентурных шифров различные виды шифров перестановки: решетка (квадрат) Кардано, маршрутные перестановки, вертикальные перестановки и др.

Маршрутные шифры заключаются в выписке текста в прямоугольник и считывании букв шифрованного текста по заранее оговоренному «маршруту»: по диагоналям, вертикалям, «зигзагами» и др.

В качестве агентурных шифров чаще всего использовались шифры вертикальной перестановки. Их главное достоинство заключалось в том, что для их использования не требовалось наличие компрометирующих агента письменно оформленных ключей. Ключ (лозунг) легко запоминался, а сам алгоритм шифрования был очень прост и доступен для понимания любому агенту. Приведем небольшой упрощенный пример шифра вертикальной перестановки.

Пусть в качестве секретного ключа (лозунга) используется фраза «БОЖЕ ЦАРЯ ХРАНИ», фраза записывается слитно, и буквы нумеруются в алфавитном порядке (при этом, если буква встречается несколько раз, номера ей присваиваются последовательно):

Б	О	Ж	Е	Ц	А	Р	Я	Х	Р	А	Н	И
3	8	5	4	12	1	9	13	11	10	2	7	6

Эта числовая последовательность является так называемым номерным рядом. Пусть требуется зашифровать фразу (указание агенту из центра): СООБЩИТЕ О ПРИБЫТИИ ЛИНЕЙНЫХ КОРАБЛЕЙ. При шифровании выписывается номерной ряд, а под ним шифруемый текст:

3	**8**	**5**	**4**	**12**	**1**	**9**	**13**	**11**	**10**	**2**	**7**	**6**
С	О	О	Б	Щ	И	Т	Е	О	П	Р	И	Б
Ы	Т	И	И	Л	И	Н	Е	Й	Н	Ы	Х	К
О	Р	А	Б	Л	Е	Й						

Шифрование производится выпиской по колонкам номерного ряда. В первой колонке стоят буквы ИИЕ, во второй РЫ и др. Получим шифрованный текст:

ИИЕРЫСЫОБИБОИАБКИХОТРТНЙПНОЙЩЛЛЕЕ

Расшифрование производится следующим образом. В шифрованном сообщении содержится 33 буквы, а длина лозунга – 13, следовательно, при шифровании использовалась следующая конфигурация выписки:

1	2	3	4	5	6	7	8	9	10	11	12	13

В этой конфигурацией выписки выписывается номерной ряд:

3	8	5	4	12	1	9	13	11	10	2	7	6
					И					Р		
					И					Ы		
								Е				

Таким образом, три первые буквы шифрсообщения были получены по колонке 1 (ИИЕ), следующие – по колонке 2 (РЫ) и др. В этом порядке агент выписывает текст по колонкам, и в результате получается «читаемая» конфигурация:

3	**8**	**5**	**4**	**12**	**1**	**9**	**13**	**11**	**10**	**2**	**7**	**6**
С	О	О	Б	Щ	И	Т	Е	О	П	Р	И	Б
Ы	Т	И	И	Л	И	Н	Е	Й	Н	Ы	Х	К
О	Р	А	Б	Л	Е	Й						

Дальнейшее развитие этого способа шифрования заключалось в использовании «двойной вертикальной перестановки»: полученный «первичный» шифртекст вновь шифровался по тому же правилу, но по другому лозунгу.

В конце XIX в. в России были предприняты попытки создания аппаратов для автоматического шифрования телеграфных сообщений. Так в 1879 г. главный механик Петербургского телеграфного округа И. Деревянкин предложил оригинальный прибор по шифрованию телеграмм, который он назвал «Криптограф». Это устройство напоминало известный шифратор эпохи возрождения диск Альберти. Прибор представлял из себя два диска, один из них был подвижным. К сожалению авторам не удалось обнаружить содержательного описания этого устройства и сведений о его дальнейшей судьбе.

Что касается телефонной связи, то здесь использовался простой прием: передаваемое сообщение сначала зашифровывалось как текст, а потом побуквенно передавалось по телефону. Таким образом, телефон фактически использовался в режиме телеграфа. Заметим, что и в других странах дело обстояло подобным образом, аппаратура засекречивания телефонных переговоров в реальном масштабе времени была разработана и пущена в эксплуатацию лишь в 30-х годах XX в.

Помимо государственных организаций в России в XIX в. и начале XX в. шифрование активно использовали различные подпольные организации, оппозиционные власти, такие как «Народная воля», РСДРП, БУНД (еврейская подпольная орга-

низация), эсеры, анархисты и др. Однако это тема для отдельной статьи.

Наряду с «государственной» и «антигосударственной» криптографией к криптографическим возможностям использования «таинственной» криптографии прибегали и частные лица. Не редко это имело вид игры, в которой авторы скрывали свое имя. Не избежал этого увлечения в молодости и наш великий поэт А.С. Пушкин.

В юные годы он использовал для подписи следующие «криптографические» преобразования.

Одна из подписей: НКШП, что означало инвертированную фамилию с пропуском гласных букв: НиКШуП.

Другая подпись: 1…14…16. Здесь буквы имени заменены на номера букв в естественном русском алфавите: 1 = А, 14 = Н, 16 = П. Подпись АНП — Александр НикшуП.

Ему нравились загадочные и ложные имена в тетрадях отцовского бюро. В них автор прятался за буквами, цифрами, анаграммами. Ему казалось, что, приобретая новое имя, он сам приобретал новый вид.

Подводя итоги краткого обзора криптографической деятельности в России в XIX – начале XX века отметим следующие обстоятельства.

1. «Государственная» криптография в основном опиралась на опыт западных стран. Тем не менее, создавались оригинальные способы криптографической защиты информации. Они значительно усилили известные к тому времени шифры.

2. Наряду с «государственной» криптографией, появилась и начала активно развиваться «антигосударственная» криптография, которую использовали различные антиправительственные организации.

3. В целом, государственная криптография в России находилась на уровне, не уступающем Западным странам. Вместе с тем в организации криптографической деятельности имелись серьезные недостатки. С последствиями этого факта читатель ознакомится в следующих разделах.

4.2. Криптографическая деятельность России с историей развития средств связи

Грибоедов Александр Сергеевич

Данный раздел посвящен криптографической деятельности в России XIX в. Во второй половине XIX в. произошли революционные изменения средств передачи информации. Стали использовать телеграф, а с начала XX в. – радио. Криптографическая деятельность неразрывна с историей развития средств связи. Поэтому в этом подразделе этому вопросу уделяется большое внимание. Здесь рассматривается криптографическая деятельность государственных органов. (Криптографическая деятельность подпольных революционных организаций и дешифровальная работа против них Департамента полиции является темой отдельной главы.)

Читателю рекомендуется предварительно ознакомиться с работой [Keitth, 1992], в которой рассматриваются вопросы влияния на развитие криптографии изобретения телеграфа, телефона и радио, а также с работой [Анин, 1996], в которой приводятся описания российских шифров XIX в. и сведения об организации шифровальной службы России в этот период.

После победы над Наполеоном роль России в мире существенно возросла. Открылись многочисленные дипломатические представительства России (посольства, консульства, миссии) в различных странах Европы, Азии (Турция, Персия, Египет, Китай), Америки (США, Бразилия). Большие объемы дипломатической переписки нужно было тщательно засекречивать. При этом объемы передаваемой информации непрерывно росли.

В 1828 г. должность российского представителя в Персии занимал известный русский писатель, общественный деятель и дипломат Александр Сергеевич Грибоедов. Он использовал в своих письмах шифр, известный как «решетка Кардано». Предложенный Кардано «шифр-решетка» лежал в основе знаменитого «шифра Ришелье» (рис. 4.1), в котором шифрованный текст внешне имел вид «невинного» послания.

		L	O	V	E		Y	O	U
I		H	A	V	E		Y	O	U
M	Y		S	K	I	N		M	Y
L	O	V	E		L	A	S	T	S
F	O	R	E	V	E	R		I	N
H	Y	P	E	R	S	P	A	C	E

Рис. 4.1. **Шифр Ришелье**

Напомним, в чем заключалась эта система шифрования. Из плотного материала вырезался прямоугольник с произвольными размерами сторон, например, 7 × 10 клеток.

В прямоугольнике проделывались окна. Секретный текст вписывался в эти окна, затем решетка снималась и оставшиеся клетки заполнялись так, чтобы получалось сообщение, не вызывающее подозрений. Суровую команду на английском языке: «YOU KILL AT ONCE» с помощью решетки можно спрятать в текст любовного содержания, например такой: «I LOVE YOU. I HAVE YOU DEEP UNDER MY SKIN. MY LOVE LASTS FOREVER IN HYPERSPACE». Этот шифр являлся классическим примером объединения криптографии и стеганографии.

Грибоедов писал своей жене «невинные» послания, с которыми знакомились сотрудники МИД. Они расшифровывали сообщения и затем доставляли письма адресату. Жена Грибоедова, видимо, не догадывалась о двойном назначении этих посланий.

Уже в советское время некоторых биографов Грибоедова смутил тот факт, что в отдельных письмах из Персии нарушался характерный стиль знаменитого писателя.

При исследовании оказалось, что эти письма содержали дипломатические послания Александра Сергеевича. Раскрыли эту систему очень просто. Сложили все листочки в стопку и просветили мощной лампой. Буквы, стоявшие на местах окон решетки, давали темные пятна, так как лежали строго друг под другом. По этим пятнам легко восстанавливалась решетка, т.е. ключ.

В России шифровалась переписка и по внутриполитическим вопросам. Например, по линии азиатского комитета МИД велась конфиденциальная переписка с восточными окраинами России. Здесь затрагивались вопросы управления подвластными России «киргизскими ордами», и проблемы отношений с Бухарой и Хивой. Связь осуществлялась с помощью дипломатических курьеров и Фельдъегерского корпуса.

В XIX в. по мере укрепления российской государственности курьерская связь уже не могла полностью удовлетворить потребности управления страной и вооруженными силами. Сообщения требовалось передавать быстро, а курьерская связь была относительно медлительной. Военные конфликты приобретали все большие и большие масштабы, расширялись пространства, на которых одновременно действовали крупные массы войск. Войсками нужно было эффективно управлять. Большое время для передачи конфиденциальных сообщений приводило к несогласованности действий соединений и даже к их гибели.

Русские ученые, инженеры работали над созданием принципиально новых средств передачи информации на дальние расстояния. Это направление исследований было настолько важным, что изобретения делались, порой, независимо в России и за рубежом примерно в одно и то же время.

Еще в 1794 г. гениальный русский изобретатель И.П. Кулибин сконструировал семафорный (оптический) телеграф и разработал код к нему (рис. 4.2). Записанный в виде одной таблицы код упрощал работу по передаче сообщений. Это позволяло быстрее передавать нужную информацию.

В 1808 г. офицер русского военно-морского флота А. Бутаков разработал свою систему семафорного телеграфа. Она

успешно была применена в 1810 г. на русской эскадре, действовавшей на Средиземном море под флагом вице-адмирала Д.Н. Сенявина.

В 1824 г. между Петербургом и Шлиссельбургом была проложена опытная линия семафорной связи по проекту генерал-майора П.А. Козена. Линия проработала до 1836 г.

Первая правительственная линия оптического телеграфа между Петербургом и Кронштадтом протяженностью 30 км была оборудована французским инженером Ж. Шато в 1833 г.

Зимний дворец в 1835 г. получил прямую оптическую телеграфную связь с Царским Селом и Гатчиной. Тогда же международные события побудили русское правительство выделить средства для строительства линии оптического телеграфа от Петербурга до Варшавы. Линия протяженностью 1200 км, построенная в конце 1838 г., имела 149 промежуточных станций, через которые сигнал проходил за 15 мин. Правительственная шифрованная депеша, состоявшая из 45 сигналов, передавалась из Петербурга в Варшаву за 22 мин.

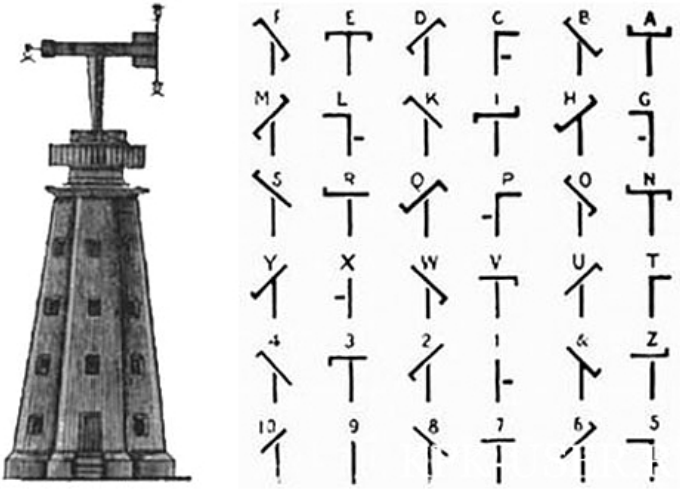


Рис. 4.2. **Оптический телеграф (1780-1880 гг.)**

Оптический телеграф просуществовал в России около полувека примерно до середины 1850-х гг. Он сыграл значительную роль в развитии внутренних коммуникаций как средство оперативного управления исполнительными органами государства в мирное и военное время.

Рис. 4.3. **Санкт-Петербург. Оптический телеграф (современный снимок)**

Однако более значительные перспективы давало использование электрического телеграфа. 21 октября 1832 г. в Петербурге состоялась публичная демонстрация электромагнитного телеграфного аппарата П.Л. Шиллинга фон Канштадта (рис. 4.4).

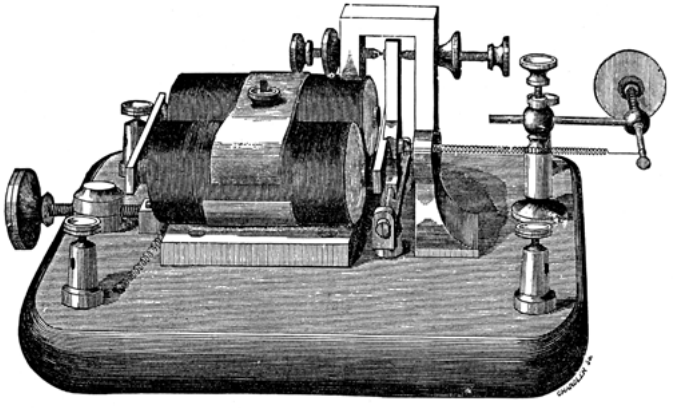


Рис. 4.4. **Электромагнитный телеграфный аппарат Шиллинга**

В 1836 г. под его руководством была проложена экспериментальная подземная кабельная телеграфная линия между крайними помещениями здания Адмиралтейства в Петербурге, которая действовала более 1 года. В том же году Шиллинг предложил подвешивать линейные провода между телеграфными станциями на деревянные опоры. В следующем году Шиллинг начал работу над проектом первой подводной телеграфной линии связи между Петергофом и Кронштадтом. Она не была завершена из-за смерти русского изобретателя 25 июля 1837 г. Работы Шиллинга как один из этапов работ по созданию и распространению проволочного телеграфа, и оказали большое влияние на развитие этой области науки и техники в других странах.

Преемником и продолжателем работ П.Л. Шиллинга по развитию и внедрению телеграфа в России стал академик Петербургской академии наук Б.С. Якоби. В 1841 г. он построил телеграфную линию между Зимним дворцом и Главным штабом в Петербурге, оборудованную оригинальными пишущими аппаратами его конструкции. В 1842 г. подобная линия была проложена от Зимнего дворца до главного управления

путей сообщения и публичных зданий в Петербурге. В следующем году была проложена новая линия до дворца в Царском Селе. Построенные Якоби телеграфные линии представляли собой зарытые в землю изолированные медные провода. В 1850 г. Якоби придумал буквопечатающий телеграфный аппарат собственной конструкции. Как говорил об этом устройстве сам ученый, в нем «регистрация знаков осуществлялась с помощью типографского шрифта».

Интенсивная работа по созданию телеграфа в России и связанные с этим теоретические и экспериментальные исследования дают право считать П.Л. Шиллинга и Б.С. Якоби основоположниками телеграфной связи в России.

Строительство и ввод в эксплуатацию первых линий связи положили начало бурному развитию сети государственного телеграфа. К концу 1855 г. протяженность телеграфных линий в России составила более 5 тыс. км. Первая большая телеграфная линия протяженностью 655 км соединила в 1852 г. Петербург и Москву.

Увеличение количества линий связи приводило к необходимости разрабатывать новые шифры и коды, удобные для закрытия секретной информации, передаваемой с помощью телеграфа.

Основными шифрами используемыми в России в XIX в. были биграммные шифры П.Л. Шиллинга и биклавные шифры барона Дризена. [Астрахан, 19996]. К усовершенствованию этих шифров и построению ключей для них привлекались специалисты шифровальной службы. Эти шифры применялись, в основном, в МИД. Также широко использовались коды. Кодовые таблицы объемом 1000–1200 словарных величин было принято называть словарными ключами и в зависимости от словаря определенного кода называть французскими, русскими, немецкими. Их применяли в Военном министерстве и МВД, в МИД и некоторых других гражданских ведомствах. Так, с помощью кодов, введенных в действие во второй половине 1860-х гг., вели секретную переписку министерство финансов, министерство путей сообщения, министерство государствен-

ных имуществ, государственный контроль, государственная таможенная служба. Ведущими специалистами по кодам того времени были начальник цифирного отделения МИД барон Дризен и сотрудник отделения М. Сухотин.

Иногда шифры употреблялись для совершенно особых миссий. Так сенатор, тайный советник Тапильский, посланный Александром II из Петербурга в Москву к митрополиту Филарету с просьбой составить царский манифест 1861 г. об освобождении крестьян, имел личный шифр для почтовых отправлений. Деликатность миссии сенатора заключалась в том, что царь считал нежелательным разглашение факта поручения духовному лицу светского дела.

Для шифрования на разных языках использовались разные ключи. Французские и немецкие ключи применялись для сношений со странами Европы, а русские – для шифрования внутренней переписки и для связи с российскими представителями в странах Востока (в частности, в Турции) и в некоторых странах Европы.

До второй половины XIX в. шифры для всех ведомств России разрабатывались в МИД. Но уже в конце 1840-х гг. в Главном штабе военного министерства была организована и начала свою работу собственная цифирная экспедиция. Создававшиеся здесь шифры утверждались военным министром. Экземплярами военных шифров снабжались военачальники, а также император и члены императорской фамилии, военный министр. Шифрованная переписка по линии Военного министерства велась не только в периоды ведения боевых действий, но и в мирное время. Зашифровывались сообщения, касавшиеся мобилизационной и военной подготовки, а также готовности армий и крепостей к боевым действиям и некоторые другие сведения. В военное время из цифирной экспедиции МИД в военное министерство поступали экземпляры тех шифров, которые действовали в сетях общей связи, куда в силу политических, военных или иных причин могли входить дипломатические представители России за границей, командующие действующими армиями, военно-морскими

силами и иные лица. Во второй половине XIX в. большинство шифров военного министерства представляли собой коды малого (до 1000 словарных величин) объема. Кодовыми обозначениями здесь являлись трех- и четырехзначные числа. Военные шифры этого типа обычно использовались в течение длительного времени, перерабатывался лишь относительно быстро устаревавший словарь, что объясняется, например, изменением географии военных действий и др. Словарные ключи были наиболее распространенным типом шифров, используемых в конце XIX в. в военном ведомстве. Их называли «военными ключами».

Следует отметить, что сроки действия ключей были очень длительными. Некоторые ключи, введенные в середине XIX в., действовали и в начале XX в. Такой длительный срок использования ключей, разумеется, снижал стойкость шифров. К тому же биклавные шифры не подходили для шифрования информации, передаваемой по телеграфу, начальник 1-й экспедиции шифровального департамента отдела МИД К. Таубе писал в начале XX в.: «Система биклавная не применима в настоящее время ввиду смешанной передачи буквами и цифрами, не допускаемой телеграфными конвенциями». Однако некоторое количество шифров биклавного типа применялось для зашифрования секретной почтовой корреспонденции и в начале XX в.

После того, как электрический телеграф начал использоваться в системе управления государством, большое влияние на его дальнейшее развитие стали оказывать требования военно-стратегического характера. Начавшаяся Крымская война (1853–1856 гг.) ускорила постройку телеграфных линий, так как нужна была оперативная связь между крупными городами. В 1854 г. была введена в эксплуатацию телеграфная линия Петербург-Варшава протяженностью более 1000 км. В мае 1855 г. закончилось строительство линии Киев–Кременьчуг–Николаев–Одесса, а в сентябре того же г. была открыта телеграфная связь на новой линии Николаев–Перекоп–Симферополь. С этого времени Петербург получил телеграфную связь с Симферополем, исполь-

зуя для данной цели ранее построенные линии Петербург–Москва и Москва–Киев.

Примером шифра, используемого во время Крымской войны, может служить русский словарный ключ №299 на 600 величин, который был введен в действие в апреле 1854 г. Предназначался он для связи командиров частей дунайской армии. После войны этот шифр продолжал использоваться. В 1891 г. им были снабжены Бухара, Кашгар, Кульджа, Сеул, Пекин, Токио, Иркутск, Омск, Ташкент, Хабаровск, Урга, Чугучак, Владивосток. Этот шифр был выведен из употребления только в 1901 г.

Расширение системы телеграфной связи обусловливалось и экономическим развитием России. В государственную телеграфную сеть включалось все большее количество городов. Телеграфные сообщения были установлены между Москвой, Орлом и Харьковом; Житомиром и Варшавой; Новочеркасском и Херсоном; Тифлисом и Владикавказом и многими другими городами. Строящиеся телеграфные станции подразделялись на правительственные и частные железнодорожные.

В 1857 г. был построен городской телеграф в Петербурге, объединивший в единую правительственную сеть важнейшие пункты государственного и военного управления. Городские телеграфы были введены в Москве в 1861 г. и в Киеве в 1881 г.

В 1871 г. была закончена постройка длиннейшей по тому времени линии правительственного телеграфа Москва–Владивосток.

Электрический телеграф приобретал все большее значение в политической и экономической жизни страны. Освоение Забайкальского края и Дальнего Востока, начавшееся в 1850-х гг., повлекло за собой строительство новых телеграфных линий, в частности, Сибирской телеграфной магистрали Казань–Владивосток протяженностью 8330 верст. Были проложены подводные телеграфные кабели, соединившие Баку с Красноводском, а также международные линии в Данию, Швецию и Японию.

К концу 1905 г. протяженность телеграфных линий в России составила 169200 верст.

Несмотря на бурное развитие телеграфной связи в России, Фельдъегерский корпус, отметивший в 1896 г. свой столетний юбилей, продолжал обеспечивать обмен наиболее важной и срочной информацией императорского дома с руководителями министерств и ведомств страны. Документальная шифрованная связь, осуществляемая Фельдъегерским корпусом, к началу XX в. оставалась важным способом организации управления и взаимодействия в высшем звене государственного руководства.

В 1860-е – 1870-е гг. военным министром России графом Д.А. Милютиным были проведены реформы, коснувшиеся всех сторон устройства армии. Появление нового средства управления войсками – телеграфа – поставило вопрос перед Генеральным штабом русской армии о необходимости регламентирования его применения и создания органов, которые бы повседневно решали вопросы боевого применения этого мощного средства управления войсками.

В 1876 г. было издано Положение о полевом управлении войск в военное время. В соответствии с Положением во главе армии стоял главнокомандующий, имевший при себе полевое управление армии, в составе которого было полевое управление военных сообщений с подчиненным ему отделом почт и телеграфов. В обязанностях заведующего отделом указывалось, что он отвечает за организацию и деятельность почт и телеграфа на военных дорогах, что означало ответственность за почтовую и телеграфную связь внутри армии и связь Главной квартиры армии с центром.

Положением предусматривалось наличие при полевом штабе армии станции правительственного телеграфа, располагавшей 4–6 телеграфными аппаратами Морзе. Предусматривалось и активное использование фельдъегерской службы.

Линейное обеспечение телеграфной правительственной связи было возложено на военно-походные телеграфные парки. Они предназначались для организации связи между штабами действующей армии и для связи отдельных частей армии как между собой, так и с государственными телеграфны-

ми линиями. В 1867 г. был сформирован первый образцовый военно-походный телеграфный парк, а осенью 1870 г. начато формирование шести таких парков. Каждый парк имел 8 телеграфных аппаратов Морзе, 35 верст телеграфного провода и необходимое количество шестов и изоляторов для подвески.

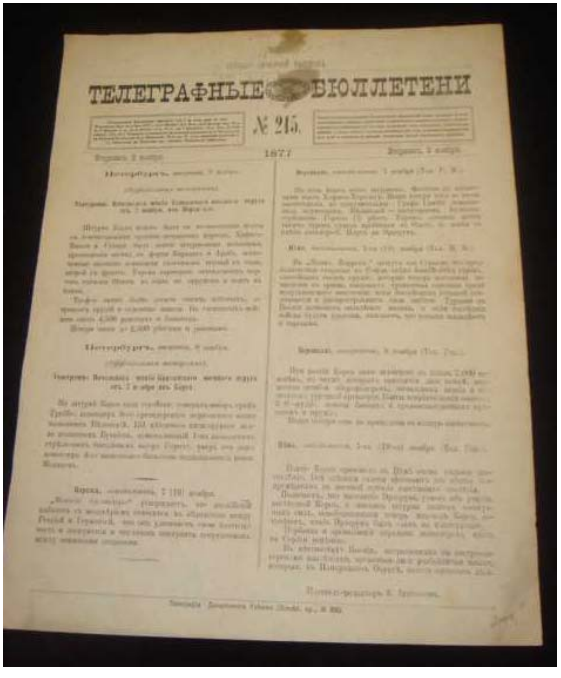
Приказом военного министра в 1870 г. было утверждено Положение о военно-телеграфных командах, которые в военное время предназначались для усиления личным составом существующих линий правительственных и частных железнодорожных телеграфов. В их функции входила постройка и эксплуатация новых военных телеграфных линий, ремонт линий, разрушенных противником при его отступлении, а также повреждение и уничтожение линий, переходящих к неприятелю.

Военно-походные телеграфные парки и военно-телеграфные команды, в отличие от подразделений правительственного телеграфа, находились в подчинении полевого инженерного управления, что значительно затрудняло координацию действий по использованию системы телеграфной связи для управления вооруженными силами в военное время.

Сложившаяся система телеграфной связи была небезуспешно применена уже в ходе русско-турецкой войны 1877–1878 гг. (рис. 4.5). Для шифрования во время этой кампании в русской армии применялись русский биграммный ключ №361, составленый в 1876 г., французский биклавный ключ №348, введенный в действие в 1870 г., и некоторые другие шифры. Шифрвеличин в русском биграммном ключе №361 было 992 – 28 букв упрощенного русского алфавита, три знака препинания, а также всевозможные биграммные сочетания этих знаков. Им отвечали трехзначные кодовые обозначения. Этот шифр был вначале разослан в консульства на Востоке, направлен в Тифлис и Одессу. Французский ключ №348 использовался на европейских линиях связи. В русско-турецкую войну оба шифра были направлены в действующую армию. Их экземпляры были у генерала Н.П. Игнатьева и генерала В.Б. Фредерикса. Использовались эти шифры и после войны: русский ключ – до 1903 г., а французский – до 1891 г.

В Турции в 1877 г. во время войны с Россией применяли четырехзначный цифровой код, составленный в Германии специально для Турции. Но опыт русско-турецкой войны, как и франко-прусской, показал недостаточную эффективность существовавших в то время военно-полевых шифровальных кодов. Они давали большое количество ошибок, были громоздкими, непрактичными и не очень стойкими.

Телеграф, широко используемый во время русско-турецкой войны, стал новым возможным источником информации о планах и замыслах противника.


ТЕЛЕГРАФНЫЕ БЮЛЛЕТЕНИ

№ 215.

1877

Рис. 4.5. **Телеграфные бюллетени русско-турецкой войны**

Для получения информации о противнике можно было перехватывать сообщения, передаваемые по телеграфным линиям связи, либо непосредственно захватывать телеграфные

станции. Известны примеры таких захватов русскими войсками. Так, много неприятностей доставлял туркам кавалерийский отряд генерала Струкова, осуществлявший стремительные рейды по турецким тылам. Отряд захватывал стратегически важные населенные пункты, мосты и телеграфные станции. На телеграфных станциях русские получали доступ к передаваемой корреспонденции и документации, в частности, к турецким кодовым книгам. Добываемая информация о противнике оперативно использовалась для действий, как самого отряда, так и других частей русской армии. При таких захватах линии связи выводили из строя, а телеграфные аппараты снимали и увозили. Иногда, правда, этого не происходило, так как действовать приходилось очень быстро. Так, один из небольших отрядов, входивший в состав отряда генерала Скобелева, развивавшего успехи генерала Струкова, напал «на телеграфную станцию Магалесси, где наткнулся на большие партии черкесов и потому не мог произвести правильной порчи железной дороги и телеграфа, а ограничился лишь тем, что прапорщик Живов, ворвавшись в телеграфную комнату, сжег находившиеся там бумаги».

В результате уничтожения турецких линий телеграфной связи оставались большие связки проволоки. Они находили применение во время оборонительных действий наших войск. Телеграфную проволоку разбрасывали перед траншеей. При внезапном наступлении противника в темную ночь шум от путавшихся в проволоке наступающих предупреждал часовых об опасности. Генерал Скобелев отмечал: «В франко-прусскую войну германские войска делали то же самое, и результаты были удовлетворительные».

Следующий важнейший этап развития электрических средств связи начался с момента изобретения телефона. Его придумал американец А.Г. Белл в 1876 г. В России интерес к телефонной связи возник сразу после того, как стало известно об изобретении. Это было новое и эффективное средство управления. Первый телефонный разговор в России состоялся в ноябре 1879 г. между Петербургом и Малой Вишерой. В 1881 г. развернулось строительство телефонных станций в Петербурге,

Москве, Варшаве, Риге, Одессе. В 1882 г. эти станции были введены в действие. Одновременно с устройством городских телефонных станций возникла необходимость в установлении междугородных телефонных связей. И в 1882–1883 гг. первые такие станции были построены, они связали Санкт-Петербург и Москву с близлежащими городами.

Телефонная связь стала широко применяться военными и морскими ведомствами. Телефонное сообщение было установлено между отдельными помещениями Главного штаба в Петербурге. С появлением телефонов военные инженеры русской армии, оценив важность этого изобретения для военной связи, сочли возможным испытать телефон в полевых условиях. Выполнением этой задачи занялся сын Б.С. Якоби подполковник В.Б. Якоби. Первые испытания телефонов в армии, давшие положительные результаты, были произведены летом 1878 г. в Выборге между островами Транзундского пролива на расстоянии 6–12 км по телеграфному кабелю и между Выборгом и Уран-Саарской правительственной станцией по линии военного телеграфа на расстоянии 30 км.

Работая над совершенствованием телефона, В.Б. Якоби в июне 1881 г. изготовил миниатюрный телефон, названный «Телекаль», который являлся первым образцом военно-полевого телефонного аппарата. Трудность использования телефона заключалась в необходимости иметь для телефонной связи отдельные от телеграфа провода. Разработкой принципа одновременного телеграфирования и телефонирования по одним и тем же проводам занялись военный инженер Г.Г. Игнатьев и русский изобретатель Е.И. Гвоздев. Практическое использование системы одновременного телефонирования и телеграфирования Е.И. Гвоздева было осуществлено впервые на линиях железных дорог, а с 1893 г. эта система стала применяться и на дальних правительственных междугородных телефонных линиях. В 1887 г. инженер К.А. Мосицкий разработал первую автоматическую телефонную станцию, а в 1895 г. русский изобретатель М.С. Бердичевский (Апостолов) совместно с М.Ф. Фрейденбергом сконструировал автоматическую телефонную станцию с шаговым искателем.

Попов
Александр Степанович

В 1896 г. в Петербурге был построен и начал выпускать продукцию телефонный завод акционерной компании «Эриксон-Гейслер», который стал производить настольные и настенные аппараты специально для государственных телефонных линий и сетей, а также полевые телефоны для русской армии. Кроме того, в армии в период с 1895 по 1896 гг. впервые появились полевые телефоны фирм «Белл» и «Сименс».

С внедрением в войска телефонной связи в штат каждой телеграфной роты было введено 24 полевых телефонных аппарата, которые предназначались для организации телефонной связи между штабами армии, корпуса и дивизии.

Последняя четверть XIX в. характеризуется бурной телефонизацией России, строительством дальних правительственных междугородных линий и городских телефонных станций, а также использованием телефонной связи в оперативном звене действующей армии.

К началу XX в. существовавшие электрические средства связи уже не в полной мере удовлетворяли потребности управления страной и вооруженными силами. Основная проблема заключалась в том, что для использования телеграфа и телефона необходимо протягивать кабель, по которому проходит сигнал. Впервые проблема передачи электрического сигнала без проводов была решена в России, где был создан беспроволочный телеграф – радио.

7 мая 1895 г. А.С. Попов выступил с публичным докладом на заседании физического отделения русского физико-химического общества, в ходе которого продемонстрировал первый в мире радиоприемник. Уже первые испытания беспроволочного телеграфа на флоте доказали превосходство

радио над другими средствами связи. Одновременно с опытами по радиосвязи на флоте подобные работы стали проводиться и в армии. Началом таких опытов нужно считать 1898 г. Именно с этого времени в них участвовал целый ряд армейских телеграфных специалистов.

После испытания в 1900 г. сконструированных А.С. Поповым переносных полевых радиостанций (рис. 4.6) на маневрах 148-го Каспийского походного полка был сделан вывод, что с помощью радио можно установить связь между высшими штабами на расстоянии 50 верст и более. Дальнейшие работы по созданию полевых радиостанций в русской армии были продолжены специалистами Офицерской электротехнической школы.

Рис. 4.6. **Радиоприемник, изобретенный А.С. Поповым**

Таким образом, беспроволочный телеграф, несмотря на свою историческую молодость, еще до начала XX в. обратил на себя внимание государственных и военных специалистов как наиболее перспективное средство связи с очень широкой предполагаемой областью применения.

Возможность быстрой передачи шифрованных сообщений на большие расстояния, а также возможность перехвата сообщений в пунктах передачи, приема и по пути следования

депеш обусловливали рост криптографических отделов и отделений с привлечением на эту службу большого количества телеграфистов, радиотехников, лингвистов, математиков.

Обратимся к дешифровальной деятельности российских спецслужб. Как и в XVIII в., в течение XIX в. велась активная перлюстрация практически всей переписки иностранных представителей в России. При необходимости осуществлялось ее дешифрование. Перлюстрировалась как дипломатическая, так и военная переписка, т.е. сообщения от иностранных военных агентов (сейчас эти представители называются военными атташе). Методы безуликового ознакомления с содержанием писем постоянно совершенствовались и были развиты настолько, что российским специалистам удавалось производить все необходимые операции за несколько минут. При этом использовалось фотографирование. Адресаты не замечали никаких следов вскрытия. Такая спешка была вызвана тем, что курьеры иностранных представительств привозили пакеты на почтамт незадолго до отхода заграничных поездов, а забирать старались сразу же после получения почты с вокзала.

Как утверждал бывший царский сотрудник «черного кабинета» (цензор) России С. Майский, «иностранная дипломатическая переписка попадала в руки российских «специалистов» практически полностью. В российском «черном кабинете» имелся полный набор безукоризненно скопированных печатей для зарубежной переписки всех находившихся в Петербурге посольств и консульств… У российского «черного кабинета» имелись копии многих шифров иностранных государств».

Успехи российского «черного кабинета» признавали даже весьма высокопоставленные деятели зарубежных государств. Так, в конце XIX в. объединитель Германии «железный канцлер» О. Бисмарк проявлял особое беспокойство о сохранности секретных посланий, отправляемых из Петербурга. Он писал: «…немецкий шифр не остается неизвестным российскому императорскому двору; ведь я знал по опыту, что даже в здании нашей миссии в Петербурге сохранить наши тайны мог не искусно сделанный замок, а только частая смена шиф-

ра. Я был уверен, что не мог телеграфировать в Ливадию ничего, что не дойдет до сведения императора». В Ливадии (Крым) в это время происходили русско-германские переговоры. Бисмарк с сожалением констатировал: «Сохранить тайну шифра в Петербурге особенно трудно».

Аналогичная мысль о русских дешифровальщиках была высказана немцами уже в конце 30-х гг. XX в. В справке главного управления полиции безопасности отмечалось: «…русские испокон веков являются мастерами шифрования и дешифрования. Уже во время Петра Первого им удавалось не только доставать шифры всех находящихся в России дипломатических представительств, но и разгадывать их».

К сожалению, информацию об успехах российских дешифровальщиков иностранцам «поставляли» и другие высокопоставленные чиновники. Так, министр иностранных дел Российской Империи Лобанов-Ростовский в разговоре с одним иностранным дипломатом упомянул о своей осведомленности о некоторых фактах, сведения о которых не могли быть получены из официальных источников. Эта информация стала известна немецкому послу. Посол тут же отправил в Берлин телеграмму, в которой были такие слова: «Использую этот шифр из осторожности, так как предыдущий употреблялся слишком часто, и у меня появились основания для недоверия. Меня предупредили о ненадежности шифра, прошу о новом шифре». Несмотря на проявленную немецким дипломатом «осторожность», эта телеграмма была дешифрована русским «черным кабинетом» и российский министр был проинформирован о крайней нежелательности разглашения сведений, полученных путем дешифрования.

Российские дипломаты имели некоторые сведения о возможностях «черных кабинетов» по перлюстрации дипломатической переписки и пускались на различные ухищрения, чтобы противодействовать этой деятельности. Так, например, посол России в Турции граф Н.П. Игнатьев (о нем упоминалось при описании примеров шифров, используемых во время русско-турецкой войны 1877–1878 гг.) знал о том, что по-

сольская переписка перехватывается. Это было видно по внешним признакам получаемых пакетов. Кроме того, по внешним признакам письма, его объему, качеству пакета (конверта), почерку, запаху, можно было судить о важности корреспонденции. «Тонкий запах», высококачественный конверт, почерк посла вызывали настороженность специальных почтовых чиновников Турции. Поэтому посол прибегнул к следующему приему. Конверт был «простейшего» качества (очень дешевый), адресацию писал его лакей (якобы отправляя письмо своему знакомому или родственнику); само письмо несколько дней выдерживали рядом с открытой бочкой, в которой находилась соленая селедка. Запах от письма появлялся специфический, свойственный людям «низшего» сословия. Этот прием себя оправдал. Послания Игнатьева по внешним признакам не перехватывались.

Будучи послом России в Англии граф Игнатьев получил письмо из Петербурга с явными следами вскрытия. На встрече с английским министром иностранных дел он указал на противоправные действия английского «черного кабинета». Поначалу министр ответил, что такого кабинета в Англии нет. Но под давлением улик признался: «А что же я, по-вашему, должен был Вам сказать? Неужели Вы думаете, что нам не интересно знать, что пишет Вам ваш министр и что Вы ему доносите про нас?..»

В конце XIX в. дешифровальная работа, в основном, была сосредоточена во второй экспедиции шифровального департамента МИД. Здесь дешифровывались копии, снятые с шифртелеграмм, перлюстрированных «черным кабинетом» главного телеграфа в Петербурге. Через главный телеграф проходила корреспонденция из других городов Российской империи (Москвы, Варшавы, Киева, Одессы и др.), где имелись иностранные дипломатические представительства. Штат этого подразделения шифровального департамента состоял из 10–12 человек. Во второй экспедиции специалистов-криптоаналитиков было всего 2–3 человек. Весь остальной штат имел лишь весьма отдаленные сведения об искусстве дешифрования.

Специального учебного заведения, где преподавалась криптография в России не было, и поэтому чиновниками в шифровальный департамент назначались лица, окончившие обычные учебные заведения (университеты или лицеи). Крупным недостатком было и то обстоятельство, что работники дешифровального отделения в основном владели лишь французским и немецким языками. Некоторые работники владели английским языком. Между тем, министерство постоянно испытывало потребность в специалистах, владеющих и другими, более редкими языками. Поэтому департамент постоянно обращался за квалифицированной языковедческой помощью к ученым, преподавателям, иным лицам, владеющим теми или иными языками. Так, для помощи в дешифровании иностранной дипломатической переписки привлекались профессор Попов, преподававший в Петербургском университете китайскую словесность, его однофамилец, также Попов, окончивший факультет восточных языков и хорошо знавший японский язык. Последний за счет министерства даже был направлен в командировку в Японию с целью совершенствования знания языка. Для переводов с венгерского или, как тогда говорили, мадьярского языка, обращались за помощью к В.И. Кривошу-Неманичу, работавшему в Генеральном штабе и знавшему 14 языков. Цензоры Комитета иностранной цензуры Смирнов и Жуковский переводили соответственно с турецкого и персидского языков.

Дешифровальщики всегда работали в тесном контакте с разведкой, одна из важнейших задач которой была выкрасть ключи к шифрам, кодовые таблицы, сфотографировать документацию. Ставилась и более трудная задача – внедрить агента в службы противника, связанные с шифрами и кодами.

Часто раскрытию шифров и кодов способствовали полученные агентурным путем открытые тексты, которые можно было привязать к соответствующим шифрованным сообщениям. Для кодов, например, это сразу давало некоторое количество раскрытых кодовых групп, после чего значительно облегчалась работа по дешифрованию. Нередко коды просто-

напросто покупались и продавались. Европейским центром подобной деятельности в то время была Вена. Там производились всевозможные сделки по покупке и продаже копий секретных документов, писем, карт, кодов, планов, чертежей и др. Упомянутый ранее С. Майский писал, что Россия покупала коды и шифры в Вене, Париже и Брюсселе. Торговцам кодами можно было даже делать «предварительные заказы». Этими методами активно пользовались разведки Германии, Австро-Венгрии и других стран. Коды, представляющие меньший интерес, греческий, болгарский или испанский, можно было легче достать. Они стоили дешевле – 1,5–2 тыс. руб. А такие коды, как германский, японский или американский, стоили десятки тысяч. Цены шифрдокументов других стран колебались между 5 и 15 тыс. В Брюсселе шифры и коды приобретались у известного авантюриста де Вернина. Его основным занятием было похищение шифров и кодов из посольств с помощью работавших там и подкупленных им лакеев, швейцаров, денщиков и др. Де Вернин делал фотографии украденных документов и продавал их. Таким образом, в шифровальном департаменте имелось большое количество иностранных кодов. В порядке взаимопомощи МИД даже делился информацией с морским и сухопутным генеральными штабами. Некоторые коды вскрывались аналитическим путем. Однажды, когда долго не удавалось купить один германский код, двум сотрудникам было дано поручение его восстановить по ежедневно получаемым многочисленным копиям шифртелеграмм. Над этим заданием больше 1 года работали 2 человек. Когда работа приближалась к концу и код был уже в значительной степени раскрыт, немцы вывели его из действия. Хотя был достигнут явный успех, воспользоваться его плодами к сожалению не удалось.

В конце XIX – начале XX вв. Россия активно использовала возможности подкупа иностранцев, имевших доступ к шифрам, кодам, шифрованной переписке. Особо важная корреспонденция иностранных дипломатов не отправлялась по поч-

те, а обычно упаковывалась в специальные портфели с секретными замками и отправлялась к месту назначения с особыми курьерами. В результате она не попадала в «черный кабинет» и не могла быть перлюстрирована. В этих случаях приходилось прибегать к подкупу. Как вспоминает Майский, не было случая, чтобы золото не открывало замок портфеля и не давало возможность всего за несколько минут сфотографировать документы. Весь вопрос был в размере суммы. Многие курьеры, фельдъегеря и служащие иностранных посольств были подкуплены. За небольшую плату они добывали практически любые документы, даже целые коды и шифровальные ключи. Для достижения этого им приходилось брать у спящего хозяина ключи от письменного стола или от несгораемого шкафа, снимать с них отпечаток из воска и заказывать дубликаты ключей или пускать ночью в посольство специалистов, которые могли бы квалифицированно добыть нужную информацию. «Поражаться надо было доверию некоторых послов к своим лакеям, которые продавали их за гроши. Однажды произошел такой случай, вместо одного посла великой державы был назначен другой, который должен был с собой привезти весь новый штат служащих, так как прежний посол старым своим слугам не доверял, но в письме к новому послу он очень ходатайствовал за одного, по его выражению, «незаменимого» человек, своего выездного лакея, т.е. именно за то лицо, которое за незначительное месячное вознаграждение доставало из посольства все, что было угодно», – писал Майский.

К сожалению, российские шифры также становились объектами кражи. Особенно крупная утрата шифров произошла в русском посольстве в Пекине 19 августа 1888 г. Несмотря на компрометацию, ключи продолжали использоваться, что совершенно недопустимо! Например, ключ №356, украденный в Пекине, был выведен из употребления лишь на некоторое время. В начале 1890-х гг. его вновь ввели в действие, но уже в Европе. В 1898 г. произошла еще одна компроме-

тация этого шифра: один экземпляр его был утрачен начальником Адриатической эскадры. Только после этого действие ключа было прекращено окончательно. В Пекине также был украден русский ключ №361. Его окончательно вывели из действия лишь в 1903 г., но и после этого барон Таубе писал: «Ключ №361 может применяться как временный в специальных случаях, кроме Дальнего Востока».

Руководителям российской криптографической службы того времени представлялось возможным использовать скомпрометированные шифры. Если шифр был скомпрометирован в одном регионе, то считалось возможным его использование в других регионах. Решающим обстоятельством здесь являлось отсутствие предполагаемых контактов между нашими потенциальными противниками из-за дальности расстояний. Другим фактором было время. Скомпрометированный шифр мог вновь вводиться в действие через значительный промежуток времени. Предполагалось, что за давностью он оказывался забыт противником. Справедливости ради надо отметить, что некоторые меры все же предпринимались. Например, в 1866 г. цифирная экспедиция МИД занималась «проверкой всех находящихся в некоторых странах шифров, а равно контролем всех книг, которые ведутся о состоянии заготовленных и разосланных экспедицией шифров». При этом оказалось, что некоторые миссии имеют у себя шифры в огромном количестве, многие из которых вовсе не употребляются. Вместе с тем проверка обнаружила, что некоторые уже закрытые миссии не возвратили находившихся у них шифров. В результате были даны необходимые распоряжения и приняты соответствующие меры к исправлению существующего положения.

Подводя итог, отметим, что развитие криптографии и связи в России в XIX в.е отвечало мировому уровню. Однако в организации шифровального дела имелись существенные недостатки, основными были длительные сроки действия ключей и использование ключей после их компрометации.

4.3. Шифры революционного подполья России XIX в.

В XIX в. и начале XX в. в России помимо государственных организаций шифрование активно использовали различные подпольные организации, оппозиционные власти, такие как «Народная воля», РСДРП, БУНД (еврейская подпольная организация), эсеры, анархисты и др. По характеру своего использования, шифры подпольщиков сходны с агентурными шифрами, поэтому к ним применяются те же требования: простота, безуликовость, легкая смена ключей по корреспондентам сети связи и др.

Необходимость применения шифров подпольными организациями вызывалась требованиями конспирации, так как правоохранительные органы Российской империи вели с подпольщиками жесткую борьбу. Наряду с шифрами широко использовалась так называемая «химия» – невидимые чернила (т.е. применялась стеганография). Нередко шифрование и стеганография использовались одновременно.

Выдающийся «диссидент» XIX в. в России А. Герцен в своей переписке использовал весьма простой прием. Буквы передаваемого текста заменялись на их числовые обозначения в старославянской азбуке. Следует напомнить, что эта замена была уже основательно забыта к этому времени. Но даже такой простой шифр был выдан российской полиции одним из помощников Герцена (В. Кельсцевым).

В эти же времена широко использовался жаргонный язык, в котором происходила подмена понятий. Так, например, слово «армяне» означало «жиды», «греки = татары», «турки = сапожники», «Грузия = Тула» и др.

Во второй половине XIX в. была создана революционная организация «Народная расправа». Она использовала шифр простой замены, а затем и так называемый «книжный» шифр. В результате обыска полиция находила книги – ключи. Расшифрованные документы были использованы при судебном разбирательстве дел революционеров.

Народническое движение в России часто использовало шифр «Гамбетта» (короткопериодическое гаммирование). Появилось даже поверье: «пи – шифр». Число π = 3,14… должны были знать все участники сети связи. Из этих трех цифр образовывалась периодическая последовательность периода 3, которая складывалась с буквами секретного послания (буквы переводились в числа в соответствии с их местом в естественном алфавите).

Применялся и такой прием, как чтение «невинного текста» (текста прикрытия) по заранее оговоренным местам появления слов секретного сообщения. Например, договоренность сторон в том, что из полученного несекретного сообщения надо читать только каждое пятое слово. Известный идеолог анархизма П. Кропоткин послал своему корреспонденту такое письмо: «Прости, что пишу второпях. Приходи ко мне вечером сег.ня. Завтра я должен …». Чтение по пятым словам дает начало секретного текста: «Приходи завтра…».

Наиболее часто использовался шифр Виженера (короткопериодическая замена по ключу – слову) с последующим использованием шифра «Гамбетта» (сложение первичного шифртекста с короткопериодической последовательностью – гаммой шифра, образуемой по другому ключу – лозунгу). Революционеры, безусловно, верили в стойкость такого шифрования.

Разумеется, квалифицированных специалистов в области криптографии у подпольных организаций не было, они пользовались шифрами, известными им по различным публикациям. Например, организация «Народная воля» применяла «шифр Полибия», который нередко называли «тюремным шифром». Этот шифр был удобен тем, что им можно было легко перестукиваться через стенки тюремных камер, в нем буквы русского алфавита последовательно вписывались в прямоугольник со сторонами 5 × 6, и буква заменялась на ее координаты в таблице. Например, буква Б стояла в первой строке на втором месте, тогда она передавалась при перестукивании следующим образом: удар – длинная пауза – два коротких удара. Еще до народовольцев таким шифром активно

пользовался декабрист М.А. Бестужев, находившийся в 1826 г. в Алексеевском равелине Петропавловской крепости. Народовольцы использовали этот опыт.

Также применялись шифры простой замены, которые были слабы сами по себе. Однако революционеры еще более ухудшали их стойкость, используя в качестве ключа легко запоминаемые фразы, из которых удалялись повторяющиеся буквы.

Активно использовались и шифры перестановки. При этом для облегчения их реализации, как правило, применялись так называемые «маршрутные шифры». Ещё в первой половине XIX в. народоволец Михайлов предложил оригинальный шифр – шифр «вертикально-горизонтальной перестановки». Покажем его суть на примере.

Пусть имеется следующий секретный ключ (шкала перестановки): 2.5.6.3.1.4.

Открытый текст, например: «РАЗВИТИЕ КРИПТОГРАФИИ ИДЕТ СВОИМ ЧЕРЕДОМ» вписывается в квадрат со сторонами 6 × 6.

	1	2	3	4	5	6
1	Р	А	З	В	И	Т
2	И	Е	К	Р	И	П
3	Т	О	Г	Р	А	Ф
4	И	И	И	Д	Е	Т
5	С	В	О	И	М	Ч
6	Е	Р	Е	Д	О	М

В соответствии с ключом производится перестановка столбцов: первый столбец встаёт на пятое место, второй – на первое и др. Получим:

	1	2	3	4	5	6
1	А	И	Т	З	Р	В
2	Е	И	П	К	И	Р
3	О	А	Ф	Г	Т	Р
4	И	Е	Т	И	И	Д
5	В	М	Ч	О	С	И
6	Р	О	М	Е	Е	Д

Затем, по этому же закону переставляются строки: первая – на пятое место, вторая – на первое и др.

	1	2	3	4	5	6
1	Е	И	П	К	И	Р
2	В	М	Ч	О	С	И
3	Р	О	М	Е	Е	Д
4	О	А	Ф	Г	Т	Р
5	А	И	Т	З	Р	В
6	И	Е	Т	И	И	Д

Шифрованный текст выписывается построчно:

ЕИПКИРВМЧОСИРОМЕЕДОАФГТРАИТЗРВИЕТИИД

В своё время такого рода шифры перестановки являлись достаточно сложными. Однако и в это время они поддавались дешифрованию.

Широко применялись и книжные шифры. Эти шифры обеспечивают достаточную стойкость, но обладают существенным недостатком. Корреспондентам сети необходимо всегда иметь с собой книгу-ключ.

Это нередко представляло неудобство, и, кроме того, при «провале» сети связи противник мог определить ключевую книгу (по наличию ее у всех корреспондентов). Поэтому часто вместо книги использовались легко запоминаемые слова или фразы, по которым воспроизводилась гипотетическая страница книги. Приведем примеры.

Шифр по слову. В этом шифре ключом является заранее оговоренное слово, словосочетание или фраза. По нему строится таблица замены. Пусть, например, это слово – «ПРЕКРАСНАЯ». Строится таблица такого вида (применительно к современному редуцированному русскому алфавиту): слово – лозунг выписывается по вертикали. Эти вертикали обозначаются числами от 1 до 0 (в слове 10 букв). Каждая буква построчно разворачивается в последовательность букв русского алфавита (циклически). В результате получается прямоугольник со сторонами 10 × 10, который и является гипотетической страницей книги-ключа:

	1	2	3	4	5	6	7	8	9	0
1	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
2	Р	С	Т	У	Ф	Х	Ц	Ш	Ь	Э
3	Е	Ж	З	И	К	Л	М	Н	О	П
4	К	Л	М	Н	О	П	Р	С	Т	У
5	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Ь
6	А	Б	В	Г	Д	Е	Ж	З	И	К
7	С	Т	У	Ф	Х	Ц	Ш	Ь	Э	Ю
8	Н	О	П	Р	С	Т	У	Ф	Х	Ц
9	А	Б	В	Г	Д	Е	Ж	З	И	К
0	Я	А	Б	В	Г	Д	Е	Ж	З	И

В соответствии с этим квадратом производилась замена букв открытого текста на их координаты (первая цифра – номер строки, вторая – номер столбца). Например, буква П получала обозначения: 11, 30, или 46 и др. Слово «агент» может иметь разные шифробозначения : «61, 94, 07, 44, 53» или «02, 64, 66, 38, 49» и др. Этот шифр обладает уже неплохой криптографической стойкостью.

Дальнейшее усложнение шифра многозначной замены связано с введением «пустышек» – фиктивных знаков в шифрованный текст. Например, пусть действует ранее описанный шифр по слову. Заранее оговорено, что столбцы и строки с номерами 2 и 9 являются «пустыми», т.е. вычеркиваются. Таким образом, появляется возможность вставлять в шифрованный текст «пустые» комбинации, содержащие указанные цифры. 27, 95, 92, 29 и др.

Следующее усложнение заключается в одновременном использовании нескольких квадратов, полученных по разным ключам-лозунгам. При шифровании квадраты таблицы используются циклически один за другим. Иногда переход следующему квадрату отмечался определенными комбинациями знаков, например, трехкратным повторением одной и той же буквы в открытом тексте. Шифр стал более стойким, но менее удобным в применении.

Стихотворный шифр. В этом шифре ключом является заранее оговоренное стихотворение, оно записывается в прямоугольник согласованными сторонами, например, 10 × 20. Этот прямоугольник является ключевой страницей книжного шифра.

Приведем реальный исторический пример стихотворного шифра, применявшегося революционерами в начале XX в. Ключом шифра являлось стихотворение Н.А. Некрасова «Школьник»: «Ну пошел же ради бога…». Стихотворение вписывалось в квадрат со сторонами 10 × 10; лишние буквы строки выбрасывались (строки стихотворения содержат более 10 букв):

	1	2	3	4	5	6	7	8	9	10
1	Н	У	П	О	Ш	Е	Л	Ж	Е	Р
2	Н	Е	Б	О	Е	Л	Ь	Н	И	К
3	Н	Е	В	Е	С	Е	Л	А	Я	Л
4	Э	Й	С	А	Д	И	С	Ь	К	О
5	Н	О	Г	И	Б	О	С	Ы	Г	Р
6	И	Е	Д	В	А	П	Р	И	К	Р
7	Н	Е	С	Т	Ы	Д	И	С	Ь	Ч
8	Э	Т	О	М	Н	О	Г	И	Х	Ъ
9	В	И	Ж	У	Я	В	К	О	Г	О
10	Т	А	К	У	Ч	И	Т	Ь	С	Я

Начало зашифрованного текста «Сообщите …» могло иметь разные варианты написания:

«3/5 1/4 5/6 2/3 1/5 7/7 7/4 7/2 …»

«5/7 5/6 8/6 5/5 1/5 5/4 9/9 6/2 …» и т.д.

Числитель дает строку, а знаменатель номер столбца. Ввиду отсутствия в таблице буквы «Щ» она заменена на «Ш» (что не мешает правильному расшифрованию).

Одна из ошибок революционеров заключалась в частом использовании произведений поэтов демократов, которые были знакомы полиции. Это облегчало дешифрование секретных посланий, поскольку сама идея шифрования была известна полиции. Защиту обеспечивал лишь ключ – «секретное стихотворение». Другая ошибка, облегчающая дешифрование, заключалась в частом употреблении стандартных слов и выражений: «Сообщите … », «Направляю вам …», «явка», «адрес» и др. Частое использование одного и того же ключа – стихотворения также облегчало дешифрование сообщений. Полиция эффективно использовала эти ошибки.

Иногда заранее обусловленная фраза или начало некоторого стихотворения использовались в качестве исходной

гаммы шифра периодического гаммирования (упомянутый ранее шифр Гамбетта). Например:

Небо лазурное в море купалося,
Солнышко ласково морю смеялося…

В соответствии с заранее оговоренным правилом подчеркивались буквы стоящие на нечетных местах: 1,3,5 и др. до 17. Эти буквы выписывались:

Н, Б, Л, З, Р, О, В, О, Е

Затем эти буквы переводились в числа в соответствии с их положением в русском алфавите. Получалось 17 чисел, которые и являлись исходной гаммой шифра. Открытый текст переводился в числа аналогичным образом (по месту букв в алфавите). Исходная гамма периодически подписывалась под преобразованным открытым текстом, и шифрованный текст получался в результате сложения буквы (числа) открытого текста с соответствующим знаком гаммы шифра. Нетрудно заметить, что данный шифр воспроизводит давно известный шифр Виженера, описанный ранее. Этот шифр получил широкое распространение и оказался достаточно стойким при его грамотном использовании.

А вот один из шифров анархистов, описанный одним из идеологов этого движения в России П.А. Кропоткиным. Он вспоминает: «У Новицкого (сподвижника Кропоткина – прим. авт.) на столе лежало моё письмо, взятое на мне в момент ареста… Это была коротенькая записка шифром, в которой я писал в Москву: «Вот вам два паспорта, передайте их так-то». Следователь, обнаруживший письмо, заявил, что ключ к шифру обнаружен при обыске одного из революционеров».

Далее Кропоткин вспоминает: «…наш шифр был самый простейший… Он опирался на 10 слов, которые следовало запомнить, не записывая:

Пустынной Волги берег
Чернеют серых юрт рядами
Железный финогеша Щебальский

Каждая буква обозначалась словом и местом буквы в слове.

П было 11, У – 12, С было 13 или 51, или 07 (10 слово, 7-я буква). Буквы, часто встречающиеся, как Е или А, обозначались, как видно, по разному: 32, 34, 42, 72, 86 или 02 для Е и 36, 74, 88, 04 для А.

Расшифровать такой шифр невозможно, тем более что мы писали сплошь, иногда ставя нечетное число букв в начале письма и в конце и еще запутывая расшифровку ненужными парами, как 26, 27, 28, 29, 20, вставленными там и сям».

Этот шифр является разновидностью книжного шифра, в котором вместо ключа – книги использовались легко запоминаемые фразы (стихотворения).

П.А. Кропоткин подчёркивал, что «у нас имелись специальные шифры для каждого из провинциальных кружков». Таким образом, шифры были индивидуальными для каждого адресата. Однако одновременно он отмечал и чрезмерную трудоёмкость зашифрования: «Мы часто работали ночь напролёт, исписывая листы каббалистическими знаками и дробными числами». Отсюда следует, что основными шифрами являлись разновидности книжных шифров (в том числе – стихотворных), а также шифры простой замены.

Следует отметить, что нередко вводились различные усложнения известных шифров (использование пустышек и др.). Можно отметить «рациональный шифр» предложенный одним из лидеров БУНДА Л. Розенталем в его книге «Шифрованное письмо», изданной в Женеве в 1904 г. Он считал его достаточно стойким, но по сути дела этот шифр является шифром пропорциональной замены. Такие шифры употреблялись и ранее и были известны методы их дешифрования.

Революционеры активно применяли стеганографию. Первоначально применялись весьма простые составы «химического письма». Так, например, Н.К. Крупская одному из своих корреспондентов писала: «Не пишите мне лимоном, все проявляется само собой» (1901 г.). Другому корреспонденту (1902 г.) она сообщила: «Передайте, пожалуйста, Парамоновой, что оба ее письма получены, но они написаны такой пло-

хой химией, что ни слова нельзя было разобрать, пусть скорее повторит…». В другом письме она рекомендовала «писать совсем чистым пером и вовсе не нажимать, а то видно».

В дальнейшем революционеры существенно усовершенствовали технологию «химической переписки». Появились сложные химические составы для стеганографической переписки. Так, например, в 1902 г. З.П. Кржижановская предложила следующий рецепт: «писать 1% спиртовым раствором *β*-нафтола; чистить резинкой. Для проявления растворить немного паранитранилина в разведенной соляной или серной кислоте, прибавить туда несколько капель раствора азотнонатриевой или азотисто-калиевой соли и тотчас при приготовлении влить эту смесь в большой объем крепкого раствора уксуснонатриевой соли ».

Но здесь возникло неудобство. Необходимо было запасаться дефицитными компонентами. Были предложены и более простые химические составы.

Использование сложных химических составов поставило перед Департаментом полиции России серьезные проблемы. Например, один из ведущих дешифровальщиков департамента И.А. Зыбин в одной из докладных записок (начало XX в.) описал рецепты проявления «химических чернил» в следующем виде:

«1. Растворить азотнокислое серебро при подкуривании аммиаком и при освещении вольтовой дугой.

2. Раствором эскулина (флюоресцирующих мест незаметно при освещении вольтовой дугой).

3. 5% -ным раствором ализариновых чернил (контроль – бумага с чистой водой).

4. Раствором желтой кровяной соли (0,5%) .

5. Раствором сернистого аммония (1%).

6. Раствором аммиака (1%).

7. Раствором красной кровяной соли с бромистым калием (1%).

Ввиду проб (1, 2, 3) пробы йодом, нагреванием и полуторахлористым железом как менее чувствительные и бесполезные применены не были».

С йодом Зыбин ошибся. В начале XX в. немцы убедились в эффективности применении паров йода для проявления стеганографических посланий.

При отсутствии заранее оговоренного шифра революционеры использовали намеки, иносказания и др. Приведем лишь один пример.

В 1900 г. соратник В.И. Ленина В.П. Ногин находился в Англии. Ленину было необходимо сообщить Ногину фамилию петербургского издателя книги К. Каутского (книга революционного содержания). Ленин писал Ногину: «Боюсь доверить фамилию почте – впрочем, передам Вам ее таким образом. Напишите имя. Отчество (на русский лад) и фамилию Алексея (Ю.О. Мартова – авт.) и обозначьте все 23 буквы цифрами по их порядку. Тогда фамилия … составится из букв: 6-й, 22-й, 11-й, 22-й (вместе же читайте следующую по алфавиту букву), 5-й, 10-й и 13-й». Настоящее имя «Алексея» известное обоим корреспондентам, было Юлий Осипович Цедербаумъ; пронумеруем это имя по буквам:

ю	л	и	й	о	С	и	п	О	в	и	ч
1	2	3	4	5	6	7	8	9	10	11	12
ь	ц	е	д	е	Р	б	а	У	м	ъ	
13	14	15	16	17	18	19	20	21	22	23	

Тогда чтение «шифрованного» сообщения дает фамилию «Смирновъ». При шифровании Ленин допустил ошибку (пропустил букву Р = 18), однако эта ошибка была легко обнаружена и устранена Ногиным.

Однако следует подчеркнуть, что подпольщики допускали при использовании шифров серьезные ошибки, что приводило к дешифрованию их переписки противником (в первую очередь, департаментом полиции). Примерами таких ошибок являются редкая смена ключей, шифрование текста не целиком, а только наиболее «секретной» его части и др. Использовались и откровенно слабые шифры (типа простой замены). Так, например, полиции удалось перехватить и дешифровать переписку народовольцев после убийства царя Александра II в марте 1881 г. В результате некоторые члены этой организации были арестованы и казнены.

Сам В.И. Ленин придавал особое значение правильному (без ошибок) использованию шифров. В письме (декабрь 1902 г.) он писал своему брату Д.И. Ульянову: «Ваше письмо получено. Написано оно неизвестным нам ключом, впрочем, мы расшифровали все, за исключением адресов. Не шифруйте иначе, как целыми фразами, иначе очень легко раскрыть ключ...». Здесь речь идет о том, что в секретных письмах часто оставались незашифрованные «не секретные» слова и фразы. Этот «клер» существенно облегчал дешифрование.

Аналогичное послание своему корреспонденту в том же году направила Н.К. Крупская. Получив плохо зашифрованное письмо она в ответ возмущалась: «Перво-наперво позвольте Вас выругать, что называется на все корки, за небрежную шифровку. Не зная, что Вы условились о ключе с Евгением, я недоумевала, каким ключом Вы пишите, и, наконец, расшифровала Ваше письмо без ключа в какие-нибудь ½ часа. Это просто скандал. Не повторяйте одних и тех же знаков для одной той же буквы, иначе шифровка никуда не годится».

Таким образом, допускаемые при шифровании ошибки часто сводили «на-нет» все усилия по защите информации. Поэтому ключи шифров и правила их использования часто менялись. Были введены так называемые «одноразовые ключи», сменявшиеся с каждым новым зашифрованием. Так, например, ключевое стихотворение оставалось тем же, но по простому закону менялась нумерация его строк (начинать со второй строки, считая ее первой, и т.д.). Иногда применялась практика смены ключа в процессе шифрования одного послания (по заранее оговоренному условию). Смена шифра практиковалась и в тех случаях, когда возникало подозрение о полицейском дешифровании ранее перехваченных писем. Так, в 1902 г. Ю. Цедербаум писал в редакцию газеты «Искра»: «Не находит ли Фекла (псевдоним – *авт.*) нужным переменить шифр, потому что, очевидно, несколько наших писем к ней пропали». Принятые революционерами меры по усилению защиты информации оказались достаточно эффективными. Так, в одном из документов «охранки» (1903 г.) говорилось о том, что дешифрование «подпольных» посланий существенно усложнилось в связи с усложнением усло-

вий применения шифров. «Теперь, – говорилось в документе полиции, – революционеры пользуются для переписки или двойными ключами, или страницами малоизвестных книг и брошюр, избирая для каждого корреспондента отдельную книгу и избегая повторения страниц. Нередко письма можно также дешифровать только в случае, если их соберется от трех до пяти из одного и того же пункта».

Здесь речь идет об использовании в дешифровании многократного повторяемого ключа шифра, что существенно облегчает процесс дешифрования.

Революционеры постоянно усиливали свои шифры, что приводило к усложнению их дешифрования со стороны департаментом полиции. В мае 1903 г. И.Зыбин в своей докладной записке писал о том, что разрабатывать шифрованные документы становится все труднее. Он указывал следующие причины.

1. Количество шифрованных посланий стало огромным.
2. Революционные деятели стали пользоваться двойными ключами.

Это означает, что шифртекст, полученный на одном ключе, повторно шифруется на другом.

При применении книжного шифра стали использоваться страницы малоизвестных книг, причем у каждого корреспондента имелась своя личная книга. К тому же они часто меняют страницы этих книг, по которым шифруется послание.

Еще ранее он сообщил об отсутствии необходимого количества квалифицированных дешифровальщиков в департаменте полиции. Зыбин предложил создать систему подготовки соответствующих специалистов. Это предложение было принято.

В заключении следует отметить, что наряду с «государственной» криптографией, появилась и начала активно развиваться «антигосударственная» криптография, которую использовали различные антиправительственные организации. Здесь возникали уникальные шифры, отвечающие требованиям «подпольного» использования.

В ответ правительство создало организации, боровшиеся с «подпольной криптографией». Деятельность этих организаций оказалась достаточно эффективной. Эта деятельность

была окружена большой секретностью и находилась под непосредственным контролем высших должностных лиц государства (включая императора). Успехи в ней щедро поощрялись как материально, так и морально.

Подводя итог рассказа о шифрах подпольных организаций, приведем стихотворение известного советского поэта Е. Долматовского «Легенда о шифре», где в художественной форме он выразил значение шифров в переписке революционеров:

«Начало века. Очень далеко
Кандальная сермяжная Россия.
Чернила заменяет молоко,
Неразличимы буквы прописные,
Они еще проявятся, когда
Над пламенем бумага опалится,
Когда протянут почту поезда
Под носом жандармерий и полиций …
Почтовым делом правят «Ильичи» –
Так называют их семью в Женеве,
И это слово для друзей звучит
Любого восхищения нежнее …
Он пишет, а она его слова
По хитрой сетке переводит в цифры.
Минск, Петербург, Одесса и Москва
Его поймут – они имеют шифры.
Подпольщиками Пушкин и Крылов
И Лермонтов тогда в Женеве были,
Шифрованные строки их стихов
Служили связью нараставшей силе.
Еще не скоро нашей будет власть,
Еще не раз узнаем пораженье,
Но проявилась в пламени, зажглась,
Строка: «Я помню чудное мгновенье».
Как к роднику. Я к прошлому приник,
Чтобы испить и стать непобедимым,
Любви и революции язык
Единым был и должен быть единым.
Прокладывать дорогу нелегко,
Но мы тверды. Единой цепи звенья.
Скрепляет старый шифр большевиков –
Я помню чудное мгновенье».

(Е. Долматовский. Собр. соч. в 3 т. т. 2. – М., 1979, с. 320–321).

В следующей главе подробно рассматриваются криптографическая деятельность ряда революционных организаций и борьба полиции с революционной криптографией.

Список рекомендуемой литературы

1. Анин Б.А., Петрович А.И. Радиошпионаж. – М., 1996.
2. Вальдман Э.К. Занимательная телеграфия и телефония. – М., «Связь», 1964.
3. Востоков К. У истоков радиовойны // Независимое военное обозрение. – 2000. – С. 7.
4. Красная книга ВЧК. т. 1. – М, 1990.
5. Красная книга ВЧК. т. 2. – М, 1990.
6. Крестовский В. Двадцать месяцевъ въ действующей арміи. (1877-1878) письма въ редакцію газеты «Правительственный вестникъ» отъ ея офиціальнаго корреспондента, лейбъ-гвардіи уланскаго Его Величества полка штабсъ-ротмистра Всеволода Крестовскаго, Т.2. – СПб.: типографія министерства внутренних делъ, 1879.
7. Кропоткин П.А. Записки революционера. – М., 1988.
8. Кудрявцев-Сфайт С. Русский флот – колыбель радио. – М.; Л.: Военмориздат, 1939.
9. Найтли Ф. Шпионаж XX века. – М., 1994.
10. Немирович-Данченко В.И. Скобелев. – М., Воениздат, 1993.
11. Николаев И. Под железной пятой. – М., 1978.
12. Очерки истории внешней разведки: в 2 т. / под ред. Е.М. Примакова. – М.,1997.
13. Синельников А.В. Шифры и революционеры России // www.cryptography.ru.
14. Спиридонович А. Записки жандарма. – М., 1991.
15. Уральский Ю.С. Пароль: «От Петрова». – М., 1988.
16. Kahn D. The codebreakers. – N.-Y., 1967.
17. Kahn D. Kahn on codes. – N.-Y., 1983.
18. Keith Melton H. The ultimate spy book. – N.-Y., 1992.

Глава 5.

Криптографическая деятельность революционеров в России

5.1. Криптографическая деятельность революционеров в 20–70-х гг. XIX в.: успехи и неудачи

Криптографические методы защиты и нападения использовались не только в международной борьбе. Во внутренней политике они также играли важную роль. Характерными в этом отношении являются эпизоды XIX – начала XX вв., имевшие место в России. Революционеры-подпольщики XIX в. в России активно использовали криптографические методы защиты информации. В статье [Бабаш, 2004], с которой читателю предварительно рекомендуется ознакомиться, описываются шифры[1], использовавшиеся революционными организациями. В данном разделе описывается как революционеры использовали шифры с целью защиты своих секретов от правоохранительных органов Российской империи.

Именно в XIX в. бурный рост революционного движения в России породил активное противоборство между революционными организациями, стремившимися защитить собственную информацию, и правоохранительными органами, защищавшими существовавшую тогда политическую систему (против революционеров работали дешифровальщики, службы перлюстрации и цензуры). Однако следует отметить, что с внутренней перепиской перлюстраторы и цензоры активно работали и ранее.

[1] Также подробно ознакомиться с российскими шифрами российских революционеров XIX – начала XX вв. можно в работах, указанных в списке рекомендуемых литературных источников к главе 5.

В XVIII в. важную роль в России стали играть органы государственной почтовой цензуры. Они были созданы сразу после создания разветвленной сети почтовой связи и почтамтов. Именно почтамты стали центрами деятельности органов цензуры.

Изучались имена всех подозрительных лиц. В связи с этим уместно напомнить высказывание сенатора И. Лопухина (конец XVIII в.). Лопухин был членом масонской ложи (мартинистов). Членами этой ложи являлись известные люди, титулованные особы. Однако деятельность этих лож вызывала тревогу у правительства, переписка их часто перлюстрировалась.

По этому поводу Лопухин пишет: «Открывали на почте наши письма, и всех моих писем копии, особенно к одному тогда приятелю бывшему в чужих краях, отсылались к государыне (Екатерине II – *авт*.). Я сим ни мало не беспокоился и знавши писал всегда так, как бы я говорил наедине в полной откровенности».

В этих письмах Лопухин рассказывал о благородных целях общества и верности ее членов государыне-императрице и России. Однако все выявленные масоны были арестованы и по суду приговорены к ссылке, а один из них (известный книгоиздатель Новиков) – к 18 годам тюремного заключения за распространение запрещенных книг. Что же касается Лопухина, то он волей государыни был оставлен в Москве, учитывая его прежние государственные заслуги, однако полицейский присмотр за ним сохранился.

Как видно, жертвой цензуры становились весьма высокопоставленные люди. Вот еще один пример. Отец декабриста П. Пестеля – Иван Пестель – директор почты России, получил тайное поручение от императора Павла I. Смысл: вскрывать подозрительные письма, копировать и пересылать копии императору (в том числе – письма А. Радищева).

С И. Пестелем сыграл шутку хитрый и остроумный князь Ростопчин. Он отправил письмо, в котором – заговор против Павла. Пестель торжествовал, но увидел в письме: «Не удивляйтесь, что пишу вам по почте. Наш директор почты тоже вместе с нами». Показать – не показать? Пестель унич-

тожил письмо. Ростопчин только этого и ждал – сообщил Павлу I. Пестеля уволили со всех должностей и отправили на жительство в Москву.

Император Павел I

Первым серьезным революционным выступлением в России стало восстание на Сенатской площади Санкт-Петербурга в декабре 1825 г. После подавления восстания декабристов многие из его участников оказались в местах заключения, где для общения между собой и с другими узниками использовали шифры. Приведем примеры.

Один из активных участников этого восстания Вильгельм Кюхельбекер был отправлен в ссылку в Сибирь. В пересыльной тюрьме его соседом оказался князь Сергей Оболенский, наказанный за разгульный образ жизни (картежник, игрок, забияка и др.) и не имевший никакого отношения к декабристам.

Вильгельм решил установить с ним связь путем перестукивания по тюремной азбуке. В ответ он получал удары по стене руками и ногами. Кюхельбекер сумел передать Оболенскому записку и получить ответ. Этот ответ начинался так: «Дорогой сосед зовут меня князь Сергей Оболенский я штабсротмистр гусарского полка сижу черт его знает за что, будто за карты и рулетку а главнейшее что побил командира …?».

Кюхельбекер понял, что Оболенский плохо владеет русским языком и прекратил попытки использовать перестукивание для общения с ним.

Князя перевели в Грузию, где в то время находился друг Кюхельбекера А.С. Грибоедов. Вильгельм сумел передать князю письмо к своему другу. Однако при обыске у князя обнаружили это письмо и определили, что оно написано рукой Кюхельбекера. Грибоедову этот факт создал очевидные проблемы (связь с декабристами). Однако он сумел доказать свою невиновность.

После декабрьских событий братья Бестужевы оказались в Петропавловской крепости. Они использовали для связи между собой «тюремную азбуку», в основе которой лежал шифр Полибия. Далее в своих воспоминаниях М. Бестужев пишет: «Когда мы достукались досыта, нам захотелось распространить наше отношение с соседями, и преимущественно с Рылеевым, который тогда сидел через одну камеру от брата. Но, к несчастью, в этой камере сидел Одоевский, молодой, пылкий челов. и поэт в душе… Этот-то пыл физической деятельности и был причиной, что даже терпение брата Николая разбилось при попытках передать ему нашу азбуку. Выждав минуту тишины в его каземате, едва брат начинал стучать ему азбуку, он тотчас отвечал таким неистовым набатом, колотя руками и ногами в стену, что брат в страхе отскакивал, чтоб не обнаружить нашего намерения. Самая ничтожная безделица разбила в прах наши мечты… Одоевский не знал азбуки по порядку».

Князь А. Одоевский после окончания срока каторжных работ был переведен на Кавказ простым солдатом, где вскоре умер в экспедиции против черкесов.

Перестукивание с использованием шифрования по квадрату Полибия позднее широко применялось арестованными революционерами – народниками, большевиками и др.

После декабрьских событий 1825 г. Николай I решил реформировать тайную службу в целях ее усиления. Прежняя служба, функции которой выполняли тайная канцелярия Павла I и особенная канцелярия при министерстве юстиции, а затем (при Александре I) тайная канцелярия при министерстве внутренних дел, по мнению императора, не отвечала потребностям времени, так как не смогла своевременно раскрыть заговор.

Чтобы предотвратить в будущем события, подобные декабрьскому восстанию, за настроениями в обществе следовало установить строжайший контроль. Николай I решил привлечь к этой работе образованных известных в обществе людей, которые бы придали тайной службе соответствующий имидж. В результате было создано знаменитое III отделение

Собственной его императорского величества канцелярии, во главе которого был поставлен генерал Бенкендорф, участник войны 1812 г.

Бенкендорф Александр Христофорович

Бенкендорф был хорошо знаком с деятельностью аналогичной службы Франции, имел навыки дипломатической работы и был достаточно популярной в обществе личностью. Он предоставил императору записку, которая называлась «Проект об устройстве тайной полиции». В этой записке особое место уделялось перехвату и перлюстрации писем. Бенкендорф писал: «Вскрытие корреспонденции составляет одно из средств тайной полиции и притом самое лучшее, так как оно действует постоянно и охватывает все пункты империи. Для этого нужно лишь иметь в некоторых городах почтмейстеров, известных своею честностью и усердием. Такими пунктами являются Петербург, Москва, Киев, Вильно, Рига, Харьков, Одесса, Казань и Тобольск».

В 1826 г. император принял предложение генерал-адъютанта графа Бенкендорфа. Был создан отдельный корпус жандармов, ставший исполнительным органом III отделения. Кадры жандармерии набирались из офицеров армии, хорошо проявивших себя на военной службе. Корпус жандармов стал основной ударной силой в борьбе с антиправительственными организациями: III отделение получило практически неограниченную власть над министерствами и ведомствами страны. Кроме того, оно стало выполнять функции цензуры в России. Сам Бенкендорф вошел в историю не только как государственный деятель, но в значительной степени как главный цензор А.С. Пушкина. Естественно, в III отделении, имелась служба анализа перлюстрированных и дешифрованных писем.

Помимо службы перлюстрации большое значение в обеспечении государственной безопасности играли органы цензуры. С развитием почтово-телеграфных связей была создана почтовая цензура. Проверялись письма, газеты, журналы и другие почтовые отправления.

В составе комитетов внутренней цензуры имелись так называемые «черные кабинеты», о назначении которых знал очень узкий круг людей. Кабинеты занимались тайным вскрытием, просмотром, снятием копий с писем и телеграмм. С появлением секретных посланий (стеганографических, шифрованных) появились специалисты по их вскрытию. Анализировались почерки отправителей. Бывший начальник царской охранки в начале XX в. А. Васильев подтверждал следующее: «Благодаря этой цензуре Россия спасла себя от шпионства, ограблений, убийств и терроризма преимущества этой системы достаточно очевидны, то время как о недостоинствах вообще можно не упоминать. Добропорядочному гражданину не нужно опасаться цензуры, потому что частная информация обычно игнорируется читающими».

В дополнение к действовавшим «черным кабинетам», занимавшимся перлюстрацией дипломатической корреспонденции, в связи с ростом революционного движения в России в 80-х гг. XIX в. в стране были открыты перлюстрационные пункты для перехвата переписки российских граждан в Петербурге, Москве, Киеве и ряде других городов. Эти перлюстрационные пункты создавались на почтамтах при отделах цензуры иностранных газет и журналов. Официально они назывались «секретными отделениями». Общее руководство всей перлюстрационной работой в России возлагалось на старшего цензора Петербургского почтамта, который был наделен правами помощника начальника Главного управления почт и телеграфов и в то же время находился в подчинении министра внутренних дел, от которого получал распоряжения и санкции на проведение перлюстрации.

Перлюстрации подлежали письма, делящиеся на две категории: «по подозрению» и «по наблюдению». Письма «по

подозрению» вскрывались в том случае, если вызывал подозрение почерк адресата. Имелись соответствующие специалисты, умеющие по почерку адреса установить необходимость вскрытия письма. Письма «по наблюдению» перлюстрировались согласно списку адресов, который присылался Департаментом полиции.

Перлюстрации могли подвергаться письма всех подданных государства, за исключением императора и министра внутренних дел. Данные перлюстрации использовались только для оперативной работы. При дознании и в суде они не использовались, как и любые материалы, добытые «частным путем», так как перлюстрирование писем было незаконным, оно противоречило Уложению о наказаниях, предусматривающему кару за нарушение почтового Устава. Поэтому работа по перлюстрации держалась в строгом секрете.

В начале XX в. ежегодно по всей стране просматривалось около 400 000 писем. Наиболее интересные сведения регулярно докладывались императору. Император Николай II проявлял значительный интерес к сведениям, полученным подобным образом.

Самый большой, поток писем шел через Петербургский почтамт. Ежедневно здесь вскрывалось от 2 до 3 тыс. писем. Конверты вскрывались особыми косточками или длинными иглами, отпаривались, отмачивались в ванночках. Письма с «интересными» сведениями откладывались для снятия копий. Просмотренные письма запечатывались. На обратной стороне каждого просмотренного письма в одном из уголков ставилась точка (мушка), чтобы письмо не было подвергнуто перлюстрации вторично. В «черном кабинете» письма задерживали недолго – всего 1 ч или 2 ч. Лишь в тех случаях, когда их текст был написан симпатическими чернилами или зашифрован, их в подлиннике отправляли в Департамент полиции, где и подвергали соответствующей обработке. Копии и выписки из писем делали в двух экземплярах. Один экземпляр по списку Департамента полиции отправляли директору этого департамента, а второй (и оба экземпляра по списку министерства

внутренних дел) шел министру внутренних дел. На местах, в других городах, перлюстрировалась только та корреспонденция, которая шла из этого города или в город, но не транзитная. Копии также делались в двух экземплярах. С местными властями перлюстрационные пункты контактов не имели. Однако, когда в письмах попадались указания на то, что готовится какое-либо политическое событие: забастовка, экспроприация и др., выписка посылалась местному градоначальнику.

В течении 30 лет до 1914 г. перлюстрацией руководил один и тот же чиновник – действительный тайный советник Фомин. Его знал очень ограниченный круг лиц, включавший министра внутренних дел и директора департамента полиции. Как только назначался новый министр внутренних дел, Фомин являлся к нему и передавал специальный пакет с надписью «Совершенно секретно». Министр вскрывал конверт и обнаруживал указ Александра III на право перлюстрации.

Теперь рассмотрим вопрос о том, как революционные организации использовали криптографические методы защиты информации и какие были успехи у правоохранительных органов в области криптоанализа.

В 60-е гг. XIX в. наблюдался непрерывный рост революционного движения. Вступивший на престол царь Александр II в 1861 г. отменил крепостное право. Начало царствования нового императора вызвало в российском обществе небывалый энтузиазм и породило надежды. Свежее дыхание обрела существующая со времен Николая I русская политическая эмиграция, которая начала налаживать связи с Россией. Усилились крестьянские и национально-освободительные движения по периферии Российской империи. В этот период в России и за рубежом возник ряд революционных организаций. Параллельно росли и преследования со стороны правоохранительных органов.

Первые сведения о шифрах подполья в России появились в начале 1860-х гг. В январе 1861 г. полиция перехватила письмо молодого подпольщика Митрофана Муравского к его другу в Петербург. Сосланный в Уфимскую губернию Мурав-

ский писал товарищу: «Позвольте предложить следующую азбуку, к которой, мне кажется, можно было бы прибегать в необходимых случаях... Я спешу и не имею времени изложить ее. Я пришлю ее вам, если не случится оказии, по почте, а именно так: этой азбукой я напишу общеизвестное... стихотворение Пушкина Декабристам... Зная это стихотворение, Вы его прочтете, и таким образом узнаете и саму азбуку; недостающие буквы я напишу отдельно. Устройство ее, как Вы увидите, очень просто». 19 февраля 1861 г. Муравский отправил в Петербург очередное письмо. Конец его оказался испещрен какими-то точками и черточками. Очевидно, это и был предложенный им шифр.

Находящиеся в Лондоне русские эмигранты в своей переписке с родиной зачастую вообще не прибегали к шифрам, а применяли условный язык – жаргонные коды. Например, применял такой способ Михаил Бакунин в «шифрованных» посланиях к Михаилу Налбандову (он же Налбандян, впоследствии – известный писатель и демократ). После провала Налбандяна при его обыске полиция обнаружила содержательный кодированный словарь: Открыть торговый дом – сосредоточить и умножить войска; покупать лен – с горцами начать переговоры и заключить союз; иметь кредит – издавать газету; для покупки товара – для восстания; хронометр – пушка; часы – штыковое оружие; мука – порох; пшеница – ядро... Судя по такому жаргону, намерения у армянских революционеров были самыми серьезными.

В конце 1861 г. в Петербурге возникла организация революционеров «Земля и Воля» (первая с таким названием). Организация с первых дней своего возникновения была строго законспирирована и имела структуру изолированных пятерок. Просуществовала она, однако, недолго и уже к концу 1863 г. самоликвидировалась. Из воспоминаний одного из членов этой организации Л. Пантелеева известно, что в практике «Земли и Воли» для переписки использовались симпатические чернила и шифры: «У одного из арестованных... нашли письмо офицера из провинции (А.Н. Столпакова); пись-

мо заканчивалось рядом шифрованных строк в виде дробей. Это был дробный книжный шифр. Не обладая необходимыми специалистами, полицейские передали шифрованное сообщение в МИД, но даже их криптоаналитики не смогли с ним справиться.

Тем временем наступали 1870 гг., революционное движение усиливалось. Началось хождение в народ. Позднее были созданы широко известные организации «Земля и Воля» и «Народная Воля».

И в эти годы революционеры активно применяли шифры, используя при этом очень простые конструкции.

В июле 1871 г. в Петербурге открылся судебный процесс «по делу о заговоре, составленном с целью ниспровержения существующего порядка управления в России», над членами организации «Народная расправа», известный также как процесс нечаевцев. На процессе прозвучала информация о шифрах, используемых в организации. Нечаевцы использовали шифр простой замены. Например, ноль означал «О»; пять – «П»; десять – «Д»; одиннадцать – «И»; три – «З»; четыре – «Ч» и др. Обычно шифрованные документы, а часто и ключи, попадали в руки жандармов при обысках арестованных революционеров. Однако иногда предпринимались и специальные мероприятия. Интересен следующий эпизод. В 1870 г. в Киев на имя подставного лица – отставного майора Криницкого – пришло письмо из Женевы. Оно оказалось от руководителя организации Нечаева, благополучно скрывшегося в Швейцарии. Адрес майора был «подставлен» Нечаеву самой полицией. Письмо же содержало некий загадочный коммерческий счет. Киевские жандармы ничего в нем не поняли и посчитали, что Нечаев ошибочно выслал счет Криницкому. Документ на всякий случай отправили в Петербург, где его без труда разобрали специалисты по шифрованным записям.

Кроме рассмотренного шифра в нечаевской организации существовал другой – буквенный. Этот шифр без особых затруднений был вскрыт специалистами министерства иностранных дел. Этим шифром был зашифрован программный

документ организации «Катехизис революционера». Он был обнаружен жандармами при массовых арестах. Он представлял собой «печатную в 16-ю долю листа книжку на иностранном языке, как бы на итальянском», – так значилось в протоколе его осмотра. Но во время следствия стало очевидным, что книжка написана шифром. Обнаружив загадочный шифр, следственная комиссия отправила документ в министерство иностранных дел, прося «поручить сведущему лицу заняться переводом книжки для определения, что именно она в себе содержит». Найденный вслед за этим в записной книжке члена «Народной расправы» А. Кузнецова ключ к шифру помог прочесть тайнопись. В результате правительство получило в свои руки главный обвинительный документ на предстоящем процессе.

В целом, к концу 1860 – началу 1870-х гг. шифры революционного подполья оставались такими же несложными, как и в начале десятилетия. Еще не были разработаны универсальные методы шифрованного письма, при которых бы система шифра не менялась, а менялся только ключ к нему. Именно такое единообразие шифров можно увидеть в практике 1870-х гг.

Слабость шифров революционеров частично компенсировалось отсутствием в III отделении в тот период времени собственной дешифровальной службы. Криптограммы, к которым не удавалось обнаружить ключи при арестах, как правило, направлялись в министерство иностранных дел, где имелись соответствующие специалисты.

Эпоха 1870-х гг. – ярчайшая страница в революционной судьбе России. В это время в России возникло и резко обозначилось два революционных направления: одно призывало к немедленной подготовке восстания. Другое больше занималось пропагандой. Кстати видные революционеры-семидесятники принимали затем активное участие в борьбе последующих десятилетий. И это дает нам возможность проследить некоторые революционные традиции России.

Зимой 1874 г. в Петербурге началось объединение различных кружков народников, в столице находились револю-

ционеры, формально не входившие ни в одну из групп, но имеющие на них определенное влияние. Отдельные революционные кружки имелись в других городах. Но центр событий находился в столице. Именно здесь к весне 1874 г. возникла идея «движения в народ». Всю зиму 1874 г. в Петербурге шла лихорадочная подготовительная работа. Каждый крупный кружок оставлял в столице своего представителя для поддержания связи с товарищами, а для переписки вырабатывались многочисленные шифры. Весной 1874 г. из Петербурга, Москвы, Киева, Одессы и других городов начался беспрецендентный поход молодых революционеров в российскую деревню. 37 губерний страны оказались одновременно охвачены общим движением. Правоохранительные органы развернули настоящую охоту за народниками, уже с мая начался повальный арест неопытных революционеров-пропагандистов. Жандармы в течение 2–3 месяцев лета арестовали около 1700 человек, участвующих в походе по деревням России. 770 из них было привлечено к дознанию, а 193 человек стали участниками «Большого процесса» 1877 г. Обвинительный акт его дает нам богатую информацию о шифрах тогдашних подпольщиков.

В своей переписке народники использовали шифр «Гамбетта» (короткопериодическое гаммирование) и стихотворный шифр. Ключами к этим шифрам служили стихотворения «Пустынной Волги берега...», «У парадного подъезда» и др. Были и ключи «собственного сочинения», в частности, содержащие нецензурные слова и выражения. В обвинительном акте народника Сергея Ковалика читаем: «Кружок Ковалика придерживался теории Бакунина, доказательством чего может служить... изобретенный последним шифр, составленный из неблагопристойных слов». Жандармами неоднократно дается подобная характеристика – нецензурный, неприличный, неблагопристойный, но сам ключ они так и не решились воспроизвести. Информация о шифрах киевских участников «хождения в народ» была получена от раскаявшихся и давших самые откровенные показания членов кружка. Эта информация серьезно повлияла на судьбу многих участников процесса

193-х. Так гимназистка Харченко указала шифрключ для переписки киевлян с эмигрантом Павлом Аксельродом: «Богъ завещалъ намъ, чтобы мы жили по братски въ духе любви, какъ братья. Шафецельев». Но имелись и иные способы шифрования. В обвинительном акте читаем: «Для письменных сношений между собой члены кружка употребляли шифр; таких шифров было несколько... были известны два шифра: один по русско-французскому лексиону Рейфа, и другой, состоящий из цинических слов, т.е. шифр Ковалика. А Польгейм и Ларионов употребляли шифр, ключом к которому служила... одна из молитв «Отче наш» или «Богородица»». Из этих показаний ясно видно, что революционеры, помимо прочего, использовали стихотворные и книжные шифры, но применение их было ограничено.

Один из организаторов «хождения в народ» С. Ковалик (кстати, по образованию – математик). В своей статье за 1906 г. «Движение семидесятых годов по Большому процессу (193-х)» он писал:

«Ключом к шифру большею частью служил подбор нескольких таких слов (иногда коротких стихотворений), в которых заключались все буквы алфавита. Каждая буква изображалась двумя цифрами, первая показывала номер по порядку слова в ключе, вторая – место данной буквы в слове. Вследствие короткости ключа, буквы изображались почти всегда одною и тою же парою цифр, что облегчало разбор шифра даже в случае незнания ключа. Так называемый гамбеттовский буквенный шифр, несколько более обеспечивающий тайну переписки, еще не был тогда в употреблении. Но и не совершенный цифровой шифр применялся часто крайне неумело: то зашифровывались только отдельные слова, то в сплошь зашифрованном письме расставлялись, по всем правилам грамматики, знаки препинания. Поэтому стоило только угадать одно слово, и весь шифр легко разбирался... Из лиц, проводивших дознание, прославился, или может быть, вернее, прославил себя умением разбирать шифры один из товарищей прокурора, хотя каждый волостной писарь сумел бы сделать то же самое».

Таким образом, можно утверждать, что у российских революционеров впервые появился типовой шифр, нашедший широчайшее употребление. В сущности, это есть шифр Полибия, придуманный еще до нашей эры. Ковалик совершенно справедливо раскритиковал данную систему, только сделал он это слишком поздно – через 30 лет! Заметим, что Петр Кропоткин в своих «Записках революционера», наоборот, считал этот способ тайнописи весьма надежным.

Для жандармов оставались ценным источником информации показания арестованных народовольцев. Арестованный в июле 1874 г. Л. Городецкий дал самые откровенные показания. Среди прочего он привел ключ к гамбеттовскому шифру, которым пользовалась его группа, который получил от члена «самарского кружка» кружка В. Осташкина. Но мы не можем приписать заслугу в появлении данной системы шифрования лишь «самарскому кружку». В декабре 1874 г. генерал Слезкин, начальник московских жандармов, доносил в Петербург главе III отделения графу Шувалову о деятельности народников в Нижнем Новгороде:

«По просьбе Ливанова, Теплов... писал в Петербург в какую-то банковскую контору раствором соли и цифровым шифром. Нефедов показал ему другой шифр, заключающийся в замене одних букв другими». Перечисленные в донесении Теплов, Нефедов и Ливанов принадлежали к «кружку артиллеристов», действующему в столице параллельно с самарской и другими группами.

Итак, новый буквенный шифр начал распространяться среди народников с лета 1874 г. Однако в обвинительном акте процесса 193-х об этом шифре имеются крайне скудные сведения. Как показал один из арестованных пропагандистов Никифоров, он пользовался «шифром по формуле Пи». Более определенно ничего не указано, но легко сообразить, что ключом к шифру могла служить последовательность цифр числа Пи, равного 3,1415… Подобные простые шифры нетрудно было запомнить. В составлении ключей к собственным шифрам революционеры особое внимание уделяли удобству их запоминания.

После погрома народников, устроенного полицией, оставшиеся на свободе начали возрождать движение. Начало новой организации положил Иван Джабадари. Когда он приехал из-за границы в Петербург, то нашел в нем полное опустошение. Тогда он решил перенести центр подпольной деятельности в Москву, где полицейские условия были гораздо легче, чем в столице. В ноябре 1874 г. было положено начало новой революционной группы. Помимо Москвы имелись представительства в Киеве, Ивано-Вознесенске, Серпухове, Туле, Шуе и Одессе. В уставе новой организации специальный раздел, регламентирующий конспирацию и организацию связи, упоминался «общинный шифр». Он состоял в том, что составлялась табличка, разделенная продольными и поперечными линиями на 9 или 10 клеток. В этих клетках расписывалась фраза, составляющая шифр, так что в каждую клетку приходилось по одной букве. Каждый, как продольный, так и поперечный ряд клеток обозначался цифрой так, чтобы каждая клетка, а следовательно, и каждая находящаяся в ней буква, соответствовала двум цифрам: одной продольного ряда клеток, а другой – поперечного ряда». Организация была разрознена, централизованного управления не было, опыт конспирации у молодых революционеров отсутствовал. А полиция между тем не дремала. Аресты начались в марте 1875 г., а к осени организация перестала существовать. В феврале 1877 г. в Петербурге открылся очередной показательный судебный процесс над революционерами «Всероссийской социально-революционной организации» получивший название «процесс 50-ти революционеров». Как и на предыдущих процессах, в обвинительных материалах имелись многочисленные материалы по шифрам. В них отмечается наличие единой системы шифрования организации и более 10 различных ключей к ней, а также шифрованные письма. Все эти трофеи были захвачены при обысках.

Однако несмотря на новые неудачи, оставшиеся на свободе продолжали борьбу. После ареста весной 1875 г. И. Джабадари руководство организацией перешло к Георгию Здано-

вичу. Ранее он заведовал техникой, транспортом и сношениями с заграницей. В сентябре 1875 г. подпольщик оказался также арестован. Находясь в одиночной камере, Зданович вел переписку с оставшимися на воле товарищами, не подозревая, что жандармы просматривают его письма. Его письма представляли собой инструкции по практике подпольной деятельности. В одном из писем содержалось описание разрабатываемого Здановичем шифра. Это был крайне ценный трофей.

Вообще говоря, российские революционеры даже в местах заключения стремились продолжить борьбу. Находясь в 1877 г. в Доме предварительного заключения в Петербурге, народники, проходящие по делу 193-х, решили создать в стенах тюрьмы подпольную организацию. Для связи планировалось использовать жаргонные коды, так как было ясно, что переписка заключенных отслеживалась жандармами. К сожалению для подпольщиков, заговор был практически сразу раскрыт. У одного из заключенных, М. Муравского (который упоминался уже в данной статье) при обыске был изъят уличающий документ, названный в оригинале «Программа бюро раненых (ссыльных)». В нем и содержалось упоминание о способе шифрования, названном «цензурной системой шифров», однако подробное его описание в архивах полиции не сохранилось.

Подводя итог криптографической деятельности народников начиная с 1876 г., отметим, что цифровой гамбеттовский шифр долгие годы был основным шифром народников и народовольцев. Весь 1877 г. шел непрерывный ряд политических процессов. Их стенографические отчеты ходили по рукам и печатались в прессе. На заседания судов постоянно проникали сами революционеры. И уже на примерах процессов 50-ти и 193-х народники могли дать оценку своим шифрам. Все их квадратные системы взламывались жандармами одна за другой. Лишь гамбеттовские ключи к переписке каким-то образом не фигурируют в обвинительных актах. В этом, вероятно, и кроется основная причина того, что начиная с 1876 г. именно гамбеттовские шифры занимают ведущее положение среди русских революционеров. И в первую оче-

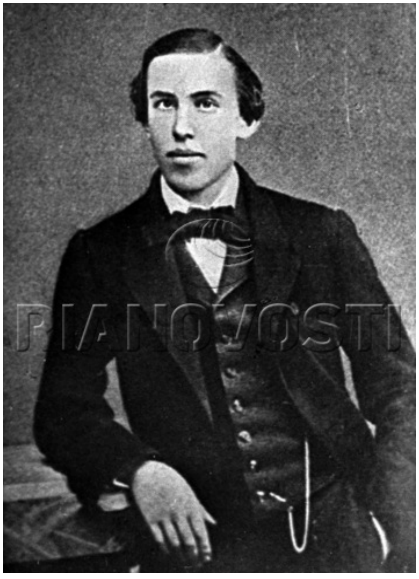
редь, это относится к такой известной организации, как «Земля и Воля». Следует отметить еще и то, что централизованной дешифровальной службы, работавшей против революционеров, по прежнему не было. Криптоанализом занимались в инициативном порядке различные сотрудники правоохранительных и судебных органов, и как видно из вышеизложенного, достигли весьма хороших результатов. Но несмотря на эти успехи, дешифрование велось в целом на любительском уровне. Каких-либо мер по организации криптоаналитической службы не предпринималось, хотя с шифрперепиской революционеров жандармы были знакомы уже более 10 лет.

5.2. Криптографическая деятельность организаций «Земля и Воля» и «Народная воля»в России в 1876–1881 гг.

В предыдущем разделе было рассказано о криптографической деятельности в период зарождения революционного движения в России. Данный раздел посвящен, в основном, организациям «Земля и Воля» и «Народная Воля». В отличии от существовавших ранее революционных групп и кружков эти организации характеризовались жесткой централизацией, а основным способом борьбы стал террор против представителей власти.

После арестов 1874–1875 гг. массовое движение «в народ» было подорвано. В 1876 г. уцелевшие от разгрома революционные кружки начали работу по воссозданию революционного движения. Главный вывод, который сделали революционеры, заключался в том, что без создания крупных централизованных, но при этом хорошо законспирированных организаций борьба с самодержавием невозможна.

В 1876 г. возвратившийся из ссылки М. Натансон возглавил так называемую «Северную революционную народническую группу». Осенью 1876 г. группа Натансона слилась с рядом провинциальных кружков и отдельными уцелевшими от



Один из организаторов общества «Земля и Воля» Николай Серно-Соловьевич

арестов революционерами. Это и стало фактическим началом знаменитого революционного общества «Земля и Воля». Тогда же были выработаны программа и устав новой организации. В основу устава революционеры положили принцип централизации и строжайшей конспирации. Центром являлся так называемый «основной кружок», а его исполнительным органом становилась «администрация». Она обязательно находилась в Петербурге и ведала распределением всех наличных сил организации и партийной техники. Целью Общества ставилась подготовка восстания под лозунгом «Земля и Воля».

Одним из основных подпольщиков, занимавшихся организационными проблемами «Земли и Воли», был Алексей Оболешев. Он руководил решением вопросов по разработке и внедрению шифров, а также созданием сети конспиративной переписки. Оболешев принимал участие в разработке упомянутого ранее устава организации. Там была оговорена возможность использования шифров для связи, при этом оговаривалось, что «…шифры и пароли, существующие для сношений между членами основного кружка, не должны быть известны никому, кроме членов основного кружка». Не отвергая возможность шифрованной переписки, устав рекомендовал максимально использовать возможности передачи информации при личных встречах. При передаче наиболее важной информации категорически запрещалось прибегать к переписке, даже шифрованной. Из этого следует, что уже на

самой начальной стадии организации своей деятельности революционеры понимали, что их шифры могут быть вскрыты противником. Веры в абсолютную стойкость шифров теперь уже не было. Таким образом, из всей предыдущей деятельности различных революционных организаций были сделаны соответствующие выводы.

В «Земле и Воле» использовались различные типы шифров: квадратные шифры Полибия, шифры перестановки, числовые ключи Гронсфельда, однако основной стала новая система, получившая так же название гамбеттовской, но качественно отличающаяся от уже известного ключа Гронсфельда. Оболешев внедрил в практику шифрования организации систему, основанную на шифре Виженера. Вскоре система подверглась усовершенствованию, подпольщики быстро поняли, что пользоваться громоздкой таблицей при шифровании и расшифровании не очень удобно. В целях конспирации ее требовалось составлять только в момент работы над криптограммами, а затем приходилось уничтожать. Все это привело к скорому появлению цифрового варианта той же системы, нашедшего широкое применение и давшего толчок к дальнейшему совершенствованию шифра Виженера. Суть же этого способа шифрования в следующем. Буквы шифруемого текста и ключа заменялись соответственно номерами их местоположения в алфавите и складывались между собой. В результате получался новый числовой ряд, т.е. шифртекст, при этом ключ (лозунг) периодически повторялся под открытым текстом. На первый взгляд, здесь получилась совершенно иная шифрсистема. Однако это все та же таблица Виженера. С 1878 г. такая система стала активно использоваться. Именно цифровой способ подобного шифра окончательно закрепит за собой название «гамбеттовского ключа». В шифрпереписке в основном использовались тридцатибуквенные алфавиты. Причем буква «Й» почти всегда ставилась в конце алфавита. При шифровании допускались серьезные ошибки. Так, часто шифровалось не все письмо, а только некоторые наиболее «секретные» места, мало того, после каждого прерывания

криптограмм открытым текстом, новая их часть опять шифровалась с самого начала ключа. И это происходило весь период деятельности «Земли и Воли», а затем и «Народной Воли». Совершенно очевидно, что это существенно снижает стойкость шифра, но революционеры пожертвовали стойкостью ради удобства использования шифра. При расшифровании можно было без труда читать письмо с любого места криптограммы, не высчитывая, на какой букве ключа закончился предыдущий шифрабзац.

Тем временем полиция, не удовлетворившись арестами 1874–1875 гг., активно продолжала работу по пресечению революционной деятельности, и не без успехов. В 1877 г. саратовский центр землевольцев был «рассеян» полицией. Однако несмотря на отдельные неудачи, «Земля и Воля» продолжала активно работать. Зимой 1877–1878 гг. в Петербурге собрался так называемый Большой совет «Земли и Воли» – около 20 человек. Основного кружка. К весне были обсуждены многие вопросы – дополнены программа и устав Общества, приняты новые члены, организована типографская группа и т.п. Организация накопила силы для продолжения своей работы, было решено создать новые поселения землевольцев среди крестьян, которые должны были стать очагами подготовки восстания.

Однако с начала 1878 г. основная ставка в борьбе с самодержавием была сделана на террор. Весь 1878 г. непрерывно происходили различные выступления, вооруженные сопротивления при арестах, убийства жандармов, прокуроров, попытки (иногда небезуспешные) вооруженного освобождения находящихся в руках жандармов товарищей. Среди жертв этих акций оказался и главный борец с революционерами шеф III отделения генерал Мезенцев, заколотый 4 августа в самом центре Петербурга землевольцем С. Кравчинским. Убийца бесследно скрылся.

Власти были крайне встревожены сложившейся ситуацией, и правоохранительные органы принимали активные меры по пресечению деятельности революционеров. Первый успех наступает в августе 1878 г., когда в Одессе был арестован

один из учредителей «Земли и Воли» Дмитрий Лизогуб. Несмотря на то, что он был богатым черниговским помещиком, Лизогуб активно занимался революционной деятельностью. С его арестом организация потеряла основной источник материального обеспечения. Однако главные события развернулись в октябре 1878 г. в Петербурге. В результате анонимного доноса на имя царя Александра II полиция выходит на Александру Малиновскую, одну из активных участниц «Земли и Воли». В результате последовавшей серии арестов были задержаны несколько руководителей организации. За 2 дня 11-12 октября 1878 г. в Петербурге был практически захвачен весь центр общества «Земля и Воля» – А. Оболешев, О. Натансон, Л. Бердников, Л. Буланов, Адр. Михайлов, В. Трощанский и с ними ближайшие помощницы А. Малиновская и М. Коленкина. Во время обысков среди прочего полиции достался ряд шифрованных документов, но большую часть революционерам удалось уничтожить. Так, Коленкина и Малиновская, оказав вооруженное сопротивление полиции, успели уничтожить свои конспиративные бумаги. Жандармам достались лишь их частичные обрывки. Оболешев съел бумаги с адресами и шифрованные письма. Только при арестах О. Натансон, В. Трощанского в руки правоохранительных органов попали некоторые шифрованные письма. Но на этот раз дешифровать их в III отделении не удалось, хотя впоследствии эти письма использовались как улики на судебном процессе против революционеров. Надо отметить, что истории известны многие случаи, когда само наличие шифрпереписки у подозреваемого, даже без ее дешифрования, служило доказательством его вины.

Успех полиции по разгрому петербургской «Земли и Воли» был бы еще более значительным если бы в ходе задержания одному из них не удалось бежать. Этим человеком был Александр Михайлов, один из руководителей организации, возглавивший оставшихся на воле землевольцев в столице, а в последствии один из создателей «Народной воли». Кстати следует отметить, что Михайлов активно занимался внедрением шифров и организацией конспиративной переписки в этих организациях.

Логотип издательства типографии «Земля и воля» 1878–1879

Даже находясь за решеткой арестованные пытались общаться с волей. Так Д. Лизогуб использовал для этой цели гамбеттовский буквенный шифр. Такой же шифр, но с другими ключами, использовали Л. Бердников и М. Коленкина. Однако и полиция не дремала. Активно применялся в частности, такой прием, как внедрение агентуры в революционную среду, причем делалось это и в местах заключения. Так, полицейские подсадили в камеру Лизогуба своего информатора. Им оказался бывший товарищ Лизогуба Ф. Курицын. Одно время он даже скрывался в имении Лизогуба от преследования полицией. Арестованный в апреле 1877 г. Курицын быстро встал на путь сотрудничества с жандармами. Его работа на полицию продолжалась довольно долго, пока в 1906 г. он не был убит эсерами. Из бесед Курицына с Лизогубом правоохранительные органы подробно узнали о существовании доселе неизвестного им революционного общества, о причастности ко многим преступлениям членов этой организации, о роли в ней самого Лизогуба. Но Лизогуб не назвал Курицыну имен своих товарищей, говорил только о прошедших событиях. Но и этого было достаточно, чтобы суд приговорил его позднее к смертной казни. Курицын также сообщил о том, что Лизогуб ведет шифрованную переписку с волей.

26 января 1879 г. полицейские достигли еще одного успеха – в Киеве был арестован один из главных идеологов революционного террора в «Земле и Воле» В. Осинский, при обыске у которого были обнаружены шифрованные письма, но как и в случае с материалами, полученными при октябрьских арестах в Санкт-Петербурге, дешифровать их жандар-

мам не удалось, хотя они были приобщены к уголовному делу в качестве вещественных доказательств.

Хотя «Земля и Воля» была самой крупной революционной организацией в конце 70-х гг. XIX в.а, в этот период действовал и ряд других групп, многие из которых так же использовали шифры для конспиративной переписки. В качестве примера приведем группу П.Л. Лаврова «Вперед». Известный теоретик народнического движения Петр Лавров проживал в эмиграции в Париже, но его группа поддерживала связи с Санкт-Петербургом. В частности, группа помогала становлению нелегальной революционной печати в России, сотрудничая с несколькими революционными организациями, в том числе и с «Землей и Волей». Группа Лаврова использовала шифр Гронсфельда, но с особенностью. Шифрованию подвергались только нечетные буквы текста, а остальные оставались без изменения. Разумеется шифрование только некоторых букв текста упрощало криптоанализ. Алфавит 30 буквенный, но здесь буква «Й» располагалась в нем в своем законном месте.

Вернемся к «Земле и Воле». К 1879 г. организация была практически разгромлена. Власти отреагировали на брошенный революционерами вызов очень жестко. В 1878–1879 гг. в различных судебных процессах приговорили к смерти 29 человек, 18 приговоров были приведены в исполнение.

Оставшиеся на свободе революционеры, в том числе А. Михайлов, горели желанием отомстить за своих товарищей. Сомнений больше не оставалось – единственным способом революционной борьбы является террор. 2 апреля 1879 г. в самом центре Петербурга А. Соловьев стрелял в императора Александра II, покушение не удалось, его исполнитель погиб. Полиция решила во что бы то ни стало найти организаторов покушения. А. Михайлов, участвовавший в подготовке покушения, преследуемый полицией покидает Санкт-Петербург. Перемещаясь по городам юга Российской Империи Михайлов проводит мероприятия по подготовке к съезду оставшихся участников «Земли и Воли». В ходе этих поездок Михайлов знакомится с Андреем Желябовым. Этим двум людям было

суждено войти в историю российского революционного движения, как главным идеологам народовольческого террора. 15 июня 1879 г. в Липецке встретились ряд видных членов организации, в том числе А. Михайлов и А. Желябов, для обсуждения планов продолжения борьбы террористическими методами. В ходе встречи принято единогласное решение – основной мишенью революционеров должен стать российский император. 18 июня в Воронеже открывается очередной съезд «Земли и Воли» на нем снова выявились серьезные разногласия по поводу стратегии и тактики революционной борьбы. Несмотря на споры, полного раскола пока удалось избежать, хотя лидер сторонников мирной работы в деревне Георгий Плеханов демонстративно покидает съезд.

В июле 1879 г. у полиции вновь появился шанс задержать Михайлова. Из-за предательства одного из революционеров правоохранительные органы нападают не след Михайлова в Чернигове, но ему опять удается скрыться. Среди захваченных полицейскими вещей Михайлова обнаружены емкости с химическими реактивами для написания и проявления невидимых писем.

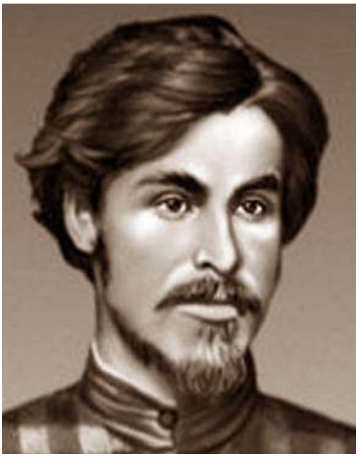
Тем временем разногласия между сторонниками террора и приверженцами мирных способов борьбы еще более усилились. 15 августа 1879 г. в пригороде Санкт-Петербурга прошел последний съезд «Земли и Воли». Родились две новые организации – «Народная Воля» и «Черный Передел». Именно «Народная Воля» стала символом борьбы революционеров в России в первой половине 80-х гг. XIX в., по сути дела эта организация и стала преемницей «Земли и Воли». Именно этим объясняется схожесть организационных структур обеих организаций, к тому же к их образованию имели отношение одни и те же люди. Программа новой партии была проста: подготовка заговоров, покушений на представителей власти, и организация народного восстания против самодержавия. При этом, хотя основная ставка была сделана на террор, народовольцы собирались вести и пропагандистскую работу во всех слоях российского общества. Основой новой организации стал

«Исполнительный комитет» (ИК), Главная роль в «Народной Воле» отводилась общему собранию, но все текущие дела решала администрация (или распорядительная комиссия) из 3 человек. В их обязанности, в том числе, входила и организация шифрованной связи. Так в уставе «Народной Воли», который был принят в конце лета 1879 г., сказано: «§ 29. Администрация устанавливает пароли и шифры, обязательные для всех членов Исполнительного комитета. Только этими установленными способами члены комитета могут вести деловую комитетскую переписку и записывать секретные сведения, адреса, фамилии и пр.». Основной системой шифрования стал цифровой гамбеттовский шифр, доставшийся по наследству от «Земли и Воли», но разумеется народовольцы применяли совершенно другие ключи. Вообще говоря у народовольцев в ходу было множество ключей к шифрам – отдельно для членов ИК, отдельно для периферии, свой личный ключ был почти у каждого подпольщика. В деятельности «Народной Воли» активно применялись стеганографические методы защиты информации, шифрованные письма довольно часто писались невидимыми чернилами между строк безобидного послания. Первоначально использовались довольно примитивные составы: раствор поваренной соли, сок лимона и молоко, все они проявлялись при нагреве письма, крахмал – проявляемый раствором йода и др. Однако революционеры быстро поняли, что такая маскировка не надежна и перешли к более сложным составам, однако вышеупомянутые вещества продолжали применяться в посланиях из мест заключения, где раздобыть более сложную «химию» было весьма сложно. Одним из основных реактивов применявшимся для написания невидимых писем был железисто-синеродистый калий, известный также под названием «желтая кровяная соль», для проявления использовался раствор полуторахлористого железа.

Исполнительный комитет был тем ядром вокруг, которого формировались группы и отдельные революционеры (которые получили название – агенты). В организации проводилась политика жесткой централизации всех структур и подчиненность их Исполнительному комитету.

Новая революционная организация сразу же приступила к активным действиям по подготовке покушения на Александра II, было организовано подпольное производство динамита, который было решено использовать для подрыва царского поезда. Одновременно разрабатывались три варианта операции под Москвой, Александровском и под Одессой. 19 ноября 1879 г. Степан Ширяев по сигналу Софьи Перовской взорвал заряд под проходящим мимо поездом. Состав сошел с рельс, но никто серьезно не пострадал. При этом атака не имела шансов на успех, так как в поезде ехала только царская свита, сам император проехал мимо раньше в другом поезде. Две другие операции так же закончились провалом – под Одессой взрыв был отменен, а в Александровске мина просто не взорвалась. Разумеется покушение под Москвой не могло не вызвать соответствующей реакции правоохранительных органов Российской Империи. В ноябре – декабре 1879 г. для «Народной Воли» началась полоса тяжелых неудач. Полиция произвела серию арестов, в руки правоохранительных органов попали ряд видных членов организации, в том числе и несколько участников покушения на Александра II включая С. Ширяева. В ходе этих мероприятий в руки правоохранительных органов попали весьма ценные материалы. Так, 4 декабря 1879 г., в один день с Ширяевым был арестован агент ИК С. Мартыновский. При обыске у него было обнаружено паспортное бюро народовольцев! При аресте среди прочего были изъяты: «пол листа писчей бумаги, сложенного в восьмую долю, на первой странице которого, разграфленной карандашом, вписано 11 лиц, которых имя и отчество означены заглавными буквами, а фамилии зашифрованы. Против фамилий поставлены в особой графе разные цифры… записная книжка с разными заметками… по разбору шифра, имеющегося в означенной книге… зашифровано следующее…». Далее следует перечень дешифрованных фамилий и адресов подпольщиков. Но на самом деле истинным хозяином большинства документов был народоволец В. Иохельсон. Они были зашифрованы на другом ключе. И здесь жандармские

криптоаналитики сделать ничего не смогли. Но и полученная из дешифрованных бумаг Мартыновского информация оказалась крайне полезной.



Степан Халтурин

Тем не менее народовольцы оправились от нанесенных потерь и борьба с самодержавием продолжилась. Прорабатывались новые варианты покушения на царя, для чего полным ходом шло тайное производство динамита. Подпольная типография продолжала печатать нелегальную литературу, в том числе очередные номера газеты «Народная Воля».

Однако и правоохранительные органы не сидели сложа руки. 18 января 1880 г. в Санкт-Петербурге полиция при проведении обычной проверки паспортов обнаружила подпольную типографию народовольцев. Революционеры оказали вооруженное сопротивление, при этом они сумели сжечь большую часть компрометирующих их документов. Но удар, нанесенный «Народной воле», был очень тяжелым, была потеряна типография, арестованы специалисты по печатному делу, в числе прочих была арестована член ИК С. Иванова. Но борьба продолжалась, 5 февраля 1880 г. в резиденции императора – в Зимнем дворце – раздается мощный взрыв, организованный Степаном Халтуриным. И это покушение не удалось, вместо царя погибают одиннадцать солдат караула и пятьдесят получают ранения.

Кстати, полиция не ограничивалась «Народной Волей» и стремилась разгромить и другие группы революционеров. Так 22 февраля 1880 г. в Киеве был арестован видный деятель «Земли и Воли», теперь организатор «Южнорусского рабочего союза» М. Попов. В этой организации была осуществлена неудачная попытка объединения членов организаций «Черный

Передел» и «Народная Воля». При аресте Попова были обнаружены два шифрованных письма. Их лично дешифровал помощник начальника Киевского губернского жандармского управления Г.П. Судейкин, который и захватил подпольщика. Кстати, Судейкин – один из самых известных борцов с революционерами в конце 70 – начале 80-х гг. XIX в., в частности именно он арестовал В. Осинского. Автором писем был И. Иванов, входящий в «Южнорусский рабочий союз». В перехваченных и дешифрованных жандармами письмах шла речь об устройстве по всей стране крестьянских бунтов и широком применении так называемого «фабричного террора». Это были серьезные доказательства противозаконной деятельности. В результате М. Попов и несколько его товарищей оказались на каторге. Однако этим правоохранительные органы не ограничились. В октябре 1880 г. опять же в Киеве были арестованы сменившие М. Попова на посту руководителей «Южнорусского рабочего союза» Е. Ковальская и Н. Щедрин. При них, в частности, были захвачены «письма, между строками которых написаны шифры, образовавшиеся от намазания письма хлористым железом». Кстати до образования «Союза» все его руководители входили в организацию «Черный передел».

В связи с увеличением количества террористических актов и особенно очередным покушением на Александра II власти приняли ряд мер по реформированию правоохранительной системы в целях повышения ее эффективности в борьбе с революционерами. В марте 1880 г. подписан указ «Об учреждении в Санкт-Петербурге Верховной распорядительной комиссии по охранению государственного порядка и общественного спокойствия» – временного чрезвычайного органа для объединения усилий всех судебных, административных, полицейских учреждений в борьбе с терроризмом. Главой комиссии назначается один из героев Русско-Турецкой войны 1877–1878 гг. граф М.Т. Лорис-Меликов. III Отделение собственной Его Величества канцелярии и Отдельный корпус жандармов подчиняются Главному начальнику верховной распорядительной комиссии «с целью сосредоточить в одних руках

высшее заведывание всеми органами, призванными к охранению государственного спокойствия, и внести в деятельность этих органов полное единство». В августе 1880 г. Лорис-Меликов становится министром внутренних дел, управление всей полицией Империи сосредотачивается в министерстве внутренних дел. В это же время упраздняются верховная распорядительная комиссия и III отделение Функции III-го отделения и командование отдельным корпусом жандармов переданы в МВД, где образуется департамент государственной полиции. В ноябре 1880 г. департаменты государственной и исполнительной полиции объединяются в один департамент государственной полиции. Первым директором департамента государственной полиции становится барон И.О. Велио. Фактически это был орган, не только руководящий розыскными действиями, но и призванный стоять на страже государственного строя. Именно в недрах этой организации впоследствии будет создана дешифровальная служба, которая будет работать против политических противников самодержавия. Здесь следует отметить, что шифровальная служба давно имелась в III отделении и Отдельном корпусе жандармов.

Тем временем осенью 1880 г. готовится судебный процесс по делу народовольцев, арестованных в конце 1879 – начале 1880 гг. Он получил название «процесс 16-ти террористов». Процесс открылся в Санкт-Петербургском военно-окружном суде 25 октября 1880 г. Его итогом стали два смертных приговора (А. Пресняков и А. Квятковский), главный участник московского покушения на царя С. Ширяев был приговорен к бессрочной каторге. Остальные получили различные сроки заключения.

Как и их предшественники, революционеры- народовольцы даже в заключении пытались продолжить борьбу и предпринимали попытки связаться с находившимися на свободе товарищами. В этом им помогли их адвокаты. Для защиты переписки использовался книжный шифр с цифровым ключом, где к порядковому номеру нужной буквы прибавлялась цифра четыре.

Как было замечено ранее, полиция активно и небезуспешно пыталась внедрить свою агентуру в революционные организации, однако и революционеры предпринимали попытки агентурного проникновения в правоохранительную систему Российской империи и вербовке (в основном на идеологической основе, путем агитации) ее сотрудников. Хотя масштабы этой деятельности не шли не в какое сравнение с операциями, проводимыми полицией, кое-каких успехов удалось добиться. Так, например, осуществлять связь с народовольцами, заключенными в Петропавловской крепости, помогал сын смотрителя Трубецкого бастиона Николай Богородский. Здесь использовался простой стеганографический прием: Богородский передавал в тюремную библиотеку книги, в которых условными значками отмечались нужные буквы письма. И заключенным требовалось только получить эти книги в свою камеру. Следует отметить, что такой способ связи с арестованными соратниками применялся народниками в первой половине 1870-х гг. И, к сожалению для революционеров, он был хорошо известен правоохранительным органам. Впоследствии Н. Богородский был разоблачен и оказался на каторге. Здесь следует отметить, что книги так же использовались для передачи сообщений и другим способом. Передаваемые послания прятались в их переплетах и обложках. Так С. Ширяев в ноябре 1880 г. просил товарищей переслать письмо его жене, заделав его в книгу, а группы «Черный передел» и «Освобождение труда» для своей связи с Россией широко использовали тот же способ. Целые брошюры революционеры прятали в корешках невинных на первый взгляд изданий.

Еще более серьезных успехов в вербовке тюремной охраны добился уже упоминавшийся в предыдущем разделе руководитель организации «Народная расправа» С.Г. Нечаев. В 1872 г. его выдала России Швейцария, и Нечаев был заключен в Алексеевский равелин Петропавловской крепости – самую строгую и секретную тюрьму Российской империи. Однако Нечаев не сдавался и стал вести пропаганду среди своих охранников. Успех был невероятным, к 1880 г. вся внутренняя стража равелина полностью подчинялась указаниям революционера. В ноябре 1880 г. в ра-

велине оказывается С. Ширяев, который под впечатлением масштабов деятельности Нечаева сразу дает ему возможность связаться с Исполнительным комитетом «Народной Воли». В начале декабря при участии охраны Алексеевского равелина началась переписка Нечаева и Ширяева с оставшимися на свободе товарищами причем, эти письма были зашифрованы неким цифровым шифром. Вероятнее всего это был цифровой гамбеттовский шифр, активно используемый организациями «Земля и Воля» и «Народная Воля».

Основатель тайного общества «Народная расправа» С.Г. Нечаев

Но самого большого успеха на поприще внедрения агентуры в правоохранительные органы добился А. Михайлов. В конце 1878 г. он познакомился с Николаем Клеточниковым и сумел внедрить его в центр борьбы с революционным движением – III отделение! Это уникальный факт из истории революционного движения России. Н. Клеточников в течение 2 лет служил сначала в III отделении, а затем (после его упразднения) стал сотрудником департамента полиции. На службе он сделал блестящую карьеру. Обладая превосходным каллиграфическим почерком, Клеточников занимался переписыванием для своего начальства самых секретных и важных документов розыска. А имея отличную память, он был в состоянии точно запомнить нужные сведения для передачи А. Михайлову. Михайлов самым тщательным образом оберегал свой источник информации, и лишь немногие революционеры имели доступ к Клеточникову. Он был причастен к высшим тайнам полиции, и этим обстоятельством народовольцы пользовались. Практически жандармам удавались только

случайные аресты, а долговременные акции заканчивались неизменным провалом. Среди поставляемой информации Клеточников передал народовольцам информацию о шифре, использовавшемся III отделением и корпусом жандармов, и о ключе к нему. Это был шифр многоалфавитной замены. В августе 1880 г. Клеточников на несколько дней был допущен начальством для шифровки секретных телеграмм. Этот факт впоследствии был специально отмечен в материалах «процесса 20 народовольцев», по которому проходили Михайлов с Клеточниковым. Скорее всего именно в это время Клеточников скопировал шифрматериалы и передал их революционерам. Кстати, данный ключ был введен в действие в 1871 г. решением шефа III отделения графа Шувалова и действовал, по крайней мере, до 1887 г. И это несмотря на то, что при аресте Клеточникова в 1881 г. следствию стало известно, что он по службе имел доступ к жандармскому шифру. Однако никакого значения этому в Департаменте полиции не придали и ключ не сменили. Сама же шифрсистема использовалась с 1861 г. до октября 1917 г. Кстати, такая ситуация, к сожалению, была характерна не только для МВД, в статье [Гольев, 2005] указано, что и в МИД Российской Империи ключи не менялись годми, и в некоторых случаях, даже тогда, когда выявлялись факты их компрометации. Это был не единственный случай утечки информации о шифрах полиции. В 1909 г. в своем парижском журнале «Былое» известный историк и революционер В.Л. Бурцев воспроизвел цифровой шифр Департамента полиции, действовавший в начале XX в. Интерес к шифрам секретной политической полиции оставался в революционных кругах России неизменным. Однако как следует из приведенного примера с арестом агента народовольцев, должного внимания к безопасному использованию шифров в департаменте полиции не уделялось. Правда тут следует отметить один важный момент – интерес к шифрам правоохранительных органов у революционеров был чисто академический, использовать эту информацию они могли лишь для возможного заимствования каких-то криптографических идей. Криптографы-революционеры занимались разра-

боткой шифров для защиты своей информации и практически не уделяли внимания криптоанализу. Но даже в случае появления в среде революционеров специалистов-криптоаналитиков вставала проблема перехвата шифрованных сообщений. Шифрованные сообщения правоохранительных органов передавались по телеграфу или пересылались с помощью фельдъегерской связи, возможность доступа к ним для революционеров была весьма затруднительна.

28 ноября 1880 г. полиция достигает крупного успеха, в полицейскую засаду попадает А. Михайлов. Арест одного из виднейших членов «Народной Воли» явился страшнейшим ударом по организации.

В 1881 г. продолжается усиление правоохранительных органов. Штаты полиции Санкт-Петербурга и Москвы, а также в провинции значительно увеличиваются. Увеличивается не только количество полицейских чинов, но и «возвысилось их служебное положение», «усиливались оклады содержания и средства, отпускаемые на канцелярские и хозяйственные нужды». Производятся и мероприятия по законодательному обеспечению борьбы против революционеров. 14 августа 1881 г. принято положение «О мерах к охранению государственной безопасности и общественного спокойствия», согласно которому министр внутренних дел может объявлять в любой части страны положение усиленной или чрезвычайной охраны, что значительно расширяет права местной полиции. Общей полиции предоставлено «право ареста по подозрению», наравне с жандармами. При объявлении местности на положении усиленной охраны губернаторы получают право издания обязательных постановлений. Они также могут передавать в военный суд дела о государственных преступлениях и утверждать приговоры по ним; имеют право закрывать любые торговые и промышленные предприятия, приостанавливать любые издания. В условиях чрезвычайной охраны полномочия губернаторов становятся еще шире. Они могут создавать сверхштатные военно-полицейские команды, налагать секвестр на недвижимое и арестовывать движимое имущество, задерживать любое лицо сроком до 3 месяцев, увольнять чи-

новников всех ведомств и прекращать деятельность городских и земских учреждений. Еще через некоторое время при министре учреждается Особое совещание в составе четырех высших чиновников МВД и министерства юстиции под руководством товарища (по современной терминологии – заместителя) министра. Министр внутренних дел единолично утверждает решение совещания об административной высылке лиц, подозревающихся в причастности к государственным преступлениям. Эти меры дали результаты, уже в начале 1881 г. начинается серия арестов народовольцев.

24 января 1881 г. из-за предательства народовольца Окладского полиция арестовала агента ИК Г. Фриденсона. Через 1 день в выставленную в его квартире засаду попадает видный член ИК А. Баранников. В тот же день на квартире последнего арестован другой член исполнительного комитета Н. Колодкевич. 28 января на квартире Колодкевича был арестован Н. Клеточников – глаза и уши народовольцев в департаменте полиции. На следующий день, там же в засаду попал Лев Златопольский – разработчик сокращенного цифрового гамбеттовского шифра, основной шифрсистемы народовольцев. Златопольский обладал выдающимися математическими способностями и хорошо разбирался в технике. Помимо разработки шифра он занимался решением проблем, возникавших при организации подкопов для взрыва царского поезда, в частности разрабатывал портативную буровую установку. Вообще его подпольная кличка «Механик» говорит сама за себя. О роли Златопольского в «Народной Воле» полиции стало известно от предателей Г. Гольденберга и В. Меркулова. В последствии Л. Златопольский был осужден на 20 лет каторги и первоначально содержался в Трубецком бастионе Петропавловской крепости. По совпадению именно туда весной 1882 г., был заключен его брат Савелий. С помощью надзирателя Провотворова братьям удалось наладить общение между собой и с товарищами, остававшимися на свободе. Однако 2 мая 1883 г. в камере Л. Златопольского при обыске были найдены записки, раскрывающие факт организации недозволенной переписки. В результате этого провала братья подверглись новым репрессиям. Льва сослали

на Карийскую каторгу, а Савелий, как и другие активные члены исполнительного комитета, попал в Шлиссельбург, где умер от чахотки в декабре 1885 г. Л. Златопольский умер в ссылке в феврале 1907 г.

Успехи полиции продолжались 27 февраля 1881 г., в полицейскую засаду попал руководитель «Народной Воли» А. Желябов. При аресте полиция обнаружила среди находившихся при нем бумаг два листка, исписанных цифровым шифром. Естественно давать какие либо пояснения по поводу обнаруженных у него документов Желябов не пожелал.

Исполнительный Комитет «Народной Воли»: С. Перовская, Н. Кибальчич, А. Желябов, М. Фроленко, Н. Морозов, В. Фигнер

Несмотря на то, что титанические усилия, которые прилагались полицией в борьбе с революционерами, приносили серьезные успехи главную задачу правоохранительным органам

Российской Империи выполнить не удалось. 1 марта 1881 г. в центре Санкт-Петербурга бомбами народовольцев Рысакова и Гриневицкого был смертельно ранен император Александр II. В ходе этого покушения первую бомбу метнул студент Николай Рысаков. Взрыв, произведенный ею, разворотил царскую карету, убил лошадей, не причинив императору ощутимого вреда. Но попытка переговорить лично с террористом прямо на месте взрыва стоила царю жизни. Другой народоволец – Игнатий Гриневицкий – кинул в его ноги еще одну бомбу. Взрыв оказался смертелен для Александра II, его убийцы, нескольких охранников и случайных прохожих. Все это кровавое зрелище произошло прямо на глазах у Рысакова. Под впечатлением увиденного, при умелом воздействии следователей, перед страхом неминуемого смертного приговора он сразу же после ареста стал давать самые откровенные показания, которые привели к быстрому разгрому народовольцев в столице. Среди прочего, Рысаков предоставил правоохранительным органом некоторые сведения о способах защиты информации, которыми пользовались народовольцы. Так, он сообщил о некоей московской учительнице, явку к которой он получил от А. Желябова. Ключом же к шифру для переписки с ней было слово «Лампада». В своих показаниях Рысаков ничего не сообщает о системе шифра, а следователи этим даже не интересовались. Скорее всего, они уже знали о чем идет речь. Вероятнее всего в этом случае был использован квадратный словарный шифр, который к тому времени был хорошо известен полиции. Также у Рысакова был обнаружен «железисто-синеродистый калий для добывания берлинской лазури». Как упоминалось ранее, это вещество использовалось народовольцами в качестве невидимых чернил. Однако в материалах следствия не дается объяснения предназначения синеродистого калия. Возможно, Рысаков планировал применить его в качестве яда на случай ареста, однако не успел им воспользоваться. Кстати в последствии при обнаружении у революционеров этого вещества в полицейских отчетах оно проходило как сильный яд, хотя жандармы давно знали о возможности использования синеродистого калия для тайнописи, однако

широко раскрывать этот факт не спешили. К тому же наличие у арестованных ядовитых веществ вносило дополнительный колоритный штрих в образ «ужасных террористов».

Вслед за убийством Александра II начался разгром революционеров, для правоохранительных органов стало делом чести отомстить за гибель императора. 10 марта в руках жандармов оказывается Софья Перовская – непосредственный организатор недавнего покушения. При ней также обнаруживают «листки бумаги с цифрами (по-видимому, шифром)». Но как и ранее Желябов, никаких объяснений Перовская не дает. Тем не менее, через 2 суток записки Желябова и Перовской дешифрованы жандармами. Это были собственноручные послания С. Нечаева из Петропавловской крепости, но в тот момент полицейским не удалось понять это. Сделать это удалось только в ноябре 1881 г. при следующих обстоятельствах. Еще августе не выдержав тюремного режима умер С. Ширяев. В казематах Алексеевского равелина оставалось всего два заключенных – С. Нечаев и Леон Мирский. В 1879 г. он, при содействии А. Михайлова, совершил неудачное покушение на шефа жандармов Дрентельна. Осенью 1881 г. Мирский не выдерживает и, стремясь хоть как-то облегчить свое положение, предает Нечаева. Только теперь стала понятной суть записок, захваченных при арестах Желябова и Перовской. Для правоохранительных органов информация Мирского стала потрясением. Заговоры революционеров происходят уже в самой секретной и наиболее охраняемой тюрьме Российской империи!

Убийство Александра II стало пиком деятельности народовольцев, после него организация была фактически разгромлена. 3 апреля 1881 г. были казнены 5 народовольцев, среди которых С. Перовская и А. Желябов. Многие другие были отправлены на каторгу. Хотя в течении ряда лет были попытки возродить организацию, но «Народная Воля» так и не оправилась от удара властей после покушения на царя. Однако борьба с самодержавием продолжилась, на смену «Народной Воле» пришли другие революционные организации.

5.3. Криптографическая деятельность революционеров в России. Агония «Народной Воли» 1881–1887 гг.

Убийство императора Александра II 1 марта 1881 г. стало переломным моментом в истории революционного движения в Российской Империи. Правительство ответило на это преступление народовольцев репрессиями и казнями. За 1881–1882 гг. были арестованы, казнены, отправлены на каторгу и в ссылку около 6 тыс. человек. Правоохранительные органы продолжали совершенствовать методы своей деятельности по борьбе с революционным движением. Особое внимание стало уделяться агентурной работе в среде революционеров. Хотя такая работа велась в 1860–1870 гг. весьма активно, но эффективность ее была далека от желаемой. Недостаточное развитие агентурной деятельности делало ее вспомогательным звеном в раскрытии преступлений. Главное место в ведении розыска отводилось дознанию. Такое положение дознания и розыска вело к тому, что нередко в постановлениях об аресте писали: «Арестовать впредь до выяснения причин ареста». Значит, арестовывали не потому, что собраны какие-либо улики, а для того, чтобы собрать эти улики. Недостатки агентурной разработки компенсировались за счет усиления полицейского надзора, стимулирования массового доносительства, облав и перлюстрации корреспонденции. Благодаря массовым обыскам и арестам полиция стремилась собрать необходимые вещественные доказательства (в том числе шифрованные письма, средства тайнописи, а если повезет и ключи к шифрам). Но революционеры быстро учились конспирации, и полиции нужно было постоянно совершенствовать средства и методы розыска. К тому же довольно часто во время облав в полицейские сети попадали случайные люди, не имеющие никакого отношения к революционной деятельности. После «близкого знакомства» с органами правопорядка у простых обывателей нередко надолго оставался на душе тяжелый осадок и общественное мнение, таким образом, отрицательно настраивалось по отношению к сотрудникам право-

Министр внутренних дел генерал-адъютант граф М.Т. Лорис-Меликов

охранительных органов. Агентурная работа позволяла наносить эффективные «точечные удары» и эта область деятельности привлекала внимание руководства правоохранительной системы России. В декабре 1880 г. органы МВД и юстиции проводят совещание по вопросам упорядочения розыска и дознания. На этом совещании прокурор Санкт-Петербургской судебной палаты В.К. Плеве (с апреля 1881 г. – директор департамента государственной полиции) отметил, что для проведения розыска необходим систематический, хорошо продуманный и строго выполняемый план действий. Плеве усматривал в розыске не просто сбор сведений через секретную агентуру и филеров, а видел в нем систему планомерных действий, направленных на обнаружение политических преступлений. Похожие мысли высказывал и петербургский градоначальник генерал Федоров. Он заявлял, что розыск, т.е. агентурное наблюдение, – необходимая принадлежность дознания, а последнее не имеет значения без розыска. По мнению генерала, сыскная часть, дающая агентов для производства розысков, является необходимым орудием в руках лица, производящего дознание, агенты сами по себе не имеют никакой цели и приносят пользу только при направлении их деятельности дознанием. О важности повышения эффективности агентурной работы указывал и министр внутренних дел граф М.Т. Лорис-Меликов.

В «Инструкции С.-Петербургскому губернскому жандармскому управлению и градоначальнику» он писал, что «секретные изыскания должны производиться параллельно с дозна-

ниями и служить последним в раскрытии преступлений главнейшим подспорьем». В дальнейшем увидим, что с 1880-х гг. полиция значительно активизировала свою деятельность по внедрению агентов в революционные организации, что привело к крайне негативным для них последствиям. Что касается криптографической деятельности, то внедренная агентура и завербованные революционеры поставляли полицейским криптоаналитикам информацию об используемых системах шифрования, средствах тайнописи и организации шифрованной связи. Также аресты и обыски, проводимые по информации, полученной от агентуры, давали дешифровальщикам материал для работы. В тот период революционеры старались не доверять почте, а предпочитали передавать информацию через курьеров с оказией и др., поэтому проблема перехвата шифрованной переписки революционеров была для правоохранительных органов Российской Империи весьма серьезной.

Теперь вернемся к событиям, происходившим после 1 марта 1881 г. Главной целью полиции продолжала оставаться «Народная Воля». Аресты произведенные сразу после покушения нанесли организации колоссальный удар, но полицейским этого было недостаточно. Они хотели полностью искоренить народовольцев. При арестах 1881–1882 гг. в руки полиции попало немало шифрованных писем народовольцев. Например, при аресте в марте 1881 г. Михаила Фроленко в его вещах было найдено длинное шифрованное письмо в виде последовательного числового ряда. Иногда при захвате шифрпереписки случались и весьма курьезные случаи. В августе 1881 г. в Москве попал в полицейскую засаду студент А. Кирхнер. При последующем обыске его квартиры был обнаружен обширный шифрованный список. В нем числилось 15 фамилий неких лиц с подробным перечислением адресов и примет. Криптограмму жандармы сумели дешифровать и тотчас начались аресты. К изумлению их, задержанные оказались совсем не народовольцами, а наоборот – секретными сотрудниками полиции! Как выяснилось впоследствии революционеры предприняли попытку создания собственной контрразведки.

У ее истоков стоял член исполнительного Комитета (ИК) «Народной Воли» Петр Теллалов, организация получила название «Революционная полиция», секретарем в ней и являлся Кирхнер. Одной из задач «Революционной полиции» стала организация наружного наблюдения за лицами, подозреваемыми в сотрудничестве с правоохранительными органами. В результате этой деятельности, начатой московскими народовольцами, и был получен упомянутый список. Надо заметить, что и у самого «начальника революционной контрразведки» с конспирацией было не все благополучно. При задержании в декабре 1881 г. П. Теллалова жандармы обнаружили частично зашифрованное письмо, предназначавшееся находящемуся под стражей Александру Михайлову.

Планировали еще остававшиеся на свободе народовольцы и более масштабные операции, нежели слежка за агентами полиции. Летом 1881 г. народовольцы решили создать организацию по освобождению высланных в Сибирь товарищей. С этой целью в августе 1881 г. туда отправились Ю. Богданович и И. Калюжный. К зиме была организована целая цепь тайных убежищ и ночевок для готовящих свой побег революционеров. Организация получила название «Общество освобождения» (другое название «Сибирский Красный крест»). Она имела свой подробный устав, содержавший 55 параграфов. В нем была четко прописана структура новой организации, ее подчиненность ИК «Народной Воли», имелись пункты, которые требовали сохранение революционерами абсолютной тайны и применение шифров в их переписке. Интересно отметить, что наряду со ставшими «стандартными» гамбеттовскими шифрами, снова стали использоваться квадратные шифры. Связано это было очевидно с притоком молодых революционеров, не имевших достаточных навыков работы с гамбеттовской системой.

Увы, 18 декабря 1881 г. в Москве были арестованы супруги Валентин и Клавдия Яковенко – видные члены организации Богдановича. Согласно материалам следствия при них обнаружено: «четыре листа шифрованных записок» и чемо-

дан «с весьма достаточным числом» шифрованных писем. Это оказались чрезвычайно ценные для правоохранительных органов трофеи. В результате дешифрования полученных материалов полиция получила адреса в Казани, Екатеринбурге, Тюмени, Томске, Красноярске и других городах. Это были явки «Общества освобождения». Так успех криптоанлитиков позволил разгромить достаточно серьезную революционную организацию. Впоследствии, весной 1882 г., был арестован и сам Юрий Богданович. Среди его бумаг оказался рецепт томской аптеки. Эта улика доказала его поездку по Сибири, а позже удалось доказать и организующую роль в создании «Сибирского Красного креста». Интересно отметить, что 10 номер газеты «Народная Воля» сообщил, что уже при аресте В. Яковенко полиция знала ключ к шифрованным спискам. Но этот факт так до конца и не прояснен. Судя по документам полиции, провал революционеров произошел достаточно случайно и только в результате обысков жандармы вышли на верный след, кстати, помимо всего прочего полиции достался и упомянутый устав «Общества освобождения».

К концу 1881 г. у оставшихся на воле народовольцев все больше и больше появлялось недоверие к надежности используемых ими шифров. Все чаще при многочисленных арестах революционеров в руки полиции попадали их криптограммы и все успешнее криптоаналитики правоохранительных органов их дешифровали. Это происходило не смотря на то, что штатное дешифровальное подразделение в МВД до сих пор отсутствовало, но работавшие «на общественных началах» специалисты делали свое дело весьма эффективно. Фактически народовольцы попадали в своеобразный замкнутый круг. Очередные аресты приводили к попаданию в руки полиции шифрованных писем и записок, их дешифрование нередко давало правоохранительным органам информацию, на основании которой производились новые аресты.

В феврале 1882 г. в Санкт-Петербурге начался очередной судебный процесс над народовольцами, известный как «процесс двадцати». На скамье подсудимых оказались Михайлов,

Баранников, Морозов, Колодкевич, Фроленко, Исаев, Клеточников, Златопольский и многие другие члены организации «Народная Воля». И опять революционеры пытаются наладить с волей. Это удается сделать А. Михайлову через своего адвоката Е. Кедрина. Михайлов писал Анне Корба не только товарищу по борьбе, но и своей возлюбленной. Она сохранила эти письма, а зря! При аресте в июне 1882 г. пять таких шифрованных записок попали в руки полиции, таким образом, дав информацию о связях заключенных народовольцев с волей. В ожидании суда А. Корба сама сумела передать ряд шифрованных писем Вере Фигнер – единственному оставшемуся на свободе члену ИК. А. Корба в этих письмах применяла буквенный гамбеттовский шифр. Вероятно, имел возможность писать товарищам на волю еще один из проходящих по процессу 20-ти народоволец – Николай Морозов.

Тем временем аресты продолжались, и полиция получала в свое распоряжении новые шифрованные письма. 6 февраля 1882 г. в Москве попал в засаду на проваленной явке народовольцев Яков Стефанович. Он был членом организации «Черный Передел» и жил в эмиграции. Весной 1881 г. Стефанович стал все более сходиться с народовольцами, и, наконец, в сентябре, покинув Женеву, отправился в Россию для продолжения активной борьбы. При аресте у него было изъято: «…Несколько писем, между которыми обращает на себя внимание весьма пространное письмо из-за границы… Причем многие места этого письма зашифрованы». Стефанович уклонился от разъяснения как зашифрованных мест письма, так и его содержания. Уже 15 февраля 1882 г. Стефанович попытался через своего надзирателя отправить письмо в Женеву. Он не подозревал, что копия тут же легла на стол жандармского следователя. Адресовалось послание Л. Дейчу, чье письмо и было конфисковано при аресте у Стефановича. В этом письме Стефанович сообщал о своем провале и предостерегал друга не ехать в Россию. Также он предполагал и о том, что специалисты из полиции уже дешифровали письмо Дейча. Под контролем полиции эта переписка продолжалась довольно долго, при этом использовались

сипатические чернила. Стефанович использовал номера газеты «Московские новости», где химией наносил свои криптограммы. В конце каждого подобного письма ставилось слово «конец» для обозначения полного окончания химического текста. Это слово присутствует в большинстве народовольческих писем, написанных с использованием стеганографии, попавшим в руки правоохранительных органов.

Я. Стефанович, впоследствии, был прямо обвинен своими бывшими товарищами в предательстве. В частности его обвиняли в выдаче жандармам упомянутого руководителя «Общества освобождения» Ю. Богдановича. Правда, прямых доказательств предательства Стефановича до сих пор не обнаружено, но некоторые косвенные улики имелись. В частности остается фактом, что полиция разрешила ему вести обширную переписку с Дейчем. Также известно, что Стефанович имел в тюрьме доверительные беседы с директором департамента государственной полиции Плеве, и составил для него подробнейший отчет о положении русской революционной эмиграции. Да и суд приговорил его «всего» к 8 годам каторги. Другие даже менее видные революционеры получали гораздо большие сроки.

Между тем продолжалось организационно-правовое совершенствование деятельности МВД в целях повышения ее эффективности. Так 1 марта 1882 г. министром внутренних дел утверждено положение «О негласном полицейском надзоре», где указывается, что «в отличие от надзора гласного, как меры пресечения и наказания, негласный надзор является мерой превентивной, способом предупреждения государственных преступлений, посредством тайного наблюдения за лицами сомнительной благонадежности», а 16 июля 1882 г. высочайше утверждена инструкция командиру отдельного корпуса жандармов «товарищу министра внутренних дел, заведующему государственной полицией». По этой инструкции товарищу министра подчинялись не только жандармские чины, но и все чины общей полиции. При этом шефом жандармов являлся министр внутренних дел.

Уцелевшие народовольцы еще пытались продолжать террор: в марте 1882 г. С. Халтурин и Н. Желваков прямо на улице убили одесского прокурора Стрельникова. Оба были судимы военно-полевым судом и повешены. Летом 1882 г. в России оставалась на свободе единственный член ИК – Вера Фигнер. Все остальные были арестованы или эмигрировали. Переезжая из города в город, Фигнер пыталась сплотить разрозненные группы народовольцев и воссоздать «Народную Волю», в ее былом величии.

Но 20 декабря 1882 г. «Народная Воля» получила очередной фатальный удар. В Одессе был арестован член военного центра «Народной Воли» Сергей Дегаев. Спасая жену, которая была арестована одновременно с ним и от страха или растерянности рассказала полиции все, что знала, Дегаев согласился на сотрудничество с инспектором секретной полиции Г.П. Судейкиным, главным борцом с революционерами. Судейкин возглавлял агентуру петербургской охранки, а после убийства Александра II фактически весь российский политический сыск. За 4 месяца Дегаев выдал военный центр партии «Народная Воля» и местные военные группы. Арестовано было более 200 человек, в том числе Вера Фигнер – последний член Исполнительного комитета. Она была арестована в феврале 1883 г. в Харькове. Народовольцы успели очистить ее квартиру и переправили хранящийся у Фигнер архив организации в Париж. Но два документа остались на хранении народовольца Владимира Чуйко. После его ареста в этом же месяце они оказались в распоряжении жандармов, а те смогли их дешифровать, одно из двух писем народовольцев, как важная улика, было приобщено к материалам «процесса 14-ти» (Фигнер и др.), состоявшемся в сентябре 1884 г.

После всех этих арестов Дегаев стал, по существу, лидером партии. Естественно он был полностью в курсе организации шифрованной связи, знал какие шифры и средства тайнописи используются революционерами, мало того некоторых из них он сам обучал ведению конспиративной переписке. Совершенно очевидно, что все эти сведения стали достоянием полиции.

В новом 1883 г. продолжилось реформирование МВД. Департамент государственной полиции переименовывается в Департамент полиции и разбивается на несколько делопроизводств с резко очерченными функциями.

Первое (распорядительное) делопроизводство – ведает вопросами назначения, увольнения награждения сотрудников полиции.

Второе делопроизводство (законодательное) – «занимается организацией полицейских учреждений во всех местностях Империи», а также «предупреждением и пресечением явного соблазна, разврата в поведении, по прекращению пьянства и нищенства».

Третье делопроизводство – собирает негласным путем сведения о людях, изъявивших желание издавать газеты, журналы, открывать частные школы, выехать за границу, а также поступить на государственную службу. Ведет переписку по доносам и заявлениям частных лиц, по преступлениям общеуголовного характера, контролирует розыск преступников.

Четвертое делопроизводство – организует работу Особого совещания при министре внутренних дел и контролирует проведение дознаний по делам о государственных преступлениях.

Пятое делопроизводство – наблюдает за исполнением «состоящихся решений по делам о государственных преступлениях». В нем имеется справочный стол со списками и фотографиями лиц, «обративших на себя внимание правительства».

Шестое делопроизводство (создано в 1894 г.) – контролирует изготовление и хранение взрывчатых веществ, соблюдение винной монополии, законодательства о евреях, а также занимается проблемами взаимоотношений между владельцами предприятий и рабочими.

Особый отдел (создан в 1898 г.) – руководит заграничной внутренней агентурой, а также вновь создаваемыми розыскными отделами. В функции Особого отдела входит обобщение перлюстрации писем, систематизация и выемка противоправительственных книг и брошюр. В отдел собирается вся информация, полученная оперативным путем. Именно в рамках этого

подразделения наконец в МВД появилась штатная дешифровальная служба, которая сразу же приступила к работе по анализу многочисленных шифрованных писем различных революционных организаций. Но об этом несколько позже.

18 февраля 1883 г. для производства дел по обвинениям в государственных преступлениях в Министерстве внутренних дел учреждается судебный отдел**.** 3 декабря 1883 г. утверждено положение «Об устройстве секретной полиции в Империи»**,** которым предусматривалась возможность создания розыскных отделений во главе с офицером корпуса жандармов, назначаемого по выбору директора департамента полиции. Иногда эта должность могла замещаться гражданским чиновником департамента полиции. Руководство деятельностью охранно-розыскных отделений возложено на уже знакомого нам инспектора секретной полиции подполковника Г.П. Судейкина. Основой деятельности новых подразделений становится агентурная работа, суть которой по замыслу Судейкина: «1) возбуждать с помощью особых активных агентов ссоры и распри между различными революционными группами; 2) распространять ложные слухи, удручающие и терроризирующие революционную среду; 3) передавать через агентов, а иногда с помощью приглашений в полицию и кратковременных арестов, обвинения наиболее опасных революционеров в шпионстве; вместе с тем дискредитировать революционные прокламации и разные органы печати, придавая им значение агентурной, провокационной работы».

Как было сказано ранее благодаря предательству Дегаева полиция арестовала многих революционеров, при их арестах захватывались шифры и лишь некоторые принимали меры по уничтожению компрометирующих материалов. Так в марте 1883 г. был арестован М. Ашенбреннер. Много позже он вспоминал: «Арестован я был при исключительно благоприятных обстоятельствах. При мне были рекомендательные письма и небольшая тетрадка из очень тонкой почтовой бумаги со списком 400 офицеров по городам. Все это было зашифровано по способу Гамбетты. Подобрать ключ к зашифрован-

ному очень трудно, но возможно; стоит только удачно подставить при выкладках, например, название города и, если в тексте есть это слово, то ключ найден. Поэтому фамилии и города в письмах мы зашифровывали другим ключом. Как раз моя тетрадка с фамилиями и не могла быть так зашифрована. Это меня страшно беспокоило и я… вознамерился выучить все эти списки наизусть… В момент ареста при мне находились еще уцелевшая часть тетради с 200 фамилиями…». Однако Ашенбреннер успел сжечь остатки документов и тем спасти многих от неизбежного ареста. Кстати о необходимости уничтожать компрометирующие документы прямо говорится в некоторых руководящих документах «Народной Воли», в частности в феврале 1882 г. центральный военный кружок «Народной Воли» выработал устав «Частного офицерского кружка» и инструкцию для его членов. Ее §15 гласил: «Шифрованную переписку надо уничтожать немедленно по миновании надобности, или владелец такой переписки должен переписывать ее по собственному ему одному известному паролю». Но, к сожалению для революционеров, не все соблюдали конспирацию тщательно.

Несмотря на существенные успехи в борьбе с революционным движением, полиция иногда получала от недобитых народовольцев чувствительные удары. Ценой предательства Дегаев получил возможность выехать с женой в Париж, якобы для выяснения замыслов русской эмиграции. Там Дегаев «раскрылся» в содеянном перед заграничным представителем Исполнительного комитета Л.А. Тихомировым. Члены Исполнительного комитета посчитали возможным сохранить жизнь Дегаеву в том случае, если он спасет известных Судейкину революционеров и организует его убийство. Оставив заложницей свою жену, Дегаев возвратился в Санкт-Петербург, где заманил 16 декабря 1883 г. к себе на квартиру Судейкина, где его убили народовольцы Н.П. Стародворский и В.П. Конашевич. Вслед за этим при содействии народовольцев Дегаев скрылся за границу. Однако методы Г.П. Судейкина по внедрению агентуры и вербовке арестованных революционеров активно применялись полицией и далее.

В это же время в Швейцарии произошло весьма важное событие. Там образовалась группа «Освобождение труда», первая ставшая нести идеи К. Маркса в Россию. Именно марксисты вскоре превратились в основную «головную боль» для правоохранительных органов Российской Империи. Группу возглавил Г. Плеханов, в нее входили ряд бывших участников организаций «Земля и Воля», «Черный передел» и «Народная Воля», в частности В. Засулич, Л. Дейч. Таким образом, была обеспечена самая тесная преемственность народников и первых русских социал-демократов. Естественно, что конспиративный аппарат новой организации был основан на лучших традициях землевольцев и народовольцев. Образовавшись в конце 1883 г., организация постоянно пыталась установить связи с Россией для распространения своих взглядов. Первоначально этим занимался Л.Дейч, а после его отъезда в Россию и ареста там в 1884 г., за организацию сношений с Родиной стал отвечать П. Аксельрод. Вскоре группа Плеханова наладила первые связи с молодыми российскими социал-демократами, входящими в кружкок Димитра Благоева. Его участник Василий Харитонов вспоминал, что при разгроме их кружка в руки следователей попало одно из писем группы «Освобождение труда». Послание было написано химическими чернилами между строк невинного текста. «Шифр этого письма остался жандармам неизвестен, они так и не разобрали зашифрованного адреса…» – замечает Харитонов, при этом отмечая, что переписка между Петербургом и Женевой была «приличная», но лишь одно письмо попало в руки полицейских. По всей вероятности для шифрования этого письма использовался гамбеттовский шифр, а неудача полицейских криптоаналитиков объяснялась малым количеством перехваченного материала.

А в России полиция продолжала добивать «Народную Волю» и жандармские криптоаналитики вносили немалый вклад в успехи правоохранительных органов. В марте 1884 г. в Киеве провалилась подпольная народовольческая типография, хозяином которой являлся Михаил Шебалин. Как указано в жандармских протоколах обыска, при его аресте было изъято: «5 писем на 8 почтовых листах среднего формата, писанные в

Василий Караулов
член «Народной Воли»,
один из ее руководителей
после арестов 1881 г.

два текста: один из которых обыкновенный, а другой химическими чернилами и, очевидно, восстановлен составом желтого цвета, частью зашифрованные…». Так же был арестован один из новых руководителей «Народной Воли» В. Караулов, у которого был обнаружен пузырек с полуторахлористым железом. Полиция уже с конца 1870-х гг. превосходно знала, это вещество является проявителем химической переписки. Повсеместно при арестах революционеров у них обнаруживали упомянутый реактив.

Дело дошло до того, что с середины 1880-х гг. даже все письма заключенных в царских тюрьмах стали проверяться полуторахлористым железом на предмет обнаружения в них химического текста. Полицейские специалисты дешифровали эти письма, зашифрованные цифровым шифром. Автором большей их части был Петр Якубович – один из руководителей организации «Молодая Народная Воля»[1]. Эти письма стали весомым доказательством на киевском процессе народовольцев в ноябре 1884 г. Но самым ценным для полиции оказалось най-

[1] Эта организация действовала в Санкт-Петербурге, Москве и ряде других городов Российской Империи в 1883–1884 гг. первоначально была оппозиционной группировкой по отношению к заграничному центру «Народной Воли» и ее представителям в России. Защищала децентрализацию и автономию в организационном строе партии. Считала необходимым ввести в программу и в практику аграрный и фабричный террор. В последствии в результате долгих переговоров единство в «Народной Воле» было восстановлено.

денное в бумагах Шебалина письмо Константина Степурина от 18 февраля 1884 г., адресованное в Киев из Петербурга. Степурин представлял центр «Народной Воли». Помимо прочего Шебалину сообщался адрес для переписки с варшавскими революционерами, и указывался ключ к их шифру – слово «Сосед». Речь шла о партии «Пролетариат», это была польская организация, созданная Людвиком Варыньским. Она имела тесные связи с народовольцами и использовала аналогичную (гамбеттовскую) систему шифрования. В марте 1883 г. в Варшаве был организован центральный комитет «Пролетариата», который утвердил различные шифры – для переписки членов ЦК, для низовых кружков, для связи с группами в Петербурге, Москве и Киеве (там имелись большие диаспоры поляков). Среди этих ключей можно найти слова «Гранит» и «Шелгунов». Польские революционеры использовали русскоязычные ключи к шифрам потому, что большинство из них долгое время жили в России, а, к примеру, Людвик Варыньский вообще родился на Украине и говорил на родном языке с ощутимым акцентом.

Полученная правоохранительными органами информация позволила варшавской полиции разгромить организацию. При задержании лидеров «Пролетариата» Варыньского, а затем Куницкого жандармы изъяли ряд зашифрованных писем. Но главный удар был нанесен при аресте мирового судьи Петра Бардовского, в варшавской квартире которого хранился архив «Пролетариата». Среди его многочисленных бумаг полиция обнаружила перечень ключей к шифрам подполья и обширные списки членов партии во всех городах Польши. Дешифрование полученных материалов привело к полному разгрому «Пролетариата». По решению состоявшегося в Варшаве в декабре 1885 г. суда, четверо революционеров было повешено, в том числе Куницкий и Бардовский. Людвик Варыньский, арестованный раньше других, был заточен в Шлиссельбургскую крепость, где вскоре погиб.

Несмотря на очередные успехи правоохранительных органов, попытки воссоздать «Народную Волю». Одна из самых

заметных принадлежит легендарному русскому революционеру Герману Лопатину. Лопатин родился в 1845 г. Революционной деятельностью начал заниматься во второй половине 1860-х гг. Не однократно арестовывается, бежит, скрывается за границей, возвращается, снова аресты и побеги. Лопатин был выдающимся человеком своего времени. Он был знаком с Марксом и Энгельсом. Он один из переводчиков первого тома «Капитала» Маркса, вышедшего в России в 1872 г. В 1883 г. Лопатин в очередной раз бежал заграницу, но в том же г. вернулся в Петербург энергично восстанавливать рассыпавшиеся организации народовольцев и вдохнуть новую жизнь в заглохшую деятельность «Народной Воли». Лопатин предпринял ряд поездок вглубь страны, сколачивал актив партии и сумел добиться определенных результатов. Но 6 октября 1884 г. произошел страшный провал. На Невском проспекте Петербурга Лопатина молниеносно арестовали сотрудники полиции. Вот как описывает этот случай народоволец Б. Д. Оржих: «Герман Лопатин, будучи хорошим теоретиком, человеком высокой культуры и глубокой эрудиции, умевший импонировать представителям всех классов интеллигентного общества, был сущим ребенком в конспиративном отношении. Разъезжая по всей России,, собирая и объединяя различные революционные и полезные общественные элементы, он заносил в свою книжку-листовку всех и все под их настоящими именами, большею частью с самыми непростительными для революционера-организатора комментариями и характеристиками, как, например, «Ейск, Лука Колегаев–банкир революции, дал три тысячи, обещал еще», «Луганск–такой-то–техник, прекрасно приготовляет бомбы», и далее характеристики целого ряда членов; группы, и т.д. и т.п. Почти все центральные группы главных городов России, где он успел побывать, были записаны у него в книжке целиком с их адресами, паролями, шифрами и др. Он наивно мечтал и упорно утверждал, что проглотит все записи в случае ареста. Но жандармы, к тому же предупрежденные московским провокатором Белино-Бржозовским, оказались хитрее и вырвали у него листки с адресами прежде, чем он дал себе отчет, что он арестован.» В тот же день схватили и Неонилу

Салову – хранительницу партийного архива и члена руководящего ядра «Народной Воли». У нее изъяли зашифрованную адресную книжку с 20-ю криптограммами и несколько писем П. Якубовича. Путем сопоставления бумаг Лопатина и Саловой их удалось полностью дешифровать. Опять начались масштабные аресты. Они проводились в 32 городах, в результате вся организация снова была полностью дезорганизована. И опять крупный успех был достигнут во многом благодаря работе полицейских криптоаналитиков. Всю оставшуюся жизнь Лопатин не смог себе простить этого провала, виновником которого он стал благодаря своей самонадеянности. Лопатина судили в 1887 г. и приговорили к смертной казни, которая была заменена бессрочной каторгой. Всего Лопатин находился в заключении 18 лет в одиночной камере Шлиссельбургской крепости, освободили его в 1905 г. Будучи тяжелобольным человеком, от революционной деятельности отошел и занимался литературной работой.

П. Якубовичу удалось избежать первой волны арестов. 3 ноября 1884 г. оставшийся на свободе он пишет в Женеву Л. Тихомирову. Предчувствуя свой скорый провал, он торопился передать заграничному центру народовольцев все оставшиеся связи: «В случае моего ареста с Вами вступит в переписку … один человек… С ним ключом Вашим пусть будет на первое время хоть «Народная Воля», одни гласные. На днях арестовали и выпустили некоего Пирогова…, потому что нашли его адрес у какого-то Лоренса в Одессе, хотя и зашифрованный, но разобранный ими. Меня всегда смущало это обстоятельство, что они умеют разбирать шифры. Я вот бы что предложил вам, если согласитесь: будем вперед шифровать так, чтобы каждая четвертая цифра ничего не значила. Дольше, но зато вернее…». Тогда же Якубович послал одной из провинциальных народовольческих групп поистине знаковое послание: «Перед глазами столько примеров гибели людей от сохранения писем и расшифровываемых полицией адресов, что страшно делается поневоле…». Наконец-то наступает осознание, что шифры революционеров вскрываются полицией и очередной подпольщик приходит к выводу о па-

Оржих Борис Дмитриевич

губности хранения шифрованной переписки. Но, увы, осознание пришло слишком поздно. В ноябре 1884 г. Якубович был арестован. Интересно отметить, что приемам шифрования и использованию средств тайнописи (все того же синеродистого калия) Якубовича обучил никто иной, как предатель Сергей Дегаев. Не мудрено, что все его письма, оказавшиеся в руках жандармов, были ими успешно дешифрованы. Кстати сам Якубович после ареста поделился со следователями криптографической информацией. Он указал на состав симпатических чернил и отметил, что криптограммы революционеров обычно имели тогда вид числовых рядов, а ключами к ним были различные слова или фразы.

Одну из последних крупных попыток «реанимировать» «Народную волю» предпринял упомянутый выше Борис Оржих. Понимая, что работать в крупных городах страны (Петербург, Москва, Киев и Одесса) полиция не даст, так как у нее уже имелся большой опыт в борьбе с революционерами Оржих решил основать новую организацию в провинции на юге России. Основными центрами деятельности народовольцев стали Новочеркасск, Таганрог и Ростов-на-Дону, там он объединил сеть кружков и отдельных лиц, а вскоре организовал две типографии – в Таганроге и Новочеркасске. В орбиту новой организации попали так же Екатеринослав и Харьков – дело ставилось на широкую ногу. Были установлены связи с Санкт-Петербургом и Москвой. В сентябре 1885 г. в Екатеринославе удается провести съезд организации. Оржих постоянно переписывался с заграницей, в основном с Л. Тихомировым. Ему и его товарищам удалось издать очередной 11/12

сдвоенный номер газеты «Народная Воля», была организована динамитная мастерская, где по рецептам Н. Кибальчича изготовили бомбы. Начали вынашиваться планы очередных покушений на руководителей Российской империи. Здесь следует отметить, что Оржих был сторонником продолжения террора. Естественно конспирации уделяется огромное внимание. При этом наконец-то пришло понимание, что шифры, используемые революционерами, не являются достаточно стойкими. По этому поводу приведем воспоминания самого Оржиха. В конце 1885 г. он встретился со своим старым товарищем, видным деятелем «Народной Воли» периода ее заката, Сергеем Ивановым. В последствии Оржих вспоминал: «Он попросил, чтобы я ему дал… ряд адресов… для писем и явок. Это мне не понравилось. Не потому, что я хоть на миг мог питать даже тень недоверия к нему. Нет. А потому, что у нас, в нашей южной компании, после опыта многих провалов было органическое отвращение к старым методам записи адресов. У каждого из нас была книжка со своими индивидуальными отметками. Например, в таком роде записывал я: «Либералы, банка и плуг, твердый». Это означало для меня: «Симферополь, Крестьянский банк, Каменецкий»… Правда, иногда случалось, что не сразу расшифруешь какую-нибудь тарабарщину; но напрягши память и путем наведений, все-таки доберешься до сути. Когда Сергей Иванов попросил у меня адреса, я знал, что он шифрует по прежнему. Я сказал ему, что шифровка не представляет гарантии, чт.е. много данных, что жандармы расшифровывают все цифровые шифры.

– Это вздор, – настаивал он, – они расшифровывают только очень первобытные шифры, а главным образом, когда предатели выдают их им. У меня двойной способ, который совершенно невозможно расшифровать.

Однако я настаивал, чтобы он заучил хорошо адреса и уничтожил свои записи, что он и обещал, но впоследствии не успел исполнить».

Надо отметить, что шифрование с помощью опорных слов (фактически это весьма оригинальный вариант использования жаргонного кода) был весьма надежен, но сильно за-

висел от человеческого фактора, забывчивому человеку такой способ не годится. Даже обладающий хорошей памятью человек может таким образом зашифровать весьма небольшой объем информации**.** И наконец способом Оржиха удобно защищать информацию при ее хранении, т.е. для себя, при передаче другому лицу возможны большие трудности при расшифровании. Что же касается «двойного шифра» С. Иванова, то, очевидно, речь идет о перешифровке с помощью разных систем шифрования. Например, шифртекст, полученный с помощью классического для народовольцев гамбеттовского шифра, перешифровывался например квадратным шифром.

Итак казалось «Народная Воля» возрождается. Однако правоохранительные органы тоже не собирались почивать на лаврах. В конце 1885 г. новой организации наносится первый крупный удар. Один из арестованных ранее народовольцев, Антон Остроумов, сидевший в Петропавловской крепости, сообщил правоохранительным органам, что он передал в Ростове-на-Дону типографский шрифт Акиму Сигиде, одному из сотрудников таганрогской типографии. 23 января 1886 г. полиция произвела обыск на квартире Сигиды. Подпольная типография была разгромлена, последовали многочисленные аресты в Таганроге и Ростове-на-Дону. Эти события вызвали у революционеров сильное опасение за судьбу и безопасность новочеркасской типографии, в которой была закончена и сбрюширована книга «Борьба общественных сил в России». Были предприняты действия по рассредоточению имевшихся материалов. Здесь следует отметить, что полицейские допустили серьезный промах. Предоставим слово народовольцу А.А. Кулакову: «Вечером 23 января 1886 г., по обыкновению, я направился в типографию, имея в кармане два шифрованных письма, полученных в тот день из-за границы… Подошел к домику, где была типография… Повернув кольцо, я стал открывать калитку, которая несколько приоткрылась, а потом опять прикрылась. Я сильнее нажал на калитку, которая, несколько приоткрылась, и в ней появилась физиономия полицейского-городового, изрекшая: «Не велено пущать». Гово-

рить о том, как я был оглушен этой короткой фразой, излишне. Повернувшись, я сначала медленно, а затем усиленным шагом направился на окраину города, на Касперовку, в квартиру рабочего Тита. Там я написал письма с извещением о провале типографии и не медля отправил их. На следующий день предупредил всех, кого следовало, чтобы меня никто не посещал. Предупреждение оказалось нелишним, так как чуть ли не на следующий день я убедился, что за мной учрежден хотя и наивно-грубый, но неуклонный надзор. По прошествии месяца у меня был произведен безрезультатный обыск, и меня оставили на свободе. Через месяц обыск повторился с теми же результатами, и только 30 апреля 1886 г., после третьего, тоже безрезультатного, обыска, я был арестован». Таким образом, удалось частично локализовать ущерб от провала. Однако полиция наносила все новые удары. В январе 1886 г. был арестован Сергей Иванов, шифрованные адреса и явки, данные ему Оржихом, как мы помним из воспоминаний последнего, Иванов их уничтожить не успел. В результате их дешифрования полицейские получили ценную информацию.

Тем временем Оржих получил в Москве телеграмму о провале типографии. Он немедленно выехал в Екатеринослав. По дороге проехал в Тулу, Орел, Курск, где закрепил связи и подготовил почву для организации новой типографии, а затем вернулся в Екатеринослав. Там он пытается организовать распространение вывезенной из Новочеркасска книги, но в ночь на 23 февраля 1886 г. полиция нагрянула на квартиру М.М. Полякова, где тогда ночевал Оржих. После попытки бежать Оржих с револьвером в руках был арестован и отправлен в местную тюрьму вместе с Поляковым, а через неделю их увезли в Петербург, в Петропавловскую крепость. У Оржиха во время ареста был найден почти готовый материал для 13 номера «Народной Воли», несколько важных писем, походный паспортный стол и 40 экземпляров только-что отпечатанной брошюры «Борьба общественных сил в России», а также написанное им письмо–ответ Тихомирову в Париж, в котором он излагал свой взгляд на современное положение

вещей в революционном мире. Защищая идею террора и выдвигая его на первый план, он писал в этом письме: «Мы употребим все усилия, чтобы, насколько это от нас зависит, создать систематический террор». Все эти улики, равно как и находка «динамитных снарядов» в Таганроге под помещением типографии, послужили основанием к обвинению Оржиха, как главного инициатора южной народовольческой организации. За этими событиями последовал полный разгром южных групп и связанных с ними подпольщиков обеих столиц. По процессу 21-ти народовольца в 1887 г. прошли Г. Лопатин, П. Якубович, Б. Оржих, С. Иванов и другие революционеры. Большинство их суд приговорил к смертной казни, замененной затем вечной каторгой. Это произошло потому, что буквально перед этим были повешены пять студентов, участников покушения на императора Александра III, произошедшего 1 марта 1887 г. (среди них был Александр Ульянов – старший брат В.И. Ленина). Император просто не решился потрясти общественное мнение в России новыми казнями.

После этих событий «Народная Воля» фактически перестала существовать как единая централизованная организация. Хотя в дальнейшем отдельные небольшие группы оставшихся на свободе народовольцев заявляли о возрождении организации, всерьез эти заявления принимать не стоит. Однако революционное движение в России не прекратилось, в конце XIX в. возникли новые революционные организации, которые можно считать приемниками (в том числе и в плане использования криптографии) «Народной Воли». Борьба с самодержавием продолжалась с все нарастающей силой.

Теперь подведем некоторые итоги криптографической деятельности народников. Именно в организациях «Земля и Воля» и «Народная Воля», основанных на жесткой централизации, фактически появились своеобразные криптографические службы, состоящие из людей, отвечавших за разработку шифров, организацию шифрованной связи, распределение ключей и др. Народники применяли разные способы шифрования и стеганографии. Основным шифром стал сокращен-

ный гамбеттовский шифр Л. Златопольского. Первоначально используемая буквенная запись криптограмм постепенно трансформировалась в цифровую. Значительный шаг был сделан в разработке симпатических чернил для химической переписки от простейших «бытовых» веществ до сложных химических соединений. Все это разительно отличалось от деятельности революционеров предыдущего периода. Однако централизация имела и обратную сторону, революционеры стали обрастать «бюрократическими» структурами: составлялись списки членов организации, адресов, появлялись различные документы (уставы, программы, инструкции и др.), которые хранились длительное время. Хотя, как правило, они хранились в шифрованном виде, правоохранительным органам довольно часто удавалось их дешифровать. Ранее неоднократно приводились примеры как из-за этого полицией практически полностью уничтожались крупные организации.

А как видно из сказанного успехи правоохранительных органов по дешифрованию переписки революционеров были весьма серьезными. Совершенно очевидно – народовольцы терпели одно поражение за другим, во многом по причине ненадежности применяемых шифров. Абсолютное большинство их основывалось на применении ключевых слов и фраз. Хотя народовольцы использовали и книжные шифры, но прибегали к ним крайне неохотно. Хотя народовольцы постоянно пытались улучшить свои системы шифрования, однако новые шифры, принципиально отличающиеся от используемых, так и не появились. Следует также подчеркнуть, что подпольщики допускали при использовании шифров серьезные ошибки, что помогало полиции их дешифровать. Примерами таких ошибок являются редкая смена ключей, шифрование текста не целиком, а только наиболее «секретной» его части и др. Иногда использовались и откровенно слабые шифры типа простой замены. Хорошую помощь дешифровальщикам правоохранительных органов оказывали внедренные в революционные организации агенты и предатели из революционной среды. Информация, добытая из переписки

революционных организаций, активно использовалась полицией. На ее основании проводились аресты и обыски, дешифрованные письма являлись уликами в судах и др.

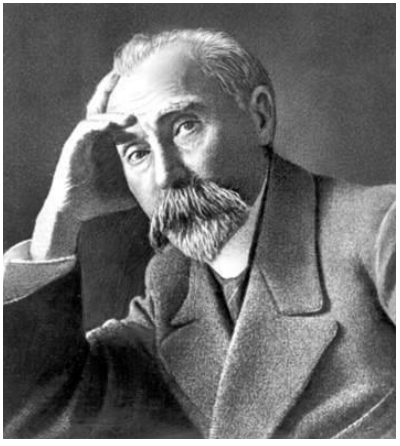
Так же следует отметить, что во второй половине XIX в. появились новые результаты в области криптоанализа. В Берлине и Париже были изданы труды Фридриха Казиского (1863 г.) и Огюста Керкхофса (1883 г.), где они теоретически разрешили проблемы дешифрования шифра Виженера, который являлся основой большинства революционных шифрсистем. В 90-х гг. XIX в. были опубликованы результаты Этьена Базери[1], также посвященные этому вопросу. Весьма вероятно, что специалисты-криптоаналитики правоохранительных органов Российской империи были знакомы с данными работами или сами разработали методику дешифрования подобных шифров.

В заключении следует отметить, что криптографическая деятельность народовольцев нашла отражение и в художественной литературе. В 1889 г. вышел на английском языке писателя-революционера Сергея Степняка-Кравчинского роман «Карьера нигилиста», получивший в русском переводе название «Андрей Кожухов». Только в 1898 г., уже после трагической гибели писателя под колесами поезда, Россия смогла ознакомиться с этой книгой. Ее издание и перевод осуществила вдова Кравчинского. Это была своеобразная «энциклопедия» жизни русского революционера-подпольщика. В романе подробно описан процесс работы с шифрдокументами: проявление стеганографии и работа по расшифровке. Наглядно представлена вся техника нелегальной переписки подпольщиков – подставные адреса, симпатические чернила и шифры. Роман Кравчинского получил самое широкое распространение в канун нового революционного подъема и способствовал обучению конспирации и ведению секретной переписки начинающих русских революционеров.

[1] Подробнее о вкладе Казиского, Керкхофса и Базери в мировую криптографию можно прочитать в статье [2].

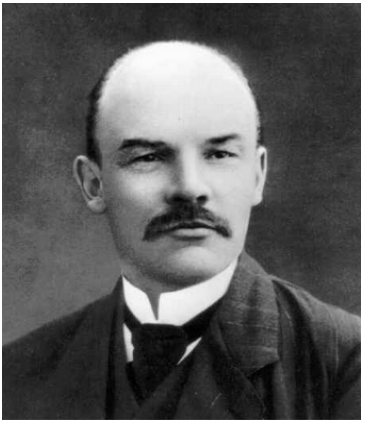
5.4. Криптографическая деятельность революционеров в России в 90-е гг. XIX в.

После окончательного разгрома «Народной Воли» на революционном фронте в России наступило некоторое затишье. Большинство из ветеранов борьбы с царизмом оказалось в заключении или эмиграции, а у молодых российских революционеров, готовых прийти на смену не хватало не сил не опыта, чтобы создать организации сопоставимые по масштабам деятельности с «Народной Волей». Однако к тому времени социал-демократические идеи прочно овладели умами русской революционной эмиграции, и была подготовлена почва для переноса их на российскую почву. Как уже отмечалось ранее [Гольев, 2006], базирующаяся в Швейцарии группа «Освобождение труда», руководимая Г. Плехановым уже с середины 80-х гг. XIX в. начала устанавливать связи с начавшими появляться в России социал-демократическими кружками. Разумеется, для связи с Родиной применялись шифры. Так, в ноябре 1892 г. один из социал-демократов Екатеринослава Илья Тейтельбаум в своем письме к П. Аксельроду указал ключ к шифру для связи с его братом Владимиром. О системе шифрования в письме ничего не сказано, но основывалась она на лозунге «Чужбина», что позволяет предположить, что использовался все тот же гамбеттовский или квадратный шифр. Для защиты информации группа «Освобождение труда» и близко стоящие к ней социал-демократические кружки России продолжали широко использовать квадратные и гамбеттовские системы. Хотя к этому времени они были уже порядком дискредитированы в глазах старых народовольцев. Однако первые российские марксисты все же видимо учитывали ошибки народовольцев и других революционеров прошлого. В практике социал-демократов встречалась двойная перешифровка. В январе 1893 г. социал-демократ В. Шмуйлов напомнил Плеханову свой ключ: «Шифр: вся первая строка, первое слово не под(…)ать, азбука без И, Ъ, Ѣ, Ѳ». Затем письмо Шмуйлова перешифровано цифровым шифром и до сих



Плеханов
Георгий Валентинович

пор до конца не разобрано. Тогдашний русский алфавит содержал 36 букв. За вычетом четырех указанных в письме, а также сравнительно малоупотребительной «ижицы» (γ), получается алфавит в 31 букву, в отличии от народнических шифров, в которых употреблялся 30-буквенного алфавит. Марксисты добавили к нему букву «Э». Группе «Освобождение труда», кроме Екатеринослава, удалось установить связи с социал-демократами в Вильно, Варшаве, Санкт-Петербурге и Москве. Но контакты были нерегулярными, часто нарушались, кружки проваливались. Закаленная в борьбе с «Народной Волей» полиция не собиралась сидеть сложа руки. И опять к специалистам правоохранительных органов среди прочего попадают шифры. Вот лишь один пример. В 1892 г. в Россию через Польшу отправился эмиссар Плеханова Семен Райчин. С собой он вез нелегальную литературу. В Варшаве были получены явки в Москву и Райчин вскоре установил контакт с марксистской группой Бруснева и Егупова. Они быстро сошлись, условились об адресах, методах переписки и шифрах. Но на обратном пути Райчин был арестован. Вслед за этим оказались разгромлены подпольные кружки Варшавы и Москвы. Полиции стало известно многое. В том числе и шифры марксистов. Они строились на лозунгах «Черемуха» и «Шпицберг», скорее всего это опять «квадратный шифр». Надо отметить, что при переписке первых российских марксистов использовались слишком короткие ключевые лозунги, а на них удобно строить именно квадратные таблицы. Однако к этому времени в Санкт-Петербурге уже действовало несколько разрозненных марксистских кружков. Хотя об объединении и



Владимир Ильич Ульянов (Ленин)

создании крупной организации речь еще не шла, столичные марксисты взаимодействовали друг с другом. По прежнему лидером в продвижении марксизма в Россию оставалась группа «Освобождение труда». Летом 1892 г. с Плехановым установил первые связи один из столичных марксистов Александр Потресов, через виленских социал-демократов в Санкт-Петербург начала регулярно поступать нелегальная марксистская литература.

31 августа 1893 г. в столицу Российской Империи из Самары прибыл никому не известный начинающий адвокат Владимир Ильич Ульянов. Тогда никто и не мог предположить какую грандиозную роль в истории России сыграет этот человек, ставший известным всему миру как Владимир Ильич Ленин (далее будет использоваться эта фамилия, хотя этот псевдоним был взят вождем мирового пролетариата позднее). К тому времени В.И. Ленин уже решил, что станет профессиональным революционером. Почти сразу он установил контакты с небольшим кружком студентов-технологов – осколком разгромленных немногим раньше марксистских кружков Санкт-Петербурга. Кружок, возглавляемый Степаном Радченко, главным образом, занимался пропагандистской работой среди рабочих Петербурга. Учитывая недавние успехи полиции, участники кружка, особенно его лидер, уделяли вопросам конспирации большое внимание. В.И. Ленин оказался крайне полезным приобретением для организации, так как еще в Самаре, он общался с рядом бывших народников и народовольцев, в частности супругами Ливановыми в прошлом активно участвовавших в революционном движении. Из общения с этими людьми Ленин много знал о методах революционной борьбы. Среди прочего ему было известно об обес-

печении конспирации, методах защиты информации и организации связи, в том числе и с местами лишения свободы, народников и народовольцев. Из этого же источника В.И. Ленин получил сведения о шифрах, использовавшихся революционерами предыдущих поколений. Разумеется, всеми своими знаниями он активно делился с новыми товарищами. Вот как об этом вспоминает Н.К. Крупская: «Из всей нашей группы Владимир Ильич лучше всех был подкован по части конспирации: он знал проходные дворы, умел великолепно надувать шпиков, обучал нас, как писать химией в книгах, как писать точками, ставить условные знаки, придумывал всякие клички…Владимир Ильич учил шифровать. Почти полкниги исшифровали. Увы, потом я не смогла разобрать этой первой коллективной шифровки».

К сожалению, о применявшихся в кружке шифрах ничего не известно, имеются лишь отрывочные сведения об их наличии. Так, в январе 1894 г. удалось установить контакт с Сергеем Шестерниным, работавшим в то время городским судьей в Иваново-Вознесенске и разделявшим социал-демократические взгляды. Позже С. Шестернин вспоминал: «В результате моих бесед с членами кружка было установлено, что я буду связывающим звеном между питерским кружком и ивановцами. Кружковцы дали мне шифр для сношения с ними…».

А вскоре у России меняется правитель. В конце октября 1894 г. умер Александр III и на престол взошел последний российский император Николай II. Впрочем, для революционеров и правоохранительных органов мало, что изменилось. Первые создавали все новые организации, вели агитацию и пропаганду, распространяли нелегальную литературу и др. А вторые в свою очередь всеми способами старались подобную деятельность пресечь.

Тем временем среди российских социал-демократов наметилась тенденция к объединению. Так среди столичных марксистов уже к началу 1895 г. стали популярны идеи интеграции в крупную единую организацию. К этому времени В.И. Ленин стал признанным лидером своего кружка, хотел

играть активную роль в объединительном процессе. Но участники других кружков еще не видели в нем своего будущего вождя. Для поднятия своего авторитета среди революционеров В.И. Ленин решает предпринять поездку за границу для установления личного контакта с группой «Освобождение труда» и непосредственно с Г. Плехановым. Весной 1895 г. перед отъездом своего лидера за границу, соратники Ленина еще активнее занялись изучением методов защиты информации и организации конспиративной переписки. Вот как об этом вспоминает один из товарищей Ленина Михаил Сильвин: «У меня съехались товарищи, и Владимир Ильич… наметил дальнейший план работы и разделение функций между нами на случай ареста… Владимир Ильич особо настаивал на соблюдении элементарных правил конспирации… Он учил писать молоком между строчек, точками в книгах… Все… сообщили здесь данные о своих связях… Надежда Константиновна, уже тогда выполнявшая главную работу… по секретной части, тут же наскоро зашифровала все это».

А вскоре после этих событий В.И. Ленин уехал в Швейцарию на встречу с Георгием Плехановым. Влияние этого человека на молодого Ильича трудно переоценить, он, по собственному признанию, воспитывался на трудах Плеханова. Одним из таких трудов была книга некоего Н. Бельтова «К вопросу о развитии монистического взгляда на историю». Под таким названием в декабре 1894 г. в Санкт-Петербурге вышла выдающаяся работа Плеханова. Много позже, когда дороги Ленина и Плеханова окончательно разойдутся, Владимир Ильич все равно будет очень высоко отзываться об этой книге, он напишет, что на этой книге «воспитывалось целое поколение русских марксистов». Однако внимание этой книге уделяется, совсем по другой причине, именно она стала ключом для книжного шифра, который будет использован для связи Ленина и его товарищей с заграницей.

Итак весной 1895 г., В.И. Ленин прибыл в Женеву. Ученик приехал на встречу с учителем. Отметим, что Владимиру Ильичу только исполнилось 25 лет, а Г.В. Плеханову было все-

го 39! Но молодые революционеры его считали уже стариком, ветераном революционной борьбы. Ленин и Плеханов провели несколько встреч и, В.И. Ленин произвел весьма хорошее впечатление на одного из первых русских марксистов. После бесед с Плехановым, которые носили теоретический характер, В.И. Ленин выехал в Цюрих для встречи с Павлом Аксельродом, который в группе «Освобождение труда» занимался практическими вопросами организации каналов связи между заграничной социал-демократической эмиграцией и Россией. Решив с Аксельродом все вопросы о способах дальнейших сношений (и за границей, и в России), получив нужные явки, В.И. Ленин отправился в Париж. Затем его путь пролег в Берлин. Все лето 1895 г. Владимир Ильич провел за рубежом. В Берлине Ленин встречается с И. Айзенштадтом и В. Бухгольцем. Первый был одним из основателей и руководителей социал-демократических кружков в Вильно. В сентябре 1894 г. он появился в Берлине и установил оттуда прочные связи с группой «Освобождение труда». Айзенштадт создал транспортную группу для контрабанды через германскую границу подпольной литературы и являлся берлинским представителем виленского подполья в только что образованном заграничном «Союзе русских социал-демократов». Весной 1895 г. для работы по нелегальному транспорту им был привлечен эмигрант Бухгольц. После возвращения в августе 1895 г. Айзенштадта в Россию, до осени 1897 г. Бухгольц оставался главным связывающим звеном между группой Плеханова и российским подпольем. Кстати Бухгольц и Ленин знали друг друга еще по Самаре. Основной темой переговоров были способы транспортировки нелегальной литературы в столицу России, удалось договориться о линиях и способах связи. В.И. Ленин предложил оригинальный стеганографический способ перевозки нелегальной литературы. Суть его состояла в прессовании и превращении в переплетный картон подлежащих тайной перевозке литературных материалов: «Листы таковой литературы или писем (только писанных тушью), по этому рецепту соединяются особым клеем, накладываются один на другой до

определенной толщины, обкладываются снаружи подходящей бумагой; в таком виде прессуются и сушатся, после чего получается обычный на вид картон, не навлекающий ничьего подозрения; когда же спрятанную в этом картоне литературу нужно возвращать в первобытное состояние, то картон кладут в теплую воду и осторожно разнимают на составные части». Хотя идея использования переплетов книг в качестве контейнера для перевозки нелегальной литературы давно активно использовалась революционерами, в том числе группой «Освобождение труда», но эта технология все время продолжала совершенствоваться. Способ, предложенный Ленином, был принят. В ноябре 1895 г. в письмах к П. Аксельроду дает дополнительные пояснения: «Писать надо китайской тушью. Лучше, если прибавить маленький кристаллик хромпика ($K_2Cr_2O_7$): тогда не смоется. Бумагу брать потоньше… Необходимо употреблять очень жидкий клейстер: не более чайной ложки крахмала (и притом картофельного, а не пшеничного, который слишком крепок) на стакан воды. Только для верхнего листа и цветной бумаги нужен обыкновенный (хороший) клейстер, а бумага держится хорошо, под влиянием пресса, и при самом жидком клейстере. Во всяком случае, способ годен, и его следует практиковать». Отметим, что хромпик это вещество в виде кристаллов красного цвета. Оно – исходный материалом для получения всех других соединений хрома. В XIX в. это вещество широко применялось как окислитель в процессе фабричного крашения тканей и в фотомеханических способах печатания изображений. Поэтому хромпик был тогда вполне доступным для подпольщиков химикатом.

А технику вскрытия тайника в переплете в конце июля 1901 г. описала в одном из своих писем Н.К. Крупская: «На днях пошлем вам книгу в переплете. Переплет нужно опустить в теплую воду и, когда он станет расслаиваться, начать отделять листы, подставляя под кран с кипящей водой. Надо только не спешить. Отделенные таким образом листы вытереть губкой, чтобы снять клей, потом дать высохнуть и сыроватыми положить под пресс».

По сравнению с другими стеганографическими способами защиты информации (симпатические чернила или точки над буквами), которые были хорошо известны правоохранительным органам метод заделки писем в картон, безусловно, был гораздо более надежен, и революционеры высоко ценили его. Однако он был громоздок, трудоемок, требовал определенных материальных затрат, в частности, на трудности вскрытия тайника в одном из своих писем указывал Н.Э. Бауман: «…Ваш переплет получил… только он причинил массу хлопот, несмотря, что этот способ я знал и имею опыт. Нужны слишком хорошие квартирные условия, чтобы без отлагательств добыть содержимое. Поэтому прибегайте к нему в крайних случаях». По этим причинам и другие способы стеганографии по прежнему находили в революционной переписке широкое применение.

В целом 4-месячная поездка В.И. Ленина оказалась весьма плодотворной. 7 сентября 1895 г. он беспрепятственно пересек границу Российской империи, в его багаже в чемодане с двойным дном находилась нелегальная литература, полученная в Берлине. 29 сентября 1895 г. В.И. Ленин прибыл в Санкт-Петербург и сразу же развил бурную деятельность по объединению марксистких организаций столицы в единую централизованную организацию. Успешная поездка за границу сделала В.И. Ленина весьма влиятельной фигурой среди петербургских социал-демократов и вскоре происходит объединение нескольких кружков в знаменитый «Союз борьбы за освобождение рабочего класса», от которого ведет свою историю партия большевиков. Эта организация стала примером и призывом к действию для социал-демократов других российских городов. Осенью 1895 г. Ленин и его соратники ведут активную переписку с П. Аксельродом, используется книжный шифр с книгой Бельтова-Плеханова в качестве ключа. Письма переправляются в переплетах книг. Интересно отметить, что в этот период Ленин сам шифрует письма, в последствии главным шифровальщиком у большевиков будет Н.К. Крупская.

Крупская Н.К.

При шифровании Ленин допускает характерные для многих революционеров ошибки: шифруется не все письмо, а лишь отдельные его участки, в основном адреса и фамилии, кроме того, при шифровании ставились пробелами между словами и знаки препинания, одни и те же буквы открытого текста шифруются одинаковыми шифробозначениями. Все это могло существенно облегчить дешифрование, особенно последнее, это очень серьезный недостаток – весьма стойкий книжный шифр многоалфавитной замены, по сути, сводится к шифру простой замены, дешифрование которого и в те времена не составляло труда. Однако следует заметить, что Ленин и его товарищи осваивали шифровальное дело фактически самостоятельно, во многих случаях буквально по наитию. Никаких учебных материалов по криптографии не было, и если о самих способах шифрования информация еще была (от тех же народников), то вопросы грамотного использования шифрсистем, стали решаться лишь с накоплением опыта. Главное, что Ленину и его товарищам повезло, их ошибки не привели к трагическим последствиям. Не смотря на ошибки при использовании шифров, в целом конспиративную деятельность ленинской организации можно признать достаточно профессиональной, для защиты информации использовались совместно криптографические и стеганографические методы, вводились подставные адреса (отдельно для переписки и для явки) и др. Но все более активная деятельность новой организации не могла не привлечь внимания правоохранительных органов. 11 декабря 1895 г. министр внутренних дел докладывал императору Николаю II: «Принимая во внимание,

что за последние месяцы кружок стал проявлять особую энергическую деятельность, приобретать материалы и инструменты для печатания и воспроизведения преступных изданий, а равно принял деятельное участие в происходивших в ноябре и декабре месяцах рабочих волнениях на Путиловском и Торнтоновском заводах, – признано было своевременным приступить к обыскам и арестам участников названного кружка. Обыски эти произведены в ночь на 9 сего декабря и вполне подтвердили имеющиеся указания на преступную деятельность заподозренных лиц». Во время проведения этих мероприятий в ночь с 8 на 9 декабря 1895 г. был арестован и присяжный поверенный Владимир Ульянов. В отличии от многих прочих арестов во время этой операции в руки полиции не попало никаких криптографических материалов, было ли это счастливой случайностью или результатом того, что Ленин и его соратники учли печальный опыт народовольцев сейчас сказать трудно, но факт остается фактом.

Успехи полиции по пресечению деятельности революционных организаций, продолжали происходить, в том числе, из-за внедрения своих агентов в ряды революционеров-подпольщиков. От агентуры правоохранительные органы, как и прежде, получали значительное количество информации, в том числе сведения о шифрах и ключах подпольных организаций. Дело Судейкина продолжало жить! Так начальник Московского охранного отделения Н.С. Бердяев в понятие «розыск» включал первичные следственные действия (обыск, арест, задержание, выемку и др.), дознание, наблюдение и надзор общей полиции. Докладывая Департаменту полиции о положении дел в охранке, он писал, что агентурное наблюдение ведется в Москве тремя способами. Благодаря секретной агентуре, охранка выявляла революционеров и их кружки. За наиболее активными членами организации устанавливалось наружное наблюдение, итогом которого были обыски и аресты. При наличии вещественных доказательств дело передавалось в Губернское жандармское управление, а если их не было, то производилось дознание на основании «Положения об охране», в результате чего следовала административная

высылка, гласный или негласный надзор, и тогда наблюдение за революционерами велось через местную полицию.

Начальный этап розыска – «выявление врагов царя и отечества» - осуществлялся за счет широкой осведомительной базы административных учреждений и должностных лиц, которые обязаны были давать полиции сведения. Это были анонимные и явные доносители, домовладельцы, сдающие квартиры, общая полиция и прочие источники, которые информировали охранку об обстановке на их участке.

Однако правоохранительные органы России стремились наладить систематический поток информации, в связи с чем прибегала к помощи осведомителей. Эта категория лиц «освещала» настроения определенных кругов и слоев населения, не образующих нелегальных политических обществ. Они вербовались из дворников, обслуживающего персонала гостиниц, ресторанов, чиновников, интеллигенции и подобных им категорий населения. Осведомители периодически информировали розыскные органы по различным вопросам, получая время от времени денежные вознаграждения.

Непосредственную разработку вели «секретные сотрудники», работая непосредственно в «исследуемой среде». После предательства Дегаева агентов полиции в революционной среде обычно называли провокаторами. Безусловно, в революционных организациях было очень много таких. Сами охранники квалифицировали деятельность своей агентуры несколько по-другому. Наибольшее значение они придавали «секретным сотрудникам». Под этим определением подразумевалась «агентура внутреннего наблюдения вообще». Но иногда так обозначался платный агент, находившийся в революционной среде. При помощи таких агентов охранка проникала в «область интеллектуальной жизни заподозренных лиц, принимая личину сочувствия и единомыслия им». В «Инструкции по организации и ведению внутренней агентуры» были даны следующие определения: «лица, состоящие членами преступных сообществ и входящие в постоянный состав такой агентуры, называются агентами «внутреннего наблюдения» или «секретными сотруд-

никами»«. «Лица, которые хотя не входят в преступные организации, но соприкасаются с ними, постоянно содействуют делу розыска, исполняя различные поручения и доставляя для разработки материал по деятельности партии, в отличие от первых, носят название «вспомогательных агентов»». Через вспомогательных агентов-осведомителей карательно-розыскные органы осуществляли «надзор за состоянием умов».

Разновидностью «вспомогательных» агентов-осведомителей были «штучники». Они оказывали охранке одноразовые услуги. К ним относились стоящие не у дел секретные сотрудники. Этой категории агентов очередной начальник московской охранки С.В. Зубатов не доверял и, поучая своих подчиненных, говорил: ««Штучников» гоните прочь, это не работники, это продажные шкуры. С ними нельзя работать». Из секретных сотрудников и осведомителей, потерявших доверие охранки, формировалась категория «агентов, не заслуживающих доверия». К ним относились «шантажисты» и «провокаторы». «Шантажистами» охранники считали агентов, дающих вымышленные сведения в целях получения вознаграждения, а под «провокаторами» подразумевались сотрудники, совершавшие непредусмотренные заданием деяния без ведома и согласия охранки.

В практике борьбы с революционным движением русская полиция практиковала два метода: пресечения и предупреждения политических преступлений. Первый состоял в том, что полиция позволяла организации сплотиться и затем ликвидировала ее, чтобы дать прокуратуре организацию с большими, по возможности, доказательствами виновности. Второй заключался в систематических ударах по революционным деятелям, чтобы мешать работе, не позволять сплотиться, проваливать их в глазах их же товарищей как деятелей неконспиративных, что вело к удалению их от работы и др. Как отмечал один из руководителей российской жандармерии генерал Спиридович, первый метод был более эффективен по результатам, второй – более правилен по существу. Для реализации этих методов использовались хитроумные комбинации различных оперативно-

тактических приемов. Это были облавы (повальные обыски и аресты), сбор сведений, ловля «на живца», оставление на «разводку», «подставка», компрометация, шантаж, подкуп, провокация, подлог, фальсификация и др.

И все же наибольшее возмущение у революционеров и общественности вызывала провокация. В зависимости от целей розыска, состояния революционного движения, тактики партии или организации, политической обстановки в стране, личных качеств охранников и наличия технических средств провокация занимала более или менее важное место в розыскной деятельности. Для выявления замыслов революционеров агент должен был «выдвинуться» на первый план для получения наиболее ценной информации. Это особо ярко просматривается в деятельности агентов-террористов и экспроприаторов. Они не только «устанавливали» злоумышленников, но и подталкивали их в нужное русло, т.е. старались перевести акции политического характера в разряд уголовных.

Одним из наиболее известных агентов-провокаторов был Евно Азеф, его основные «подвиги» будут показаны несколько позднее. Пока же отметим, что в 1895 г. Азеф, уже будучи полицейским агентом, еще не определился в своих симпатиях и одновременно вращался и в среде бывших народовольцев и среди первых русских социал-демократов. Среди прочей информации Азеф доносил начальству: «Между г-ном Петерсом и Меерович установлен шифр для их переписки в России. Слово шифра «Великобритания». Азбука составлена из первых чисел: 1 – А, 2 – Б, 3 – В и др. К каждой букве прибавляется буква слова «Великобритания» и все цифрами, например, слово «вода» пишется так: В –3 (в) + 3 (в) = 6 (в одной строке), О = цифра, соответствующая «О» + цифра для «Е» и др.». В достаточно неуклюжем объяснении начинающего провокатора нетрудно распознать гамбеттовский шифр. Использовали эту систему социал-демократы Б. Петерс и Ф. Меерович, в заграничный кружок которых одно время входил и Азеф. Любопытно, что речь идет в донесении о первоначальном варианте гамбеттовского шифра. В конце XIX в. он получил назва-

ние «раздельного гамбеттовского ключа», а «сокращенный гамбетт» был забыт. Однако время безраздельного царствования среди шифрсистем российских революционеров «гамбеттовских ключей» и вариаций на тему шифра Виженера подходило к концу, стали внедрятся в практику революционной работы другие шифрсистемы.

Как и его предшественники даже находясь под арестом В.И. Ленин продолжает революционную борьбу. К тому же во время декабрьских арестов 1895 г. организация была разгромлена не полностью. Оставалась на свободе и Н.К. Крупская. С помощью приехавших в Санкт-Петербург матери и сестры Анны, с Владимиром Ильичом была установлена тесная связь. С помощью родственников и разных других ухищрений (например, заказа по очереди одной и той же книги из тюремной библиотеки) арестованные члены «Союза борьбы» установили связь между собой. Еще перед арестами среди членов «Союза борьбы» были разработаны определенные шифры. К сожалению, точно сказать какие применялись шифры сейчас уже невозможно. Однако следует отметить, что В.И. Ленин и его товарищи умели уже применять книжный, стихотворный и гамбеттовский шифры. В пользу возможного использования книжного шифра говорит следующий факт, что среди книг, которые получил в камеру В.И. Ленин, была и та самая книга Бельтова-Плеханова, которая служила ключом для переписки с заграницей, ничего не мешало использовать ее для шифрования переписки с волей. Отмечается и использование стихотворных шифров. При этом историки отмечают, что Ленин при шифровании разных частей одного письма использовал разные шифрсистемы. Также части письма могли быть написаны на разных языках, например английском и немецком. Напомним, что В.И. Ленин хорошо владел несколькими иностранными языками. О применявшихся стеганографических приемах известно гораздо больше, вот что об этом вопросе вспоминает сестра В.И. Ленина А.И. Ульянова-Елизарова: «Это, пожалуй, самые интересные страницы из его тюремной жизни… Конечно, никаких химических реактивов в тюрьме

получить было нельзя. Но Владимир Ильич вспомнил, как рассказывал мне, одну детскую игру, показанную матерью: писать молоком, чтобы проявлять потом на свечке или лампе. Молоко он получал в тюрьме ежедневно… И вот он стал писать им меж строк жертвуемой для этого книги… Таким образом, шифрованные письма точками были заменены этим, более скорым способом. В письме точками Ильич сообщал, что на такой-то странице имеется химическое письмо, которое надо нагреть на лампе. Вследствие трудности прогревания в тюрьме этим способом пользовался больше он, чем мы. Надежда Константиновна указывает, впрочем, что можно было проявлять письма опусканием в горячий чай и что таким образом они переписывались молоком или лимоном, когда сидели (с осени 1896 г.) одновременно в предварилке. Вообще Ильич, всегда стремившийся к уточнению всякой работы, к экономии сил, ввел особый значок, определявший страницу шифрованного письма, чтобы не рыться и не разыскивать в книгах. Первое время надо было искать этот значок на странице семь. Это был тоненький карандашный штрих, и перемножение числа строк с числом букв на последней строке, где он находился, давало страницу: так, если была отмечена 7-я буква 7-й строки, мы раскрывали 49-ю страницу, с которой и начиналось письмо… Этот способ обозначения, – страницы время от времени менялись, – сохранялся у нас постоянно».

Больше года провели в стенах дома предварительного заключения В.И. Ленин и его товарищи. 13 февраля 1897 г. Владимир Ильич был отправлен в ссылку в Восточную Сибирь под гласный надзор полиции на 3 г. Аналогичные приговоры получили и большинство его товарищей. По ходатайству родственников высылаемым в Сибирь марксистам разрешили до 17 февраля остаться в столице. И это время не было потрачено даром, помимо встреч с родственниками и товарищами, сборов в дорогу, участники «Союза борьбы за освобождение рабочего класса» договорились о способах конспиративной переписки и применяемом шифре. Для защиты информации был выбран книжный шифр. Ключ – книга А. Волгина «Обоснование народниче-

ства в трудах г-на Воронцова (В.В.)», изданная в феврале 1896 г. Эта вторая книга Г.В. Плеханова, легально изданная в России под новым псевдонимом.

Конец XIX в. в России характеризовался поразительно быстрым ростом социал-демократических кружков во многих регионах Российской империи, а в Санкт-Петербурге, Москве, Одессе, Вильно, Киеве, Екатеринославе и некоторых других городах возникали уже крупные организации марксистов. Несмотря на преследование правоохранительными органами, постоянные аресты и погромы, вызванные неопытностью начинающих подпольщиков, процесс распространения идей Маркса в России шел полным ходом. Одно из важных мест в социал-демократическом движении стали занимать с 1895 г. еврейские социалистические группы. Они были связаны между собой и сконцентрированы вокруг виленского кружка. Фактически в тот самый момент Вильно превратился в центр социал-демократии России. В сентябре 1897 г. на учредительном съезде в Вильно был основан «Всеобщий еврейский союз в Литве, Польше и России» (БУНД). Через БУНД шла литература от заграничных организаций, еврейские марксисты имели прочные связи со всеми крупнейшими подпольными организациями от Петербурга до Киева. Первоначально эта организация стояла на социал-демократических позициях и внесла значительный вклад в становление марксисткого движения в России.

Активность русского революционного движения продолжала возрастать. Принимались меры по созданию единой политической организации, в марте 1898 г. в Минске состоялся первый съезд российской социал-демократической рабочей партии (РСДРП). Инициатива его созыва принадлежала Киевскому «Союзу борьбы», а практическое обустройство съезда взяли на себя еврейские социал-демократы из БУНДа. Бундовцы первыми проинформировали о прошедшем съезде группу «Освобождение труда». Сделал это Арон Кремер («Александр») – член ЦК БУНДа и делегат съезда. Письмо его в Женеве получил эмигрант И. Блюменфельд. Оно было зашифровано точками в присланной газете и, после расшиф-

ровки криптограммы, Блюменфельд немедленно проинформировал о событии П. Аксельрода и Г. Плеханова. Оба находились в тот момент в Цюрихе.

Правоохранительная система Российской империи ответила на рост революционного движения также организационными мерами. 1 января 1898 г. в составе департамента полиции создается Особый отдел, возглавивший работу с заграничной и внутренней агентурой, а также вновь создаваемыми розыскными отделами. В функции особого отдела входит обобщение перлюстрации писем, систематизация и выемка противоправительственных книг и брошюр. В отдел собирается вся информация, полученная оперативным путем. Особый отдел департамента полиции стал центральным органом, руководившим всем розыском империи, возглавил его приглашенный из Москвы С.В. Зубатов, считавшийся лучшим практиком розыскного дела. Отдел стал подлинным штабом политического розыска. В поле его зрения находились не только революционные и оппозиционные организации, но и министры, генералы, даже лица императорской фамилии – великие князья. Агентура департамента имелась во всех без исключения революционных партиях и организациях. Но в центре его внимания находились наиболее опасные для самодержавия партии – эсеров и социал-демократов. Делалось все, чтобы секретные сотрудники занимали в партиях как можно более важное и влиятельное положение. Это давало возможность им не только быть в курсе всех замыслов и дел в партийных организациях, но и вмешиваться в партийные дела, создавать склоки и враждебное отношение революционных лидеров друг к другу, добиваться тех решений, которые были выгодны департаменту. (Министерство внутренних дел, например, опасалось того, что социал-демократическая партия, разбитая на большевистскую и меньшевистскую фракции, может объединиться. 16 сентября 1914 г. был разослан циркуляр (приказ) Департамента полиции: всем охранным и жандармским управлениям приказывалось «безотлагательно внушить подведомственным секретным сотрудникам, чтобы они участвовали в разного рода партийных совещаниях, не-

уклонно и настойчиво проводя и отстаивая идею полной невозможности какого бы то ни было организационного слияния течений и в особенности объединения большевиков с меньшевиками».) Быстро рос архив ведомства. Активно велась регистрация лиц, связанных с революционной деятельностью. В 1902 г. особый отдел департамента полиции располагал именной картотекой из 55 тыс. учетных карточек. Имелось также около 20 тыс. фотографий «государственных преступников» и «политически неблагонадежных лиц», а также 5 тыс. экземпляров различных революционных изданий. Все это служило серьезным подспорьем при дознаниях, разработках секретных операций, для составления учебных пособий для курсов по подготовке жандармских офицеров. Но нужно отметить, что высоким профессионализмом, знанием техники розыскного дела обладали только верхи жандармской иерархии в Петербурге и Москве. В провинции дела с политическим розыском в начале XX в. обстояли значительно хуже. Мало было опытных офицеров по наружному наблюдению, вербовке агентуры, разработке секретных сведений. С точки зрения криптографической деятельности создание особого отдела стало этапным. Именно в этом подразделении департамента полиции после более чем 30 лет борьбы с шифрами революционеров «на общественных началах» в МВД Российской Империи была создана штатная дешифровальная служба.

Образовательный и профессиональный уровень сотрудников департамента полиции был весьма высок. Уже в 90-е гг. XIX в., когда его директором был назначен Степан Петрович Белецкий, начинается активная работа с кадровым составом департамента, в 1900-х гг. уже девять из десяти служащих этого органа были людьми с высшим образованием и в большинстве случаев с немалым практическим служебным стажем.

Белецкий чрезвычайно заботился о всестороннем развитии своих сотрудников, расширении их кругозора, углублении знаний. Так, все, что было нового в подпольной прессе и на русском и заграничном книжном рынке из области социальных вопросов, все выписывалось, переводилось, читалось, посылалось в форме ежемесячников розыскным офицерам. Вся-

кие сведения, даже личного свойства, касавшиеся того или иного видного деятеля политической оппозиции, принимались Белецким во внимание при обсуждении планов борьбы с различными революционными партиями и группами.

Белецкий Степан Петрович

В этой борьбе правоохранительных органов империи с революционерами продолжало существенную роль играть изучение почтовой переписки подпольщиков. Как уже отмечалось, письма подпольщиков нередко попадали в руки жандармов в результате обысков и арестов, но не сидела без дела и служба перлюстрации. «Черные кабинеты» по всей России выполняли заявки особого отдела департамента полиции по перехвату писем и их изучению. Письма изымались на почтамтах по подозрительным признакам: «знакомый почерк», размер, вес, качество и цвет конвертов, адреса и фамилии и др. Письма изучались на предмет наличия в них секретных посланий, написанных «химией» (симпатическими чернилами). Революционеры нередко продолжали использовать простейшие «чернила»: сок лимона, лука, молоко, слабые растворы серной и соляной кислот. Техника проявления проста: нагревание над керосиновой лампой. К сожалению, довольно часто наступало «самопроявление» конспиративного текста, что приводило к его лёгкому прочтению в «чёрном кабинете» России. При поиске следов стеганографии искались дефекты бумаги при нанесении «невидимого текста»: продавливание (бороздки), возникающие при нажатии пера, самопроявляющиеся микрофрагменты послания и др. Подозрительные письма передавались на дополнительное изучение. Кстати революционеры имели представление о некоторых методах работы перлюстраторов, так Н.К. Крупская рекомендовала одному из революционеров «писать совсем чистым пером и вовсе не нажимать, а то видно».

Работали в «черных кабинетах» и по так называемым спискам. Это дело было организовано следующим образом. Письма для вскрытия отбирались по двум спискам. Первый список особого отдела департамента полиции содержал фамилии лиц, письма которых подлежали просмотру, и адреса, посланные по которым письма подлежали перлюстрации. Также должны были перлюстрироваться письма, освещающие деятельность съездов, партконференций противоправительственных организаций, содержащие материалы об их подготовке, проведении, деятельности основного партийного состава и членов различных организаций. Второй список составлялся министерством внутренних дел и предписывал перлюстрацию писем общественных и политических деятелей, редакторов газет и журналов, профессоров, членов государственного совета и государственной думы, членов царской фамилии. Не подлежали перлюстрации письма только самого министра внутренних дел и царя.

В свою очередь революционеры нередко предпринимали ответные меры защиты. Так, например, как само письмо, так и адрес на конверте исполнялись печатными буквами. Иногда отправитель менял свой почерк, письма от мужчин подделывались и стилизовались под письма, написанные женщинами. Это значительно затрудняло работу «черного кабинета». Так как непосредственно перлюстрацией по всей России занимались всего 40–50 человек, которым помогали работники почт, отбиравшие письма. В места, где перлюстрационные пункты отсутствовали, в случае необходимости командировались чиновники из центрального пункта в Санкт-Петербурге. Но часто губернские жандармские управления привлекали к этой работе узкий круг местных почтовых чиновников и проводили перлюстрацию сами.

Следует отметить, что письма, перлюстрированные в российских «черных кабинетах», не несли на себе сколько-нибудь заметных следов перлюстрации. И здесь и революционерам, и иностранным дипломатам не помогали никакие ухищрения: ни «царапины печати, ни заделка в сургуч волоса, нитки, булавки и др. В материалах чрезвычайной следственной

комиссии Временного правительства, разбиравшей в 1917 г. вопрос о перлюстрации, имеются данные о том, что в 1910 г. командир Отдельного корпуса жандармов П. Курлов обратился к старшему цензору с просьбой, чтобы адресованные ему письма не носили явных следов вскрытия. Такая же просьба высказывалась поборником перлюстрации директором Департамента полиции С.П. Белецким.

В год перехватывалось примерно 150–200 конспиративных шифрованных писем. Дешифрованием писем занималась группа дешифровальщиков, созданная специально для этого в особом отделе. Вот что по этому поводу пишет один из исследователей деятельности подпольных революционных организаций конца XIX – начала XX вв. Ю.С. Уральский: «Многие чиновники особого отдела имели физико-математическое образование и довольно большой опыт дешифровальной работы… Техника дешифровки конспиративной переписки основывалась, во-первых, на фонетических законах письма…, во-вторых, на допускаемых революционерами ошибках при шифровании…, в-третьих, на сведениях, полученных от агентуры и провокаторов, засылаемых в социал-демократические организации… Агентура пыталась добывать конспиративные адреса, ключи для шифрованной переписки…».

Начиналась новая эпоха в революционном движении Российской империи, из разрозненных кружков возникла единая марксисткая организация и, хотя вскоре последовало размежевание между членами РСДРП, начало триумфальному шествию коммунизма по России было положено.

5.5. На рубеже веков. Криптографическая деятельность революционеров в России 1898-1900 гг.

В последние гг. XIX в. революционное движение стремительно расширялось. В Минске 1 марта 1898 г. прошел первый съезд РСДРП. Благодаря соблюдению мер конспирации пра-

воохранительным органам не удалось сорвать проведение съезда российских социал-демократов. Интересно отметить, что о существовании БУНДа в департаменте полиции вообще не подозревали, хотя организация активно работала, издавались газеты, листовки, прокламации, организовывались забастовки, велась агитация и др.

Учитывая опыт народников российские социал-демократы, придавали важное значение защите информации в революционной работе, стали проводиться организационные мероприятия, разрабатываться правила защищенной связи и издаваться инструкции на эту тему для участников подполья. Так, например, для киевской организации «Союза борьбы» накануне первого съезда РСДРП один из видных революционеров В.М. Сапежко подготовил специальную «инструкцию», которая должна была стать для российских социал-демократов основным руководящим документом в области конспирации. Рассмотрим ее подробно. «Инструкция» содержала следующие разделы: «Введение», «Поведение на свободе», «Поведение во время следствия», «Русское делопроизводство дел политических», «Порука», «Корпус жандармов и организация шпионов».

Во «Введении» обосновывалась необходимость строжайшего соблюдения конспирации в деятельности социал-демократических организаций.

В разделе «Поведение на свободе» рассматривались вопросы функционирования тайной организации: правила конспирации, методы транспортирования нелегальной литературы, способы ухода от наружного наблюдения, методы обнаружения наружного наблюдения, условные знаки об опасности (например горшок с цветами в окне мог означать, что явка провалена или в квартире находятся посторонние люди), меры безопасности принимаемые при аресте членов организации и др. Было предложено ввести специализацию, каждый член организации должен был выполнять только определенную работу. В случае его ареста работу по остальным направлениям продолжали оставшиеся на свободе. Здесь же

было сформулировано требование о запрете делиться какой-либо информацией (фамилии, адреса, время собраний, места хранения нелегальной литературы и др.) не только с посторонними (включая родных и близких), но и с самыми надежными членами организации, если эта информация непосредственно их не касается. О важнейших делах организации должен был знать предельно ограниченный круг лиц.

Важное место в «инструкции» уделялось проблеме подбора кадров. К нелегальной работе должны допускаться только проверенные, «кристально чистые и честные лица, для которых общее дело должно быть превыше личных интересов» [Уральский, 1980]. Особое внимание уделялось постоянному поддержанию бдительности, говорилось о том, что это чувство может притупиться из-за продолжительной работы в нелегальных условиях.

В этом разделе содержались и рекомендации по организации защиты информации, приведем их полностью.

«Необходимо избегать излишней корреспонденции, не нужно также составлять и сохранять заметки, касающиеся вопросов нелегальных. В случае необходимости написать письмо лучше всего пользоваться заранее условленным ключом или писать иносказательно, т.е. так, чтобы только заинтересованное лицо могло понять истинный смысл письма. Однако не надо употреблять такие выражения, которые нельзя объяснить самым легальным образом, так как случалось, что жандармы в темных, двумысленных фразах доискивались до того, чего даже не было в действительности. При употреблении химических чернил не мешает шифровать некоторые слова, но нельзя их ставить вперемежку с обыкновенными, ибо тогда их нетрудно прочесть; поэтому необходимо шифровать целые предложения. Все шифрованные фразы надо заранее списать и проверить, нет ли ошибок. В письмах следует, безусловно, избегать фамилий, адресов, чисел. Надо твердо помнить пословицу: «Что написано пером, того не вырубишь топором». Письменные документы составляют самые важные доказательства виновности, весьма желательные для жандармов.

Прочитав, следует немедленно сжечь письма деятелей, даже если они были самого неважного содержания, – все таки случаются неопровержимым доказательством сношений. Наоборот, полезно сохранять письма лиц благонадежных: разных школьных товарищей и начальства, знакомство с которыми легко объяснить. Пусть жандармы в случае обыска потрудятся прочесть все эти документы и убедятся, арестованный поддерживает связи и знакомства исключительно легального характера. Если необходимо дома записать какую – либо информацию или адрес, то в этом случае всего пользоваться ключом, известным только пишущему, или же писать, не оканчивая слов и обозначая некоторые из них начальными буквами; удобно также пользоваться аспидной доской, с которой в минуту опасности нетрудно стереть заметки, или, например писать их на клочке промокательной бумаги и иметь её всегда при себе, чтобы в случае надобности проглотить или сжечь. Надо, кроме того, заметить, что нельзя разбрасывать книги и брошюры по квартире, следует их держать их в одном месте, чтобы легче было устранить в минуту в минуту необходимости и быть уверенным, что в квартире не осталось ничего нелегального». [Уральский, 1988].

Таким образом, революционерам предлагалось использовать три способа защиты информации: физическая защита носителя, стеганография и криптография.

В разделе «Поведение во время следствия» давались рекомендации поведения во время ареста и следствия, а так же были изложены законодательные акты, касающиеся порядка ареста, ведения следствия и др. Знание законов должно было помочь арестованному эффективно защищаться и отстаивать свои права.

В разделе «Русское делопроизводство дел политических» разъяснялся порядок судопроизводства в Российской Империи.

В разделе «Порука» разъяснял порядок и условия освобождения на время следствия.

В последнем разделе «инструкции» – «Корпус жандармов и организация шпионов», рассматривались задачи и ме-

тоды работы правоохранительных органов Российской Империи по противодействию революционной деятельности. Особо подчеркивалось, что помимо кадровых сотрудников полиция имеет добровольных помощников и внештатных сотрудников из различных слоев общества (дворников, мелких торговцев, уголовного мира и др.). Эти люди могли вести наблюдение за подозрительными элементами и оказывать содействие правоохранительным органам. Наибольшую опасность для революционеров представляли агенты, внедренные в их среду (их обычно называли провокаторами). Они могли внедряться уже в существующие организации или создавать свои «подставные» кружки, в любом случае информация о революционерах попадала в полицию, а она принимала меры по пресечению их деятельности. Таким образом «инструкция», первый нам известный документ революционеров, в котором систематизировались сведения об их противниках.

Киевские социал-демократы высоко оценили «Инструкцию», однако некоторые высказывали сомнения о возможности практического использования данного документа. Вот, в частности, что писала по этому поводу участница киевского подполья Вера Крыжановская: «Чем интенсивнее работа, тем больше риска провалиться, и потому к вопросу о конспирации мы относились чрезвычайно серьезно. У нас был даже теоретик конспирации В.М. Сапежко – «великий конспиратор», как мы его называли, составивший целую инструкцию для работников подполья; но в его педантичных указаниях многое было не применимо, и потому взять эту инструкцию за руководство было нельзя. Однако многие его указания имели жизненное значение и применены были в дальнейшей подпольной работе» [Синельников].

Что касается шифров, которые использовали социал-демократы в то время, то это были, в основном, шифры многоалфавитной замены, книжные, стихотворные и шифры по слову (описания этих шифрсистем приведены в статье [Бабаш, 2004]). Активно использовалась и стеганография, в качестве невидимых чернил применялись молоко и лимонный сок

а так же такой прием, как сокрытие сообщений в книгах (на заранее оговоренной странице над буквами секретного сообщения карандашом ставились едва заметные точки). Можно заметить, что если в области стеганографии применяли те же способы что и предыдущие поколения революционеров, то в области шифрования использовались нехарактерные для народников шифры (напомним, что народники в основном использовали шифры гаммирования «виженер», «гамбетта» и др.). При правильном использовании многоалфавитные шифры имеют гораздо более высокую стойкость, чем короткопериодическая гамма.

Так сотрудник охранки Леонид Меньшиков в своей книге [Меньшиков, 1932] привел один ключ к шифру московских революционеров, который использовался в конце XIX в. и строился в квадрате по слову «Кулябко». В юности Л.П. Меньшиков участвовал в работе организации «Народная Воля». 5 февраля 1887 г., в возрасте 16 лет он был арестован и обвинен в антиправительственной деятельности. На допросе Меньшиков дал откровенные показания. Позднее в своих мемуарах он утверждал, что сделал это по заданию своей подпольной организации. Цель признания заключалась в том, чтобы завоевать доверие полиции, а затем передавать полученные сведения своим товарищам. В полиции оценили его как перспективного агента и зачислили в штат. Он сделал быструю карьеру – от агента до одного из руководителей особого отдела департамента полиции.

О работе Меньшикова в полиции сложилось противоречивое мнение. С одной стороны, он действительно доставал подпольщикам важные сведения, например, передал революционерам информацию о том, что правоохранительные органы разделяли агентов на несколько категорий, а именно: агенты-пропагандисты, агенты-типографщики, агенты-террористы и агенты-экспроприаторы. Вокруг них объединялись революционеры, и полиция легко могла контролировать их работу. Поставлял Меньшиков и другую ценную информацию.

С другой стороны Меньшиков служил в правоохранительных органах. Благодаря его работе проводились аресты,

а однажды была разгромлена крупная сеть подпольщиков. В результате эффективных действий «черного кабинета» в России были арестованы участники Белостокской[1] конференции представителей комитетов и организаций РСДРП, разгромлен «Северный союз». Основную роль здесь сыграло дешифрование двух писем: первое – от Петербургского «Союза борьбы за освобождение рабочего класса», направленное в редакцию газеты «Искра» (в город Бремен, Германия) и второго направленного из редакции «Искры» в Самару на имя Г.М. Кржижановского. Это позволило полиции определить: место и время проведения конференции, адреса участников, пароли и др. Информацию, способствующую успешной работе криптоаналитиков Департамента полиции, предоставил внедренный в подпольную организацию агент. Им был Л.П. Меньшиков. За эту работу он был награжден орденом.

Обе эти версии не противоречат друг другу. Работая в полиции, Меньшиков обязан был добросовестно выполнять получаемые приказы и одновременно мог снабжать подпольщиков известными ему секретными сведениями.

После увольнения из полиции (в 1909 г.) он уехал из России и сделал ряд сенсационных разоблачений, касающихся методов работы правоохранительных органов Российской Империи (в том числе и по поводу перлюстрации и дешифрования писем подпольщиков). Эта информация оказалась весьма ценной для революционеров. Позднее в 1913 г. Меньшиков опубликовал в парижских газетах очередную статью о деятельности российских «черных кабинетов». На основе статьи Меньшикова появились публикации на эту тему в ряде изданий в России, разразился скандал. Общественность требовала закрытия «черных кабинетов». Департамент полиции применил репрессивные меры к авторам и газетам, опубликовавшим разоблачительные статьи. «Черные кабинеты» не были закрыты, но их деятельность стала еще более законспирированной [Берштейн], [Максимова, 2004].

[1] Более подробно о Белостокской конференции и деятельности ленинской «Искры» будет рассказано в последующих подразделах.

Зубатов
Сергей Васильевич

Важную роль в борьбе против революционного движения сыграл Сергей Васильевич Зубатов. В глазах революционеров Зубатов был злодеем, как его только не называли: «великий провокатор», «отец провокации» и др. Сотрудники правоохранительных органов нередко восхищались его методами работы, называли «гением политического сыска».

С.В. Зубатов родился в Москве в 1864 г. Уже в гимназии Зубатов участвовал в работе революционного кружка. По ходатайству отца в 1882 г. исключен из 6 класса гимназии. Будучи офицером, отец захотел вырвать Сергея из народовольческой среды. С этой же целью в 1883 г. по настоянию отца Зубатов женился дочери армейского офицера А.Н. Михиной. Однако Зубатов не прекратил заниматься революционной деятельностью, мало того он привлек к ней супругу, в библиотеке тестя они организовали революционный кружок. В 1883 г. арестован полицией и освобожден под залог. В 1885 г. Зубатов был завербован лично начальником Московского охранного отделения Н.С. Бердяевым, которому удалось убедить молодого человек в опасности революционных процессов для России. С этого момента Зубатов стал негласным агентом охранки и передавал полиции информацию о своих товарищах. По настоянию полиции Зубатов работал на Московской центральной телеграфной станции, возможно там Зубатов занимался перлюстрацией телеграфных сообщений. Благодаря информации, полученной от Зубатова о «преступной деятельности членов кружков революционеров-бомбистов» [Лурье] 2 мая 1887 г. было арестовано более 200 человек. Узнав о разоблачении Зубатова революционерами, 13 июня 1886 г. он был выведен из агентурной работы и стал штатным сотрудником

московского охранного отделения. Интересно отметить, что в 1911 г. Л.П. Меньшиков в открытом письме министру внутренних дел Столыпину, вспоминая свой арест, писал: «С самого начала моего сидения в тюрьме в мою душу закралось подозрение, что я сделался жертвую доноса. Моя догадка нашла себе подтверждение. Очень скоро выяснилось, что я и многие другие были арестованы в следствие предательства одного молодого человек. Имя этого господина Вам должно быть известно; министерство, во главе которого Вы числитесь платит ему ныне 5000 рублей ежегодной ренты. Это был С.В. Зубатов» [Лурье].

С 1886 по 1894 г. Зубатов – сотрудник московской охранки, а 1894 по 1896 гг. он находился в должности помощника начальника московского охранного отделения, а затем и возглавил его.

Как человек, талантливый, думающий, знающий не понаслышке проблемы революционного движения изнутри, Зубатов становится в буквальном смысле новатором своего дела, а заняв руководящий пост, получил возможность реализовать свои идеи в оперативно-розыскной деятельности. Зубатов принципиально меняет подходы к политическому сыску, к целям и задачам оперативной деятельности. Зубатов переходит от хаотичного, неэффективного и в известной степени консервативного сыскного ремесла к принципиально иному, основанному на прогнозе, аналитической работе, глубоком знании предмета, стремлении упредить и нейтрализовать в нужный момент наступление тяжких последствий. Более того, многое, если не большинство из придуманного им стало азбукой сыска. Для контроля за революционными группами Зубатов приказывал арестовывать только их руководящие звенья, рядовых участников оставляли «на разводку». Лишь в исключительных случаях, когда, например, замышлялось убийство видного чиновника или готовилось покушение на лиц императорской фамилии или крупный теракт, полиция полностью ликвидировала организацию. Такая система борьбы с революционным движением впоследствии была принята всеми охранными отделениями и жандармскими управлениями.

И здесь был отнюдь не злой или особо коварный умысел. Масса участников революционных групп выполняла роль статистов, вся их вина состояла только в том, что они разделяли оппозиционные взгляды. Тотальные зачистки ничего, кроме компрометации власти, дать не могли. Аресты лидеров на время парализовали действия революционной организации. Зубатов увидел и осознал главное, что существовавший тогда принцип «держать и не пущать» не просто устарел, а стал вредным. Старый полицейский аппарат был практически обречён на неуспех, так как влившиеся в революционное движение люди были молоды и значительно образованнее своих противников, работавших в охранных структурах. Зубатов заложил принципиально новые подходы к агентурной деятельности, создав так называемый институт внутренней агентуры. Он создал мощную разветвлённую сеть своих агентов на самых ключевых участках, откуда исходила угроза для государственной и общественной безопасности России, в первую очередь террористического характера. При этом Зубатов увидел в марксизме, который набирал силу в политической жизни страны, серьёзнейшую опасность для самих устоев Российской Империи, и по этому предпринимал все меры для уничтожения этой угрозы изнутри. Он был фактически первым, кто обратил внимание на деятельность социал-демократии и лично В.И. Ленина. Являясь убежденным монархистом, он обратил внимание своего руководства на то, что главную опасность представляют не столько эсеры – «бомбисты», сколько социал-демократы – противники индивидуального террора как недостаточно действенного революционного способа борьбы.

В своей работе Зубатов сталкивался со значительными трудностями. Консервативная часть чинов полиции яростно сопротивлялась новшествам в сыскном деле. Многие из сотрудников охранки на тот момент были малообразованы и заскорузлы в своём мышлении, процветала бюрократия, некоторым руководителям уже давно было пора на пенсию, но они продолжали цепляться за «хлебные места». По этим причинам внедрение новых методов работы нередко откровенно саботировалось.

Тем не менее активная работа продолжалась. «Сейчас вопрос стоит так, – убеждал Зубатов Великого князя Сергея Александровича (тогдашнего московского генерл-губернатора – *авт.*), – кто владеет этим рабочим движением: мы или социалисты? Если им владеют социалисты, революция в России будет неизбежна». [Михайлов, 2003].

Идея Зубатова состояла в создании легальных рабочих организаций, действовавших под контролем правоохранительных органов и активного внедрения агентуры в революционное подполье. Легальные кружки должны были отвлекать рабочий класс от политической борьбы подменяя политические требования экономическими.

Эту идею экономического просвещения рабочих поддержали на самом верху. Концепция Зубатова содержала четыре основных принципа:

- отрицание всех форм и методов насилия, замена революционного движения «эволюционным»;
- самодержавная форма правления – «внеклассовая» – в области социальных отношений включает в себя «третейское начало, склонное к справедливости»;
- противопоставление профессионального движения, не отрицающего капиталистического строя, рабочему движению, исходящему из социалистических начал;
- строгое разграничение самодеятельности власти. Самодеятельность ограничивается там, где начинаются права власти. Всё должно идти через власть и ею направляться. [Михайлов, 2003].

Зубатов, вынашивая планы борьбы с революционным движением, также считал необходимым работать в массах рабочих. Он внимательно изучал произведения Маркса, а также критиковавшего его немецкого социал-демократа Бернштейна и других европейских и отечественных авторов, специалистов по истории и практике реформистского профсоюзного рабочего движения. Зубатов решил приспособить западные идеи к российским условиям. В результате он оказался инициатором создания государственного реформистского рабо-

чего движения, построенного по профессиональному принципу, и считал, что можно допустить любые экономические способы борьбы вплоть до стачек, если в них не будет явной политики или уголовщины. Одна такая стачка на заводе французского подданного Гужона в Москве настолько обострила отношения между хозяином и рабочими, что Зубатов, используя авторитет и поддержку московского генерал-губернатора, начал дело по высылке из России предпринимателя-иностранца Гужона, не пожелавшего идти на уступки русским рабочим. Самым большим успехом Зубатова стала, организованная им, десятитысячная манифестация московских рабочих, состоявшаяся 19 февраля 1902 г.

С.В. Зубатов осознавал острую необходимость информационного обеспечения оперативно-розыскной деятельности, он утверждал: «Охранение общественной безопасности невозможно без политического розыска, а розыск без информации – это гончая собака без нюха». [Михайлов, 2003].

После назначения в октябре 1902 г. начальником Особого отдела Департамента полиции Зубатов стал продвигать своих единомышленников и подчинённых по Московскому охранному отделению в столичные полицейские учреждения. Быстро рос архив ведомства. Активно велась регистрация лиц, связанных с революционной деятельностью. Составлялись своеобразные «базы данных» о революционных движениях, изучались их цели, политические платформы, методы борьбы, огромное внимание уделялось выявлению разногласий между революционерами. Вся эта информация доводилась до руководства полиции в столице и на местах. Всё это служило серьёзным подспорьем при дознании, разработке оперативных мероприятий, при составлении учебных пособий для курсов по подготовке сотрудников правоохранительных органов. Одним из главных источников информации про революционеров по-прежнему были перехват, перлюстрация и дешифрование писем революционеров и донесения агентуры.

Зубатов вкладывал значительные средства в поощрение действий сотрудников полиции, добившихся хороших ре-

зультатов. Впрочем, справедливости ради надо отметить, что система исключительных награждений существовала и ранее. Однако страсть некоторых чинов правоохранительных органов к материальному обогащению таила в себе огромную опасность. Они стали стимулировать не процесс по оздоровлению общества и пресечение крамолы, а, наоборот, имитировали развитие революционного движения, которое они «благополучно» пресекали. Фактически стимулировалось самое большое зло, которое впоследствии и явилось основой для осуждения действий Зубатова. Взлёт Зубатова на вершину полицейской карьеры фактически и был её концом. В августе 1903 г., Сергей Васильевич Зубатов был отстранён от занимаемой должности, без суда и следствия отозван в Москву, где находился под гласным надзором полиции, а в октябре был сослан во Владимир. Осенью 1904 г. уже после убийства министра внутренних дел Плеве, о возможности которого Зубатов предупреждал, его вызывают в Санкт-Петербург. Он объясняется, его реабилитируют. Ему дают пенсию, снимают гласный надзор, но на службу не возвращают. Отставка Зубатова повлекла за собой отставку его команды. Пришедшие им на смену руководители правоохранительных органов не смогли справиться с «прикормленными» революционерами, что породило таких деятелей как Гапон, Азеф и пр. Об их деятельности будет рассказано позже. В феврале 1917 г. после отречения Романовых от престола, С. В. Зубатов, искренне и верно служивший российской монархии, покончил жизнь самоубийством [Берштейн], [Максимова, 2004], [Овченко, 2003].

Теперь же рассмотрим ряд операций проведенных в 1898 г. московским охранным отделением возглавляемым С.В. Зубатовым связанных с криптографией.

В конце февраля 1898 г. агенты службы наружного наблюдения Московского охранного отделения в Харькове[1] вышли на след лидера киевского подполья Бориса Эйдельмана.

[1] Напомним, что под юрисдикцией Московского охранного отделения на тот момент находилось 13 губерний.

27 февраля филеры проследовали за ним из Харькова в Минск. На следующий день по прибытии в Минск была зафиксирована встреча Эйдельмана с одним из членов центрального комитета (ЦК) БУНДа Абрамом Мытниковичем (он же Мутник). За ним тоже было установлено наблюдение, но на некоторое время им удалось оторваться от слежки. Шла завершающая стадия подготовки съезда, но полиция еще не знала об этом. После завершения работы съезда делегаты быстро покинули Минск, однако многие были зафиксированы службой наружного наблюдения. Под руководством Зубатова развернулась масштабная операция по отслеживанию перемещений и выявлению связей революционеров. В ночь с 11 на 12 марта в Киеве, Москве, Екатеринославе и многих других городах были произведены массовые аресты. Только в Киеве было задержано 175 человек. А всего в 27 городах Российской Империи в руки правоохранительных органов попало 500 социал-демократов [Синельников]. В руки полиции попало множество нелегальной литературы, различной документации (в том числе шифрованные письма, открытые тексты, ключи к шифрам) революционеров, в Екатеринославле была обнаружена типография киевской организации. У оказавшегося среди задержанных Б. Эйдельмана полиция обнаружила вышеописанную «инструкцию». Это был ценный трофей, позволивший правоохранительным органам ознакомится с методами конспиративной деятельности российских социал-демократов [Уральский]. В Москве был арестован «перекрещенный еврей Константин Константинов (на самом деле это был один из первых российских марксистов-нелегалов Владимир Перазич – *авт.*) … При нем оказалась масса подпольных изданий, рукописные документы и… шифр для сношений» [Синельников].

В ходе дальнейшего наблюдения Мытниковичем полиция зафиксировала его встречи с А. Кремером, также членом ЦК еврейской подпольной организации. Наблюдение за этими людьми позволило выявить значительное количество участников БУНДа. В июле 1898 г. С.В. Зубатов принимает решение о ликвидации БУНДа. Были проведены массовые аресты,

среди задержанных все члены ЦК еврейского Союза, множество рядовых бундовцев, разгромлена типография в Бобруйске. Среди прочих трофеев полиция конфисковала у ряда арестованных листы бумаги с числами. Сразу же возникли подозрения, что это шифр, материалы были направлены в особый отдел департамента полиции и дешифрованы там И.А. Зыбиным. Полученная информация оказалась очень важной, в руки полиции попали списки членов БУНДа, получавших нелегальную литературу. На основании, полученных сведений были произведены новые аресты, всего было задержано более 70 человек. Однако полностью разгромить организацию еврейских социал-демократов не удалось, БУНД напоминал гидру у которой вместо отрубленной головы вырастали две новые. Вот, что по этому поводу начальник особого отдела департамента полиции Л. Ратаев писал Зубатову в июле 1900 г., т.е. спустя 2 г. после описываемых событий: «Не могу не остановить Вашего внимания на одной характерной особенности. На вид розыск ведется успешно, параллельно с точным агентурным указанием, и приводит к желанным результатам, т.е. к обнаружению подпольных типографий, со всеми вещественными доказательствами и соприкасающимися к оным революционными группами. Тем не менее, движение не только не ослабевает, а напротив, разрастается, на смену одной типографии через месяц появляется другая, взамен ликвидированной группы вырастает другая, еще более серьезная и обширная. Такая особенность, по моему мнению, указывает на то, что в пределах еврейской оседлости революционным движением руководят строго замкнутые комитеты, которые, не принимая непосредственного активного участия, остаются нетронутыми и после ликвидации одной революционной группы немедленно пополняют поредевшие ряды» [Синельников].

Тем не менее по социал-демократическому движению был нанесен очень сильный удар и опять, как у предыдущих революционных организаций, во многом причиной провалов была слабая стойкость шифров, которые применяли революционеры. К сожалению, понимание этого пришло к ним спус-

тя многие годы. Вот, что пишет об этом в своих мемуарах, написанных во второй половине XX в., один из участников петербургского подполья конца 1890-х – начала 1900 гг. Станислав Струмилин (Струмилло-Петрашкевич):

«В нашей группе был в ходу, между прочим, такой весьма элементарный метод шифровки. Ключом к шифру избиралось какое-нибудь слово, например, «Халтурин». Выписав это слово один или два раза акростихом по вертикали и продолжив каждую строку следующими буквами, в порядке алфавита, по горизонтали, мы получали в квадрате 9 × 9 = 81 букву алфавита, годную для любой шифровки. Каждая буква в этом квадрате обозначается двузначной цифрой, указывающей ее место в горизонтальном и вертикальных рядах. Так допустим, что требуется расшифровать запись:

22 26 31 82 36 51 79 34 23 83 61 34 23 82 72 21 41 76 36.

Строим по ключу «Халтурин» указанный квадрат:

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	Х	ц	ч	ш	щ	ы	э	ю	я
2	А	б	в	г	д	е	ж	з	и
3	Л	м	н	о	п	р	с	т	у
4	Т	у	ф	х	ц	ч	ш	щ	ы
5	У	ф	х	ц	ч	ш	щ	ы	э
6	Р	с	т	у	ф	х	ц	ч	ш
7	И	к	л	м	н	о	п	р	с
8	Н	о	п	р	с	т	у	ф	х
9	Х	ц	ч	ш	щ	ы	э	ю	я

Затем, определяя букву за буквой в этом квадрате по номеру строки и месту в ней буквы, расшифровываем всю запись: «*Белорусов провокатор*». В свое время этот шифр казался нам очень остроумным и надежным. Но после первого же ареста обнаружилось, что его расшифровали жандармы. И в этом не было особой премудрости. Пороком шифра был алфавитный порядок букв в каждой строке квадрата. Угадав лишь одну букву, вы владели всей строкой шифра. В самом деле. Ис-

ходя из более чем вероятного предположения, что в ключе шифра, т.е. в первой вертикали квадрата должна найти себе место первая буква алфавита и что она непременно встретится и в записи, мы находим в ней только пять цифр из первой вертикали: 21, 31, 41, 51 и 61. Одна из этих цифр, значит, обозначает букву А. Пробуя их одну за другой, мы уже при первой пробе – второй строки – раскрываем пять букв нашей записи: 22, 26, 23, 23 и 21 и получаем: «Бе … в … в … а …». Допуская далее, что первое «В» в этом тексте заканчивает собой фамилию на «ов», раскрываем уже и всю третью строку шифра, в которой буква «О» занимает четвертое место. Вместе с тем расшифровывается еще пять букв записи: 31, 36, 34, 34 и 36. Подставив их на свое место в текст, получим: «Бел … р … ов … в … а … ор», после чего дальнейшая расшифровка представляет собой уже совершенно детскую задачу. После букв «Бел» сама напрашивается буква «О», обозначенная в записи цифрой 82, откуда раскрываем всю 8-ю строку шифра и, дополняя наш текст еще тремя буквами (82, 83 и снова 82), получаем: «Белор…ов п…ово… а …ор». Полагаю, что любой жандарм, знающий свою агентуру, прочел бы такую запись уже без запинки» [Синельников].

Как видим, автор этой цитаты «моделирует» возможные действия полицейских криптоаналитиков, однако попытки криптоаналитической оценки используемых шифров в то время практически не предпринимались революционерами. Так же в своих мемуарах Струмилин упоминает действующие в Петербургском «Союзе борьбы» средства стеганографической защиты информации, традиционные молоко и лимонный сок.

Теперь перенесемся из европейской части России в далекую Сибирь. Находящийся в ссылке в селе Шушенском В.И. Ленин вовсе не собирался прекращать революционную деятельность. Вот что вспоминает о работе Ленина во время ссылки один из его соратников Фридрих Ленгник: «Наряду с углубленной литературной работой Владимир Ильич принимал самое деятельное участие в установлении самых оживленных сношений с группой «Освобождение труда», … а так же пере-

писывался с Петербургом, Москвой и другими российскими городами и с товарищами по ссылке, с которыми он находил время переписываться в виде длиннейших писем, в которых освещались иногда очень сложные и интересные вопросы революционного движения…» [Синельников].

Разумеется, конспиративная переписка шифровалась, В.И. Ленин и его товарищи в то время использовали книжный шифр многоалфавитной замены. В качестве ключей использовались страницы двух легально изданных в России книг Г.В. Плеханова. Для связи с группой «Освобождение труда» (основным корреспондентом Ленина был П. Аксельрод) использовалась книга Н. Бельтова «К вопросу о развитии монистического взгляда на историю»[1], напомним, что об этой книге-ключе Ленин и Аксельрод договорились еще во время заграничной поездки Владимира Ильича в 1895 г. Для связей с корреспондентами внутри Российской Империи использовалась книга А. Волгина «Обоснование народничества в трудах г-на Воронцова (В.В.)». Об этом Ленин с товарищами договорился перед отъездом в ссылку в феврале 1897 г. Кстати заметим, что эта книга использовалась в качестве ключа ленинским крылом РСДРП довольно длительное время – до конца 1905 г.

В мае 1898 г. в Шушенское приезжает Надежда Константиновна Крупская, которая вскоре становится женой В.И. Ленина. Крупская активно помогала мужу в его революционной работе, в частности она взяла на себя ведение конспиративной переписки будущего вождя мирового пролетариата, Надежда Константиновна стала личным шифровальщиком Ленина на долгие гг. нелегальной работы.

А вот что вспоминает о конспиративной переписке с Лениным его сестра Анна Ильинична: «Переписка с Ильичом шла у меня в те гг. все время самая деятельная… Во время моей летней поездки за границу (1897 г.) я познакомилась с членами группы «Освобождение труда», отвезла им привет от Владимира Ильича… Речь шла о том, чтобы он посылал писа-

[1]Обе книги Плеханова были изданы в России под псевдонимами.

ния для рабочих за границу… и обсуждался вопрос, каким образом наладить это. Владимир Ильич писал, что знает только один способ – химией, но что трудно найти переписчика. Аксельрод считал этот способ чересчур кропотливым… Некоторые работы… были переправлены, тщательно заделанные в переплетах… Даже личная переписка с Аксельродом ни у Ильича, ни у меня регулярно не установилась. Вообще Аксельрод был очень неаккуратен и рассеян в отношении переписки… Все более интересное… я, ездившая время от времени в Петербург, …описывала Ильичу (химией) на листах каталогов, ненужных книг, последних страничках журналов, иногда даже не разрезанных, чтобы еще больше отдалить подозрение в возможности каких-либо шифрованных сообщений. Ни разу, за все три г. ссылки Ильича, ни одно из таких писем не пропало, не обратило на себя внимания. Никто, кроме самых близких людей, не знал, каким способом идет переписка… Все имена, кроме того, шифровались» [Синельников]. Как видим Ленин и его соратники продолжали использовать методы защиты информации, выработанные во время поездки Владимира Ильича за границу. Криптографическая защита осуществлялась книжным шифром, стеганографическая – применением невидимых чернил и маскировкой в переплетах, интересно отметить, что на рубеже веков социал-демократы использовали в качестве невидимых чернил самые простые вещества (при этом А.И. Елизарова упоминает, что при использовании молока, его надо было разбавлять водой, так как буквы, написанные слишком густым продуктом написанные молоком могли «самопроявиться»), ни о какой более сложной «химии» речь не шла, хотя как мы помним, те же народники использовали раствор поваренной соли, крахмал – проявляемый раствором йода, железисто-синеродистый калий и другие химические вещества.

По возвращении А.И. Елизаровой из заграницы в сентябре 1897 г. ее деятельностью заинтересовалась полиция. Сестра Ленина тогда проживала в Москве и через подставной адрес в немецком городе Штутгарте вела нелегальную пере-

писку с П. Аксельродом. Корреспонденция А.И. Елизаровой регулярно перлюстрировалась. Иногда из даже открытой переписки правоохранительным органам становилось известно о типе используемых революционерами шифрсистем. Вот, например, какое агентурное донесение было направлено начальником особого отдела Департамента полиции Л. Ратаевым в московское охранное отделение к С.В. Зубатову.

«10 февраля 1898 г. Совершенно доверительно.

… 7 сего февраля по известному Вам адресу на имя Бабеты Вагнер в Штутгарт отправлено письмо, писанное печатными буквами, следующего содержания: «В письме опять лишь начало можно было разобрать. Но из того, что начало вполне верно, видно, что дело совсем не в издании, а лишь в небрежном отношении к делу. Можно было прочесть лишь о том, что Вы не можете исполнить моего поручения, – только теперь собрались ответить… с октября просим и ждем… Дальше же идет след.: «*агобо Вы изо революции и пришлите сюда озвенокилезтууаах*» … Разобрать такую тарабарщину не имею ни времени, ни желания…». Сообщая об изложенном, долгом считаю добавить, что вышеприведенное письмо … будет отправлено по назначению. Подписал: Л. Ратаев» [Синельников]. Из агентурных сведений жандармам было известно, что адрес Бабеты Вагнер использовался для переписки с Россией группой «Освобождение труда», а цитируемое письмо принадлежало Анне Елизаровой. Нетрудно заметить, что речь опять идет об использовании книжного шифра.

Срок сибирской ссылки В.И. Ленина истек 29 января 1900 г. Ссылка продолжалась почти 3 г. за это время благодаря огромной теоретической и литературной работе Ленин становится одним из ведущих марксистов России. За гг. тюрьмы и ссылки Владимир Ильич и его соратники приобрели огромный конспиративный опыт. До этого им не доводилось в таком объеме вести нелегальную переписку, используя стеганографию и криптографические средства защиты информации. В.И. Ленин намеривался продолжить революционную борьбу, он тщательно продумывал свои дальнейшие планы, списывался.

Именно в Шушенском был разработан знаменитый проект создания марксистской партии в России вокруг нелегального печатного органа, издающегося за пределами Российской империи, этим органом стала газета «Искра». Дальнейшая криптографическая деятельность российских революционеров будет рассмотрена в следующих подразделах.

5.6. Криптографическая деятельность революционеров в России. Полиция против революционеров

Рассказ о криптографической деятельности русских революционеров был бы не полон без освещения работы тех, кто с ними боролся – правоохранительных органов Российской Империи. В предыдущих подразделах было рассказано о некоторых силовых структурах и неоднократно приводили эпизоды работы полиции по пресечению криптографической деятельности революционеров. Однако далее будет рассказано о некоторых людях и спецслужбах подробнее.

В статье [Гольев, 2006] рассказано об образовании особого отдела департамента полиции. В этой организации справедливо полагали, что развитие социал-демократического движения вызовет активизацию «подпольной» переписки. В качестве одной из первоочередных задач сотрудникам отдела была указана «организация перехвата и перлюстрации корреспонденции социал-демократических организаций в «черных кабинетах», экспертиза почерков по перехваченным письмам и рукописным документам с целью установления их авторов, проявление «химических» посланий и дешифровка зашифрованных писем» [Уральский, 1988]. Эта работа считалась чрезвычайно важной. Помещения почтовой цензуры тщательно изолировались от остальной части почтамта. Вход в «черный кабинет» разрешался только лицам непосредственно занятым перлюстрацией. В качестве цензоров подбирались наиболее благонадежные чиновники, с высшим образо-

ванием и свободно владевшие иностранными языками. Перлюстраторы самым тщательным образом исследовали книги, их переплеты и корешки. Искались возможные ключи к книжным шифрам, стеганографические послания и тайники.

Лица, вызывавшие интерес у правоохранительных органов оказывались под самым плотным контролем, за ними устанавливалось наружное наблюдения, в их круг общения внедрялась агентура. Вот что об этом пишет член комиссии Временного правительства по изучению архивов полиции М.А. Осоргин: «Вы окутывали себя вуалем конспирации, вы шептали свою тайну на ухо ближайшему другу, вы переписывались своим шифром по условному безопаснейшему адресу, и днем позже ваш шепот переписывался на машинке, ваш шифр подшивался к делу, а почтовое ведомство посылало в агентурный отдел письма на условный адрес. Ибо даже тяжелый и долгий революционный опыт не выкуривал из нас излишней доверчивости... Есть весьма видные и искренние революционные деятели, круг ближайших соратников и друзей которых состоял на 50–75% из провокаторов. Это может быть подтверждено документами, совершенно неопровержимыми» [Осоргин, 1917].

В 1918 г. в своем журнале «Былое», издававшимся в Париже известным историком и революционером В.Л. Бурцевым приводилась следующая характеристика деятельности российской цензуры в 1903 г.: «Перлюстрация частной корреспонденции служила для органов самодержавной бюрократии не только приемом чисто политической борьбы с политическими противниками, но также и источником ознакомления правящих кругов с подлинным настроением общественного мнения…» [Уральский, 1988]. Перлюстрация приняла тотальный характер. Перехватывались письма всех отправителей и адресатов, какое бы положение они не занимали в обществе. Среди них были и видные деятели культуры того времени Л.Н. Толстой, А.М. Горький, А.И. Куприн, В.И. Немирович-Данченко и др. В связи изложенным упомянем один исторический эпизод. Летом 1888 г. известный русский писатель А.П. Чехов отдыхал в городе Сумы в усадьбе семьи Линтаревых. Сво-

им корреспондентам Чехов дал адрес этой усадьбы, попросив направлять на него письма. Либеральная семья Линтваревых была «на подозрении» у полиции, и ее почтовая переписка контролировалась. В одном из своих писем к своему издателю А. Суворину Антон Павлович писал: «Отвечаю на Ваше письмо, которое получено мною только вчера; конверт у письма разорван, помят и испачкан, чему мои хозяева и домочадцы придали густую политическую окраску» [Бабаш, 2004]. Позднее Чехов и сам попал в список Департамента полиции «по наблюдению»[1]. В своих письмах во время поездки на Сахалин он отмечал, что замечает явные следы перлюстрации на полученной корреспонденции.

Следует отметить, что с формальной точки зрения перлюстрация была делом противозаконным и уголовно наказуемым. Так ст. 1104 действовавшего Уложения о наказаниях предусматривала отстранение почтового служащего от должности за распечатывание письма «хотя из одного только любопытства», а «если содержание письма будет сообщено другому», то предусматривалось заключение в тюрьму на срок от 4 до 8 месяцев. А согласно ст. 1102, если почтовый чиновник «из-за каких-либо видов согласится с кем-либо передавать ему письма, адресованные на имя другого лица без позволения последнего», то он приговаривался к тюремному заключению или ссылке на поселение [Соболева, 2002].

Следует отметить, что перехват и перлюстрация сообщений революционеров велись не только на территории Российской Империи, этим занималась и заграничная агентура департамента полиции. Так, например, в конце XIX в. парижская агентура получила указание об усилении работы против активно действовавшей в то время в Западной Европе революционной марксисткой группы «Освобождение труда». Во главе агентурной сети департамента во Франции тогда находился П. Рачковский. В 1888 г. он в своем докладе в Санкт-Петербург указывал на необходимость организации в Женеве

[1] Подробнее о списках Департамента полиции в статье [Гольев, 2005-2].

(Швейцария) систематической перлюстрации корреспонденции видных политических эмигрантов Г.В. Плеханова, В. Засулич и др. Это предложение было принято. Позднее заграничная агентура (в первую очередь в Австро-Венгрии и Германии) осуществляла активный перехват переписки, которую вела революционная газета «Искра» со своими корреспондентами.

Особое внимание при перлюстрации уделялось сокрытию этих действий, получатели корреспонденции не должны были знать, что их переписка отслеживается. Однако в некоторых случаях правоохранительные органы вынуждены были идти на риск. Так, например, перехваченные в 1901 г. письма Н.К. Крупской одесским революционерам после их проявления (они были написаны «химией») и дешифрования были направлены в Париж, руководителю агентурной сети департамента полиции со следующим сопроводительным письмом: «Я умышленно посылаю Вам подлинные письма в том предположении, что, может быть, агентура по почерку признает автора сих писем… Все подобные письма калькируются, воспроизводятся химическим способом и отправляются по назначению» [Уральский, 1988].

Деятельность «черных кабинетов» была достаточно эффективной. К этому выводу привел последующий анализ тяжелых последствий, массовых арестов революционеров-подпольщиков. Так, например, дешифрованная переписка К. Захаровой из Одессы, поддерживающей связь с находившейся в тот момент за границей Н.К. Крупской, привела к аресту одесских социал-демократов и пресечению пути транспортировки газеты «Искра» через Болгарию.

Несмотря на принимаемые меры, иногда революционерам удавалось обнаружить факт перлюстрации своей переписки. В 1902 г. Н.К. Крупская в одном из писем в Москву сообщала о том, что письмо, написанное химическими чернилами, было проявлено и потом вновь восстановлено. В связи с этим Крупская убеждала адресата как можно быстрее скрыться из Москвы. Также информацию об обнаружении фактов перлюстрации Надежде Константиновне сообщали корреспонденты «Искры» с мест.

В департаменте полиции, куда поступала шифрперепи-ска из «черных кабинетов» и иногда от министра внутренних дел, шел процесс обработки полученных материалов: регистрация (каждое перехваченное письмо получало свой номер, простые и стеганографические («химические») письма регистрировались раздельно: первые просто получали номер, к номеру химических прибавлялась буква «Х», фамилии, упоминаемые в письмах, заносились в картотеку. Именные карточки составлялись на автора письма, получателя, на все имена и фамилии, упоминаемые в письме. Так подробно расписывались только письма революционеров. Письма государственных и общественных деятелей редко проходили такую обработку, они обычно не регистрировались, подшивались в отдельные дела в порядке хронологии проявление стеганографических текстов и дешифрование (при необходимости), копирование, размножение копий. На основании полученных сведений при содействии подразделений правоохранительных органов на местах выяснялись личности корреспондентов, их адреса, проводились оперативные мероприятия, аресты и обыски [Соболева, 2002].

Перехваченные материалы поступали в 5 отделение Особого отдела Департамента полиции, где велась работа по политическим партиям, существовавшим в Российской Империи. Копии писем, касавшихся деятельности эсеров, анархистов, а также других террористических организаций, направлялись во 2 отделение Особого отдела, отвечавшее за борьбу против них. Материалы по социал-демократическим организациям шли в 3 отделение, национальными революционными организациями занималось 4 отделение. В этих подразделениях велась дальнейшая разработка шифрпереписки для проведения оперативных и следственных мероприятий. Это была кропотливая и сложная работа, требующая глубокого знания структуры и методов работы революционного подполья. Изучая впоследствии эту работу российских правоохранительных органов, М.А. Осоргин писал, что при работе с перлюстрационными материалами устанавливались «не толь-

ко адрес, но и каждое лицо, упомянутое в письме, иногда только уменьшительным именем, одной буквой или описательным выражением» [Осоргин, 1917], [Соболева, 2002]. Копии дешифрованных писем передавались в распоряжение правоохранительных органов в различных регионах страны для выявления лиц, участвующих в революционной деятельности, установки за ними наблюдения, принятию мер по пресечению деятельности революционеров др.

Следует подчеркнуть, что департамент полиции строго сохранял тайну деятельности своей дешифровальной службы. Полученные в результате дешифрования материалы никогда не использовались в судебных процессах против революционеров, а применялись лишь на стадии следствия. Попытки использования дешифрованных материалов в ходе судопроизводства жестко пресекались руководством МВД. Приведем ряд примеров.

В 1908 г. из уфимского окружного суда тогдашнему начальнику особого отдела департамента полиции были направлены шифрованная записка и ключ к шифру. В сопроводительном письме, подписанном судебным следователем, излагалась просьба расшифровать письмо, сообщить, какая подпольная организация пользуется таким шифром, и дать возможность допросить в качестве эксперта сотрудника особого отдела, который будет проводить дешифрование. Через некоторое время в Уфу были направлены материалы, в которых сообщалось содержание шифрованного письма, приводилось краткое описание шифра (достаточно распространенного), но категорически отказывалось в возможности допроса специалиста-криптоаналитика [Соболева, 2002].

Начальник Лифляндского губернского жандармского управления попросил выслать ему перехваченное письмо для ознакомления с почерком, руководство департамента полиции напомнило ему, что согласно «Положению о государственной охране», письмо не может быть предъявлено посторонним лицам, невзирая на их служебное положение, а также не может быть приобщено к дознанию.

В 1915 г. допросить криптоаналитиков особого отдела пожелал судебный следователь из Витебского уезда. По приказу директора Департамента полиции прокурору Санкт-Петербургской судебной палаты было направлено письмо с просьбой одернуть провинциального следователя. В письме указывалось, что «...разоблачение произведшего дешифровку лица является для Департамента полиции по особым соображениям весьма неудобным» [Соболева, 2002].

В связи с выше изложенным, в последние годы существования Российской Империи заинтересованность в специалистах-дешифровальщиках проявили органы юстиции. В июле 1915 г. проходил съезд управляющих кабинетами научно-судебной экспертизы при прокурорах судебных палат. На съезде внимание присутствующих было обращено на то, что этим кабинетам нередко приходится иметь дело с расшифровкой документов. Не имея специальной литературы и соответствующих руководств, сотрудникам кабинетов самим приходилось изыскивать способы и приемы дешифрования. Съезд принял решение о временном командировании чинов кабинетов в департамент полиции, МИД и военное министерство для ознакомления с практиковавшимися приемами дешифрования, имея в виду, что в этих ведомствах накоплен по данному вопросу уже большой опыт. Однако само Министерство юстиции не торопилось выполнять решение съезда. Лишь через 1 год, в июле 1916 г., было направлено письмо начальнику особого отдела департамента полиции Е.К. Климовичу с просьбой допустить сотрудника московского кабинета Русецкого на стажировку в департамент и ознакомить его с наиболее распространенными видами шифров и приемами их разбора. Такое разрешение было дано. Но революционные события 1917 г. не позволили организовать дешифровальную службу в министерстве юстиции.

Следует отметить, что в конце XIX – начале XX вв. в департаменте полиции служил ряд талантливых криптографов-дешифровальщиков. Расскажем об одном из них. В середине 1890-х гг. на службу в Департамент полиции на должность пи-

саря поступил молодой человек, которому вскоре суждено было стать одним из ведущих криптоаналитиков своего времени. Это был Иван Александрович Зыбин. Не имея никакого специального образования (он окончил обычную гимназию), Зыбин к началу 1901 г. стал ведущим специалистом-дешифровальщиком в МВД Российской Империи. В скором времени он фактически возглавил дешифровальную службу Особого отдела Департамента полиции. Это стало возможным благодаря таланту, интуиции, стремлению к знаниям (Зыбин активно занимался самообразованием) и трудолюбию Ивана Александровича. Приведем ряд цитат характеризующих криптоаналитические способности Зыбина, вот что сказано о нем в книге [Соболева, 2002]: «Работая в области дешифрования переписки революционного подполья, Зыбин естественно накопил огромный теоретический и практический опыт. Кроме того, являясь от природы личностью высокоодаренной, обладая прекрасной памятью, Зыбин к тому же был широко образован, что позволяло ему получать сведения о шифрах не чисто научно-аналитическим способом, а с помощью косвенных сведений. Именно Зыбин ввел в практику чинов полиции, производивших арест или обыск революционеров, обычай тщательно искать среди имевшихся у них книг именно те, которые могли представлять интерес для Зыбина-дешифровальщика (эти материалы нужны были для дешифрования книжных шифров – авт.)». В качестве примера можно привести отрывок из письма Зыбина начальнику саратовского губернского жандармского управления от 7 февраля 1910 г.: «…Отобранные по обыску у мещанина Николая Сергеевича Кузнецова записки зашифрованы 4, 15, 25, 29 и 35-й страницами какой-то неизвестной книги и разбору не поддаются по недостаточности материала. Прошу Ваше Высокоблагородие уведомить в самое непродолжительное время, не было ли обнаружено по обыску у названного Кузнецова, кроме означенных записей, какого-либо издания или легальной книги с пометками на отдельных страницах или загрязненных более других какой-либо страницей от частого, сравнительно с дру-

гими, употребления и, кроме того, не встретилось ли одно и то же издание у прочих лиц, принадлежащих к одной с Кузнецовым организации, так как подобное явление в большинстве случаев указывает, что таковое издание служит ключом для шифрованных сообщений» [Соболева, 2002]. Приведем другой пример. Во время налета полиции на один из домов в Севастополе, в котором предполагалось нахождение революционеров, была обнаружена шифрованная записка. Руководство департамента полиции передало ее Зыбину для дешифрования. Зыбин предположил, что для шифрования здесь был использован книжный шифр и затребовал доставить к нему все книги, обнаруженные в доме. После анализа полученных материалов Зыбин определил книгу-ключ (это была повесть А.И. Куприна «Поединок») и успешно дешифровал криптограмму. Содержание криптограммы оказалось весьма важным, за этот успех Зыбин был награжден и получил повышение по службе. Еще в одном случае достигнуть успеха в дешифровании одного из писем революционеров Зыбину помогло знание цены фунта динамита. Сотрудники Департамента полиции подозревали, что в письме может содержаться эта информация и сообщили ее Зыбину, а он проведя атаку по методу «открытый – шифрованный текст» прочитал письмо.

А вот что вспоминают о Зыбине его современники. Один из руководителей московского охранного отделения П.П. Заварзин писал: «По отношению к своей работе он был фанатиком, если не маньяком. Чтобы вскрыть простой шифр, ему достаточно было увидеть его только один раз. Если же ему приходилось иметь дело со сложным шифром, то он почти впадал в состояние транса, из которого выходил лишь тогда, когда шифр был вскрыт» [Жухрай, 1919]. Приведем также свидетельство бывшего сотрудника Департамента полиции Михаила Бакая: «Если встречались письма с шифром, то они расшифровывались специалистом этого дела чиновником Департамента полиции И.А. Зыбиным, который в дешифровке дошел до виртуозности, и только в редких случаях ему не удавалось этого сделать. Зыбин считается единственным своего

рода специалистом в этой области, и он даже читает лекции о шифровке и дешифровке на курсах для офицеров, поступающих в отдельный корпус жандармов… Для Зыбина важно уловить систему ключа, тогда для него не составляет труда подобрать соответствующее значение для букв или цифр… Пользуясь случаем, я обратился к Зыбину с просьбой ознакомить меня со способом разбора шифров и на это получил указание, что письмо с шифрами заранее известных ключей дешифруется очень легко, при этом он мне указал на некоторые ключи революционных организаций, полученные при посредстве провокаторов» [Синельников].

Следует отметить, что Зыбин занимался не только криптоанализом, он разбирался в вопросах проявления тайнописи (невидимых химических чернил), работал в тесном контакте с органами перлюстрации и цензуры (интересно отметить, что материалы Зыбин забирал лично, так как их пересылка не допускалась). В первую очередь дешифровались «химические письма», в которых довольно часто оказывались адреса и явки, потом дело доходило до дешифрования документов захваченных при обысках и арестах. Важное значение придавал Зыбин выявлению корреспондентов революционных сетей связи по почерку. Вот один пример: в сентябре 1910 г. «старший помощник делопроизводителя, коллежский советник Зыбин и чиновник для письма ДП коллежский регистратор Жабчинский рассматривали фотоснимки воззвания под заголовком «РСДРП», начинавшееся словами: «Товарищи! Тяжелое и безотрадное время...» и подписанное: «Орловская группа РСДРП», а также протокол допроса ротмистром Шульцем крестьянина Ивана Федоровича Курбатова». Был проведен подробный анализ почерка воззвания и почерка Курбатова и дано очень осторожное заключение «о схожести букв». Подобная работа проводилась весьма активно. Так в результате исследования «по почерку» была выявлена переписка крупных революционеров В.И. Ленина, В. Ногина, Ю. Цедербаума и других активных деятелей РСДРП [Соболева, 2002].

Занимался Зыбин и вопросами улучшения условий труда дешифровальщиков департамента полиции. Надо сказать,

они были весьма далеки от идеальных, дешифровальщики размещались в тесных и душных помещениях, в которых постоянно применялись химические вещества для проявления стеганографии, царила бесконечная толчея. Разумеется продуктивно работать в таких условиях было трудно, поэтому неудивительно, что большую часть дешифровальной работы Зыбин и его коллеги проводили дома.

Большой вклад внес И.А. Зыбин в подготовку дешифровальщиков для правоохранительных органов России. В 1901 г. Зыбин докладывал руководству Департамента полиции о необходимости обучения криптоанализу сотрудников правоохранительных органов (прежде всего жандармских офицеров на местах). Такая потребность обуславливалась следующими причинами.

Во-первых, объем перехваченной революционной корреспонденции стремительно возрастал. Если в конце XIX в. (как отмечалось в статье [Гольев, 2005-2]) по всей России перехватывалось около 200 шифрованных писем в год, то, начиная с 1901 г., эта цифра увеличилась на порядок – 2,5 тыс., а в 1910-х гг. она подскочила до 4–5 тыс. ежегодно! Объемы шифрованных документов добываемых при обысках и арестах также лавинообразно росли. При этом всю дешифровальную работу приходилось вести немногочисленным сотрудникам Особого отдела.

Во-вторых, системы шифрования, применяемые революционерами постоянно усложнялись, простые словарные и стихотворные шифры применялись все реже, как писал Зыбин в докладной записке от 22 мая 1903 г. директору Департамента полиции А.А. Лопухину «…более опытные революционные деятели (группа «Искра» и др.) пользуются для переписки в настоящее время или двойными ключами, или страницами малоизвестных книг и брошюр, избирая для каждого отдельного корреспондента отдельную книгу и избегая повторения страниц, что крайне осложняет работу» [Синельников]. Если раньше нередко дешифровались одиночные криптограммы, то теперь для успешного дешифрования обычно требовалось наличие комплекта из нескольких криптограмм зашифрованных на одном ключе.

Между тем штат дешифровальной службы Особого отдела был весьма небольшим. Так в 1903 г. работой по дешифрованию революционной корреспонденции помимо Зыбина занимались всего несколько человек. Среди них был ученик Зыбина, выпускник Санкт-Петербургского университета В.Н. Жабчинский. Зыбин говорил о нем, что Жабчинский может разбирать шифры на любом языке. Специалист по фамилии Владимиров занимался дешифрованием и переводом «химических» писем, прокламаций и прочих материалов, написанных на еврейском языке. Так же вместе с Зыбиным работали В.Н. Зверев и ротмистр Мец. На местах дешифровальной работой продолжали заниматься «на общественных началах». Разумеется, справиться с все возрастающим потоком шифрованных материалов, такими малыми силами было крайне трудно.

Именно поэтому Зыбин готов был сам обучать криптоанализу сотрудников правоохранительных органов, начать он предложил с офицеров штаба отдельного корпуса жандармов. Зыбин хотел обучить их с методами дешифрования наиболее употребляемых революционерами шифров. По мнению Зыбина эти знания пригодились бы и для офицеров наиболее важных жандармских управлений и охранных отделений. «И в скором времени можно было бы достигнуть того, чтобы в каждом из наиболее важных жандармских управлений, а также в охранных отделениях имелись офицеры, «знакомые» с приемами дешифрования», – писал Зыбин [Соболева, 2002]. Руководство одобрило инициативу Зыбина, и через некоторое время началось обучение. Одновременно с этим И.А. Зыбин стал преподавать основы криптоанализа для офицеров военного ведомства.

Иван Александрович Зыбин занимался дешифрованием не только революционной переписки. В функции департамента полиции входила и контрразведка, в том числе и наблюдение за дипломатами и другими иностранцами, находившимися на территории России. Известно, что Зыбин работал с шифрперепиской австрийской агентуры в России. В период Первой мировой войны Зыбин и его коллеги из департамента полиции работали над дешифрованием военных

и агентурных сообщений противников России (Германии, Австрии и Турции). К сожалению дешифровальщикам из МВД материалы поступали с задержкой, часто это были короткие сообщения, отдельные криптограммы, не передавалась информация о возможном содержании сообщений, обстоятельствах перехвата криптограммы. Вся перечисленная информация могла бы существенно помочь криптоаналитикам. Но все же сотрудники и агентура департамента полиции и военные старались делать все возможное для помощи своим дешифровальщикам. Так известно, что в ходе войны были добыты ряд немецких и турецких военных и агентурных шифров и кодов. Разумеется велась и аналитическая работа по вскрытию вражеских шифров. Именно таким образом весной 1915 г. команда Зыбина вскрыла ряд криптограмм австрийских и немецких агентов, посланных в Берлин, Вену и Брашов. В этом же году был прочитан ряд австрийских военных сообщений. Группа криптоаналитиков департамента полиции во главе с Зыбиным за дешифрование вражеской шифрпереписки была награждена денежной премией.

Еще одним аспектом деятельности Зыбина-криптоаналитика была оценка стойкости российских шифров. Приведем оценку одного из них сделанную Зыбиным 20 июля 1910 г.: «Предлагаемая система шифрования с помощью двух вращающихся концентрических кругов является мало удобной, во-первых, потому, что по ней подлежащий зашифрованию текст предварительно пишется длинными 40-буквенными группами в две строки каждая; последнее возможно лишь в тех случаях, когда весь текст депеши шифруется сплошь, без всяких пропусков; во-вторых, обязательное отделение каждого слова от следующего за ним знаком препинания, причем последний всякий раз обозначается парою цифр, излишне удорожает шифр и др.; в-третьих, сама система концентрических кругов излишне громоздка и не достигает цели в смысле сохранения секрета депеши, так как при любом наложении кругов и при всяких комбинациях для обозначения каждой буквы и каждого знака препинания имеется лишь два числа – четное

и нечетное. Например, буква А всегда будет обозначаться числом 37 или 28; буква Б – 39 или 20 и др., вследствие чего круги эти являются совершенно излишними; значения букв гораздо удобнее можно расположить в виде таблицы, как в Департаментском полицейском ключе, в котором, между прочим, для каждой буквы имеется от двух до четырех значений» [Соболева, 2002].

В 1916 г. И.А. Зыбин был уволен по подозрению в разглашении известных ему секретных сведений. В книге [Соболева, 2002] приводится текст одной из докладных руководству департамента полиции от оставшегося неизвестным сотрудника: «Ваше Превосходительство! Вы удивляетесь, что секреты ДП являются достоянием публики, а дело очень просто: находящиеся на службе в ДП писцы и чиновники постыдным образом продают эти тайны. Удачно удален Зыбин…».

И.А. Зыбин, обладая исключительными способностями и талантом, на протяжении своей карьеры занимал весьма скромные должности. В начале своей службы он был старшим помощником делопроизводителя, а к концу ее дослужился до делопроизводителя.

После Октябрьской революции И.А. Зыбин стал сотрудничать с Советской властью, он поступил на работу в знаменитый спецотдел ВЧК – криптографическую службу советской России. Иван Александрович внес большой вклад в обучение молодых советских криптоаналитиков и возрождении криптографической службы на своей Родине. Интересно отметить, что во время своих занятий Зыбин охотно рассказывал, как он дешифровал криптограммы революционеров, в том числе и письма В.И. Ленина.

Интересная историческая параллель – в это же время, а точнее в 1897 г. в петербургский «Союз борьбы за освобождение рабочего класса» вступает Глеб Иванович Бокий. Он родился в 1879 г. в старинной дворянской семье. Г.И. Бокий вскоре стал видным революционером, с 1900 г. он член РСДРП, на протяжении 20 лет с 1897 по 1917 гг. он являлся одним из руководителей петербургского большевистского

подполья. В конце 1916 – начале 1917 г. Глеб Иванович был членом русского бюро ЦК РСДРП в октябре 1917 г. он член Петербургского военно-революционного комитета, один из руководителей вооруженного восстания. На протяжении своей революционной карьеры Бокий активно использовал шифры, мало того он разрабатывал и собственные шифрсистемы. Так, при аресте Г.И. Бокия сотрудники правоохранительных органов нередко обнаруживали на первый взгляд самые обычные ученические тетради, исписанные математическими формулами. В действительности это были конспиративные записи, зашифрованными изобретенным Бокием математическим шифром. Ключ к нему был известен только автору. Дешифровальщики департамента полиции подозревали, что за этими «формулами» скрывается шифр, но дешифровать его так и не смогли. «Сознайтесь, – предлагал Бокию следователь, – это шифр?» А Глеб Иванович невозмутимо отвечал: «Если шифр, то расшифруйте». С досадой следователь возвращал ему эти загадочные тетради» [Соболева, 2002]. В 1921 г. Г.И. Бокий возглавил спецотдел ВЧК, он руководил советской криптографической службой до 1937 г. Именно Глеб Иванович пригласил на работу в Спецотдел целый ряд специалистов, работавших при царском режиме, среди них был и Иван Александрович Зыбин.

Особый отдел Департамента полиции в 1898–1917 гг. был главным подразделением МВД Российской Империи по борьбе с революционным движением. Однако на местах основная тяжесть борьбы с революционерами легла на губернские жандармские управления (ГЖУ) и охранные отделения («охранка»). Обе эти структуры уже не раз упоминались в нашем повествовании, однако теперь рассмотрим их поподробнее.

Слово «жандармерия» или «жандарм» в России впервые употребляется в 1772 г. Тогда в составе гатчинских войск цесаревича Павла Петровича была учреждена конница, называвшаяся жандармским полком (иногда кирасирским полком). В 1815–1817 гг. было сформировано еще несколько жандармских частей в армии и корпусе внутренней стражи, обслуживающим гражданские власти «при поимке воров и разбойни-

ков, в случае неповиновения власти, при взыскании податей и недоимок» [Жухрай] (фактически этот корпус был аналогом современных внутренних войск). Армейские жандармы должны были следить за порядком в воинских частях и выполняли функции военной полиции.

Вооруженной силой Российской политической полиции – Третьего отделения, жандармы стали 1827 г. Указом императора Николая I от 28 апреля 1827 г. Из разрозненных жандармских частей создан Отдельный корпус жандармов. В задачи корпуса входила силовая поддержка чинов III отделения при проведении различных мероприятий при арестах, обысках, конвоировании задержанных, а также исполнении обязанностей «наблюдательной полиции» [Жухрай]. Командир корпуса обладал правами командующего армией. Численность Отдельного корпуса жандармов составляла в то время 4278 человек (3 генерала, 41 штаб-офицер, 160 обер-офицеров, 3617 рядовых и 457 нестроевых чинов). Руководитель III отделения А.Х. Бенкендорф разработал первое положение о корпусе жандармов. Вся страна была разделена на несколько (сначала пять, потом восемь) жандармских округов. Каждый из округов возглавлял генерал. В округ входило от 8 до 11 губерний. Округа делились на отделения, включавшие от двух до трех губерний. Возглавляли их, как правило, полковники. В каждую губернию назначался штаб-офицер корпуса жандармов в чине от майора до полковника. В случае необходимости штаб-офицер мог прибегнуть к помощи губернской жандармской команды численностью до 34 человек. Возглавлял ее обычно поручик или штабс-капитан. Практическая деятельность жандармерии состояла в понуждении к исполнению законов и приговоров судов. Чины ее посылались на поимку беглых крепостных крестьян, задержание беспаспортных лиц, на преследование воров, контрабандистов, «расследование законом запрещенных скопищ» [Жухрай], препровождение особо важных преступников и арестантов. Занимались жандармы и борьбой с коррупцией.

В 1867 г. были упразднены жандармские округа, а вместо них были созданы губернские жандармские управления.

С 1880 г. губернские жандармские управления, подчинявшиеся ранее штабу корпуса, перешли в подчинение департамента полиции. В ходе своей работы жандармы внимательно изучали печатную продукцию и литературу (пригодился опыт взаимодействия с цензурными органами), использовали доносы и слухи (исходили из того, что и там могут быть подлинные сведения). Стоящие задачи помогала решать перлюстрация корреспонденции, наружное наблюдение, вырабатывались методы вербовки агентуры, задействовались полицейские приемы в работе – аресты, обыски, допросы.

С 1905 г. численность корпуса жандармов неуклонно увеличивалась. В середине 1913 г. он насчитывал 12700 человек, а концу 1916 г. в корпусе служили около 16 тысяч жандармов. В это время корпус состоял из главного управления (штаба), 75 губернских жандармских управлений, 30 уездных жандармских управлений, 33 жандармско-полицейских управлений железных дорог с 321 отделением в городах и на крупных станциях.

Ведущим структурным подразделением политического розыска являлось губернское жандармское управление, подчинявшееся по сыскной части департаменту полиции. Управления размещались в губернских городах, в крупных уездных центрах они имели отделения или одного ответственного за политический сыск в этой местности офицера. Вопросы службы жандармов регламентировались законом от 19 мая 1871 г. Главным направлением их деятельности по этому акту становится дознание, а также политическое следствие. В ведении жандармских управлений находились жандармские части. В некоторых городах создавались городские жандармские управления.

Подготовка жандармских офицеров в начале XX в. по сравнению с предыдущими десятилетиями значительно улучшилась. Если в первой половине XIX в., зачисленные в корпус проходили лишь двухмесячную стажировку при его штабе, то теперь их готовили на специальных курсах в Санкт-Петербурге, куда прибывали офицеры армии и флота, прошедшие тщательный отбор и выдержавшие предварительные испытания.

Будущие жандармы изучали уголовное право, методы дознания и расследования политических преступлений, про-

граммы и историю российских политических партий, железнодорожный устав. Их также знакомили с техникой фотографирования, дактилоскопией и прививали другие навыки, которые могли пригодиться офицеру розыска. Уделялось внимание практическим курсам по владению оружием, приемам самозащиты. Уже в самом начале XX в. жандармский корпус первым в России начал изучать восточные единоборства, а именно – борьбу джиу-джицу. Этой борьбе уже в 1902–1903 гг. обучали на специальных курсах. Благодаря стараниям И.А. Зыбина в число изучаемых дисциплин входил криптоанализ. После выпускного экзамена окончившие курсы указом царя переводились на службу в корпус и получали назначение в различные жандармские управления и в армейские части. Вот что пишет по этому поводу бывший жандармский генерал А. Спиридович [Спиридович, 1991]: «Для поступления в корпус от офицеров требовались прежде всего следующие условия: потомственное дворянство, окончание военного или юнкерского училища по первому разряду, не быть католиком, не иметь долгов и пробыть в строю не менее шести лет… прослушать четырехмесячные курсы в Петербурге и выдержать выпускной экзамен… Желающих было так много, что без протекции попасть на жандармские курсы было невозможно». Даже выдержав предварительные экзамены при штабе корпуса в Петербурге, офицер не направлялся на жандармские курсы. Он должен был вернуться в свою воинскую часть и ожидать вызова. Иногда до двух лет. А в это время местная жандармерия собирала о кандидате наиподробнейшие сведения. Политическая благонадежность и денежное состояние подвергались наибольшей проверке.

Другой структурой политического сыска в регионах были охранные отделения. Первое было создано в 1866 г. как Отделение по охранению общественной безопасности и спокойствия при петербургском градоначальнике после покушения на Александра II. Штат его состоял всего из 12 человек. Это охранное отделение с 1880 г. подчинялось непосредственно Департаменту полиции министерства внутренних дел.

В этом же году создали московское охранное отделение. В первые годы оно было малочисленным, так в 1889 г. его штат составлял всего 6 человек. Однако на отделение работали сотрудники «охранной наружной службы», т.е. филеры и осведомители. Вскоре московское отделение увеличилось, оно стало районным и уже охватывало своей деятельностью 13 губерний, являясь самым большим в России.

В столичных «охранках», кроме канцелярии, имелись два отдела: наружного наблюдения и агентурный (отдел внутреннего наблюдения). К ним примыкали секретные делопроизводства. В агентурных отделах разрабатывались данные, полученные от осведомителей и путем перлюстрации писем в «черных кабинетах» при почтамтах. В агентурном отделе анализировались все сведения, полученные от агентов. Секретные агенты являлись предметом постоянных забот и попечения всего департамента полиции. Об агентуре постоянно говорится в его циркулярах начальникам охранных отделений и губернским жандармским управлениям. Напомним, что именно агентура довольно часто становилась источником сведений о шифрах революционеров, организации конспиративной связи и др.

Именно в охранных отделениях начал проявляться научный подход в борьбе с революционерами. Революционное движение, его различные общества и их ответвления изучались, на учет брались все люди, оказавшиеся по разным причинам в поле зрения охранки. В результате образовались громадные картотеки на граждан, собирались коллекции бомб и листовок. Данные поступали от многочисленной и хорошо оплачиваемой агентуры в стране и за границей. Исследователь Жилинский [Жухрай] отмечал: «Руководители и вдохновители охранного отделения были офицеры отдельного корпуса жандармов, они заведовали различными отделами охранки. Это не простые жандармские офицеры – это отличившиеся по службе способные и умные инквизиторы, выказавшие особое рвение. Это люди почти всегда с высшим образованием, развитые, это интеллигенты полиции и ...всегда либералы и радикалы, о чем сами же докладывали вся-

кому интеллигентному политическому арестанту, только они считали, что Россия еще не созрела для реформы. Они были «учеными», они проходили особые курсы, более молодые из них выслушивали лекции и изучали историю революционного движения и партий в России по источникам, доступным только им. Этого мало, они сами изучали революционное движение по источникам особым, недоступным даже ученому миру – это были печатные книги, издаваемые Департаментом полиции, ученые труды жандармских генералов и полковников». Одним из важнейших требований в их деятельности была секретность. Как подчеркивал исследователь, «все, что делалось в охранке, все, что приходило туда и исходило оттуда, – все было «секретно» или «совершенно секретно». Работа их была тайной, и тайна была их девизом» [Жухрай].

После образования Особого отдела охранные отделения поступили в его ведение, они по замыслу правительства принимали на себя основную нагрузку по предотвращению и пресечению политических преступлений. На рубеже веков охранка достигла значительных успехов. Под их неусыпным надзором оказались все революционные общества и организации. Так в конце XIX в. встревоженное рабочими выступлениями, которыми начала руководить социал-демократия, правительство в спешном порядке укрепляет Петербургскую «охранку». Репрессии ее нанесли ощутимый урон ленинскому «Союзу борьбы за освобождение рабочего класса». Аресты учеников и соратников В.И. Ленина привели к тому, что в столице перестала существовать единая социал-демократическая организация.

После революции 1905–1906 гг. в стране насчитывалось 60 охранных отделений. В 1914 г., когда окрепли губернские жандармские управления и жандармско-полицейские управления железных дорог, а также в связи с ослаблением революционного движения охранные отделения оставили только в самых крупных городах, являвшихся центрами рабочего и студенческого движения.

Формально функции ГЖУ и охранных отделений были разделены. «Охранка» отвечала за тайный сыск, жандармы за процессуальные действия аресты, обыски, ведение следствия и

др. Однако в реальности эти структуры нередко конкурировали между собой. Вот что писал в то время журнал «Статский советник»: «Человеку, не сведущему в хитросплетениях ветвей древа русской государственности, непросто было бы разобраться, в чем состоит различие между Охранным отделением и Губернским жандармским управлением. Формально первому надлежало заниматься розыском политических преступников, а второму – дознанием, но, поскольку в секретных расследованиях розыск от дознания бывает неотделим, оба ведомства делали одну и ту же работу: истребляли революционную язву всеми предусмотренными и непредусмотренными законом способами. И жандармы, и «охранники» были людьми серьезными, многократно проверенными, допущенными к сокровеннейшим тайнам, однако же Управление подчинялось штабу Отдельного жандармского корпуса, а Отделение – Департаменту полиции. Путаница усугублялась еще и тем, что руководящие чины Охранного нередко числились по Жандармскому корпусу, а в жандармских управлениях служили штатские чиновники, вышедшие из Департамента. Очевидно, в свое время кто-то мудрый, опытный, придерживающийся не слишком лестного мнения о людской природе, рассудил, что одного надзирающего и приглядывающего ока для беспокойной империи маловато. Ведь недаром и человекам Господь выделил не по одной зенице, а по две. Двумя глазами и крамолу выглядывать сподручней, и риска меньше, что одинокое око слишком много о себе возомнит».

Постоянная борьба друг с другом отвлекала жандармов и сотрудников «охранки» от государственных дел. С момента организации охранных отделений между их начальниками и руководством местных жандармских управлений шла непрерывная «подковерная» борьба за руководство политическим розыском. Пока революция была на подъеме, обе структуры волей-неволей должны были тесно сотрудничать. Однако после некоторого «успокоения» страны конфликт между руководством двух правохранительных органов вспыхнул с новой силой. К тому же начальники охранных отделений все чаще

шли на провокационные действия, тревожившие руководителей министерства внутренних дел.

К тому моменту корпус жандармов был слишком независим от начальства. Не только губернаторы и сенат, но и даже прокуратура не имела контролирующей власти над видоизмененным жандармским корпусом, связанным через департамент полиции с министерством внутренних дел. Бывший директор департамента полиции А. Лопухин, отмечал следующее: «…будучи поставлено в такие условия это учреждение ничего, кроме произвола и вреда для населения и интересов государства, принести не могло… Все политическое мировоззрение корпуса жандармов заключается в представлениях о том, что существуют народ и государственная власть, и последняя находится в постоянной опасности со стороны первого… и что для осуществления охраны от таковой опасности все средства хороши» [Жухрай].

Тем не менее, можно отметить, что на рубеже XIX–XX вв. Россия имела эффективную систему органов защиты государственной безопасности. В результате использования перлюстрации, криптоанализа, а также многочисленной тайной агентуры в стране и за границей, добровольных помощников правоохранительные органы могли быть в курсе всего происходящего. Они внедряли своих агентов в потенциально опасные круги, действовали на опережение, изучали возможных противников. Спецслужбы имели опыт крупных политических процессов, взаимодействия с прессой (что помогало в дискредитации возможных противников). О дальнейших событиях, связанных с криптографической деятельностью во внутриполитической жизни России мы расскажем в следующих статьях.

Список рекомендуемой литературы

1. Ансимов Н.Н. Охранные отделения и местная власть царской России в начале XX в. // Советское государство и право. – 1991. – №5.

2. Антонов В., Русский друг Маркса Г.А. Лопатин. – М., 1962.
3. Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Шифры революционного подполья России XIX века // Защита информации. Конфидент. – 2004. – №4.– с. 82–87.
4. Берштейн А. Революционеры-оборотни // www.hronos.km.ru
5. Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Научно-технический прогресс и криптографическая деятельность в России XIX века. // Защита информации. INSIDE. – 2005. – №2. – с. 67–75.
6. Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптографическая деятельность организаций «Земля и Воля» и «Народная воля» в России в 1876 – 1881 годах: успехи и неудачи // Защита информации. INSIDE. – 2005. – №6.– с. 90–96.
7. Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптографическая деятельность организаций «Земля и Воля» и «Народная воля» в России в 1876–1881 гг. // Защита информации. INSIDE. – 2005. – №6. – с. 90–96.
8. Гольев Ю.И., Ларин Д.А., Шанкин Г.П. Криптографическая деятельность революционеров в России. 1881–1887 годы: агония «Народной Воли» // Защита информации. INSIDE. – 2006. – №2. – с. 88–96.
9. Ерошкин Н.П., История государственных учреждений дореволюционной России, 2-е изд. – М., 1968.
10. Жандармы его величества // www.agentura.ru
11. Жухрай В.М. Тайны царской охранки. – М., 1991.
12. Заварзин П.П. Жандармы и революционеры. Воспоминания. – Париж, 1930.
13. Записки императрицы Екатерины II. – М., 1990.
14. Записки сенатора Лопухина. – М., 1990.
15. Защита информации. Конфидент за 1994–2000 гг. – СПб., 2004.
16. История сыска в России. – Минск, 1996, с. 8.
17. Йосифова.Б. Декабристы. – М., 1983.
18. Кан Д. Взломщики кодов. – М.: Центрполиграф, 2000.
19. Лурье Ф. Гапон и Зубатов // www.hrono.info.

20. Максимова Л. Опасное противостояние: российский политический сыск и революционеры // Бельские просторы. – 2004. – №3.
21. Меньшиков Л.П. Охрана и революция. Ч.1-3. – М., 1925–1932.
22. Михайлов А. Великий провокатор // «Версия» 1.04.2003.
23. Николаевский Б. История одного предателя. – М., 1991.
24. Овченко Ю.Ф. Провокация на службе охранки // Новый исторический вестник. – 2003. – №1.
25. Осоргин М.А. Охранное отделение и его секреты. – М., 1917.
26. Перегудова З.И. Политический сыск России (1880–1917 гг.). – М., 2000.
27. Политический сыск в России: история и современность. – СПб., 1997.
28. Синельников А.В. Шифры и революционеры России // www.cryptography.ru.
29. Соболева Т.А. Тайнопись в истории России. – М., 1994.
30. Соболева Т.А. История шифровального дела в России. – М.: ОЛМА-ПРЕСС-Образование, 2002.
31. Спиридонович А. Записки жандарма. – М., 1991.
32. Тайные операции российских спецслужб. – М., 2000.
33. Тайные страницы истории. – М., 2000.
34. Тынянов Ю. Кюхля. – М.,1981.
35. Тынянов Ю. Пушкин – М., 1988.
36. Уральский Ю.С. Конспирация в деятельности ленинской «Искры» (1900–1903 гг.). Диссертация на соискание ученой степени кандидата исторических наук. На правах рукописи. – М., 1980.
37. Уральский Ю.С. Пароль: «От Петрова». – М., 1988.
38. Хлобустов О. Музей «Гороховая, 2» // Независимое военное обозрение. – 2007. – №3. – с.7.
39. Черняк Е.Б. Пять столетий тайной войны. – М., 1991.
40. Чехов А.П. Собрание сочинений, т. 11. – М., 1956. – с 228.
41. http://www.agentura.ru
42. www.hronos.km.ru
43. http://en.wikipedia.org

Приложение к гл. 5

Роль Ленина в конспиративной переписке «Искры»

В последнее время стало модным осуждать коммунистическую партию и руководство Советского Союза, но нельзя забывать и о том позитивном, что было создано коммунистами для нашей страны, да и просто не представляется возможным вычеркнуть из нашей истории почти целый век правления коммунистической партии. Далее речь идет о периоде подпольной работы РСДРП, а точнее об организации конспиративной переписки «Искры» и виднейших революционеров. Данный подраздел знакомит читателя с некоторыми принципами построения конспиративной переписки[1].

Вопросы установления, развития, совершенствования связей и их конспирации всегда находились в центре внимания В.И. Ленина. «Не забывайте, что сила революционной организации в числе ее связей» [1] – это ленинское положение наилучшим образом нашло свое подтверждение в деятельности редакции газеты «Искра», ее Русской организации и явилось краеугольным камнем в практической работе искровцев. В.И. Ленин подчеркивал, что «без регулярных сношений невозможно никакое общее дело» [2].

Одна из важнейших функций связи заключалась в пересылке конспиративной корреспонденции. В.И. Ленин и редакция «Искры» вели обширную переписку с Россией и с заграницей.

В разработанном плане создания русской организации «Искры» В.И. Ленин указывал на важную роль конспиративной переписки для сплочения революционных организаций различных городов, внутри города, с заграницей. Он писал, что «без писем нет ничего кроме полной разрозненности» [3].

---

[1] В этом разделе используются материалы курсовой работы студента Кулай Александра Юрьевича (при научном руководстве Бабаша А.В.).

Подчеркивая преимущества конспиративной переписки перед другими видами связи, редакция «Искры» советовала своим агентам не предпринимать без надобности поездок, ибо «лишние разъезды тяжело отражаются на кассе и могут быть легко заменены перепиской» [4].

ИСКРА

РОССІЙСКАЯ СОЦІАЛЬ-ДЕМОКРАТИЧЕСКАЯ РАБОЧАЯ ПАРТІЯ

№ 1.

Первый номер газеты «Искра»

Сохранившийся редакционный архив «Искры» включает более 1300 писем, относящихся к переписке с агентами газеты, социал-демократическими организациями, группами содействия [5]. Это, конечно, далеко не все. Многие письма во время пересылки затерялись, другие были перехвачены «Черным кабинетом». Часть писем социал-демократы уничтожали после прочтения, чтобы при обыске или аресте полиция не получила улик противозаконной деятельности обвиняемых.

Редакционный архив «Искры», который создавала Н.К. Крупская, составляют заграничные и российские письма В.И. Ленина и редакции газеты. Заграничная корреспонденция архива включала переписку В.И. Ленина с соредакторами (Г.В. Плехановым и П.Б. Аксельродом) о различных сторонах организационной и редакционной деятельности по налаживанию издания печатного органа – газеты «Искра» и журнала «Заря».

В.И. Ленин вел переписку с социал-демократами (Ю.М. Стекловым, В.П. Ногиным и многими другими), а также с организаторами групп содействия «Искре» (М.Г. Вечесловым, Г.Д. Лейтейзеном) об организационно-издательской деятельности, транспортировании «Искры» в Россию.

Н.К. Крупская поддерживала оживленную переписку с берлинской группой содействия «Искре», занимавшей видное место в организационно-конспиративной деятельности газеты. В переписке освещались организационные стороны работы, которую проводили редакция газеты и искровцы, в том числе по вопросам конспирации, о подготовке чемоданов с литературой для отправки в Россию, о паспортах для лиц, уезжающих в Россию.

Основная же часть редакционного архива «Искры» включала российскую переписку В.И. Ленина, Н.К. Крупской и членов редакции с агентами газеты, социал-демократами, группами и организациями.

Среди большого количества писем выделялась переписка по теоретическим вопросам, связанным с опубликованием статей на страницах газеты. Давались рекомендации и указа-

ния по перестройке практической работы местных комитетов и организаций, преодолению остатков кружковщины и кустарничества в их деятельности, а также в работе отдельных агентов. С агентами газеты велась значительная переписка по вопросам доставки и распространения газеты и другой политической литературы в России. Направлялись многочисленные советы, рекомендации и указания по их конспиративно-организационной работе. В письмах освещались вопросы организации связей, применения шифров, химических средств, условностей, паролей и других составных элементов конспирации, формирования «русской социалистической почты».

Российские социал-демократы и организации в своих письмах В.И. Ленину, редакции газеты освещали различные вопросы организационно-партийной и конспиративной работы. Редакция газеты дорожила перепиской с корреспондентами и очень аккуратно со всей полнотой отвечала на их письма.

Среди почтовых отправлений выделялись информационные письма, в которых приводились факты, события, происшедшие в том или ином городе, описывались действия рабочих, студентов и других слоев населения в ответ на притеснения и репрессии царского самодержавия. Как отмечала Н.К. Крупская, «отзывчивость и жизненность органа в значительной мере зависит от того, насколько деятельно русские товарищи будут заботиться о том, чтобы этот орган был надлежащим образом информирован» [6].

Следовательно, постоянная взаимная связь редакции «Искры» со своими корреспондентами и читателями являлась непременным условием ее успешной деятельности.

Редакция «Искры» требовала от своих агентов полной и правдивой информации о положении на местах и предпринимала активные меры к получению такой информации различными способами, в том числе посылкой в Россию своих людей, по существу выполнявших задачи специальных корреспондентов. Так, в связи с нерегулярностью получения писем от представителей газеты в Киеве В.Н. Крохмаля и С.Н. Афанасьевой редакция газеты «Искра» в конце ноября 1901 г. направила в

Россию через берлинскую группу содействия А.А. Кузнецову с задачей «писания корреспонденций, сообщения сведений и т.д.» [7]. В подробных письмах из Киева А.А. Кузнецова информировала газету об отсутствии там нелегальной литературы, без которой нельзя создавать в России революционную партию и развивать рабочее движение, о слабой работе местного комитета, об отрыве членов комитета от рабочих масс. Такая правдивая информация позволила редакции «Искры» разобраться с фактическим состоянием дел, которое сложилось в тот период в Киевском комитете РСДРП. Прочитав корреспонденцию А.А. Кузнецовой, В.И. Ленин просил берлинскую группу непосредственно связать А. А. Кузнецову с редакцией «Искры» в целях дальнейшего получения информации [8].

Анализ развития конспиративной переписки по годам из сохранившегося редакционного архива «Искры» показывает ее непрерывный рост (табл. 5.1).

Таблица 5.1

Развитие искровской конспиративной переписки с Россией [9]

Год	Количество писем		Количество корреспондентов		
	отправленных в Россию	полученных из России	Комитеты и социал-демократические организации	Отдельные лица, агенты	Примечание
1901	182	82	6	42	* В таблицу включена корреспонденция до начала работы II съезда РСДРП – 17(30) июля 1903 г.
1902	240	368	15	64	
1903	170	220	20	24*	

Как видно из таблицы, если в 1901 г. преобладала переписка редакции с Россией, то начиная с 1902 г., в связи с расширением связей, их упрочением, увеличилось количество писем, направляемых в адрес редакции. Одновременно наблюдался рост количества социал-демократов, а также социал-демократических организаций и групп, вступивших в переписку с «Искрой». Этот анализ характеризует признание ими «Искры» своим руководящим органом, повышение ее роли и авторитета в социал-демократическом движении.

В.И. Ленин считал, что для укрепления связей с Россией необходимо было сформировать организацию, которая бы занималась доставкой полных и своевременных сведений о движении и обеспечивала снабжение периодической прессой Россию. Такую организацию В.И. Ленин назвал «русской социалистической почтой». Она должна была способствовать расширению влияния общепартийного органа среди пролетарских и демократических сил России, а также централизации искровских связей, усилению их конспирации.

Для обеспечения регулярных связей «Искры» вначале необходимо было создать в России опорные пункты будущей газеты, разработать такую организацию связи, которая бы противостояла попыткам «Черного кабинета» перехватывать и дешифровывать нелегальную переписку.

Становление первых искровских связей было подготовлено огромной организационной работой В.И. Ленина в России перед его отъездом за границу.

По окончании срока ссылки В.И. Ленин приступил к непосредственному осуществлению плана создания общерусской газеты. В первой половине 1901 г. он встречался с социал-демократами во многих городах России и знакомил их с планом издания «Искры». Во время этих встреч закладывались первые связи будущей газеты.

Одновременно члены Литературной группы, созданной В.И. Лениным в середине 1899 г. [10] (Ю.О. Цедербаум и А.Н. Потресов) побывали в Полтаве, Казани, Вильно, в Крыму, повсюду устанавливали связи с местными социал-демократами, проводили ту же работу, что и Владимир Ильич.

При встречах с социал-демократами В.И. Ленин уделял большое внимание организации связи и ее конспирации. «В Уфе, – писала А.И. Ульянова-Елизарова, – Владимир Ильич виделся с местными товарищами. Помню из них Крохмаля, с которым он условился о шифре; знаю, что из некоторых уездов приезжали ссыльные повидаться с ним» [11].

С В.И. Лениным виделись революционеры из Нижнего Новгорода, Ярославля, Астрахани. Со всеми он договаривался об организации связи.

Встречаясь с И.В. Бабушкиным в Смоленске, В.И. Ленин практически показывал способы ведения конспиративной переписки. По воспоминаниям жены И.В. Бабушкина (П.Н. Рыбась), Ленин и Бабушкин «составляли химические письма, писали так, чтобы жандармы не прочли, когда распечатают письмо на почте» [12].

Таким образом, в результате напряженной работы, проведенной В.И. Лениным и другими членами Литературной группы, в России были созданы опорные пункты будущей общерусской нелегальной марксистской газеты, подобраны ее первые корреспонденты, разработаны способы связи с ними и приняты меры безопасности конспиративной переписки.

Пересылка писем, книг, посылок осуществлялась главным образом посредством почты. Россия состояла членом Всемирного почтового союза, созданного в 1874 г., и имела почтовые связи с Германией, Австрией, Болгарией, Румынией, Сербией, Бельгией, Грецией, Швейцарией, Великобританией и другими странами [13].

Большие расстояния, отделявшие редакцию «Искры» от ее адресатов, а также несовершенство организации доставки почтовой корреспонденции неблагополучно отражались на устойчивости и общем состоянии искровских связей. Письма месяцами шли в отдаленные местности России. Они часто терялись в пути.

Для пересылки конспиративных писем и других видов почтовой корреспонденции, кроме почты, применялись так называемые оказии – лица, сочувствовавшие социал-демократическому движению. Иногда письма из-за границы и обратно доставляли русские студенты, обучавшиеся в западноевропейских странах. Этот способ пересылки писем был крайне нерегулярен, но он до некоторой степени лишал охранку возможности беспрепятственно перехватывать корреспонденцию.

В целях противодействия перехвату и перлюстрации полицией конспиративной переписки искровцев связь между адресами состояла из отдельных звеньев (цепочек) с использованием многочисленных посреднических адресов. Так, в 1900–1903 гг.

в Германии и Бельгии редакция «Искры» использовала около 60 адресов, из них в 1903 г. – 20 (№10, 11, 13, 14, 15, 16, 17, 18, 20, 22, 28, 29, 30, 31, 32) и, предположительно, №19, 25, 27, 34, 37. Этот вывод подтверждается анализом искровской переписки и учетом писем, помещенных Н.К. Крупской в «Тетради №I входящих материалов редакции «Искры» (январь-август 1903 г.), а также расшифровкой адресов, на которые посылались письма для газеты. По данным советских исследователей к концу 1903 г. в Германии и Бельгии редакция имела 30 посреднических адресов. Со ссылкой на немецкого исследователя Wuttke Irmtraund считает, что искровцы для конспиративных связей в тот период имели 84 адреса [14].

Все письма, предназначенные В.И. Ленину и редакции газеты «Искра», пересылались по почте с указанием на конверте известного адреса. На месте письма изымались у владельцев посреднических адресов доверенными лицами. Так, в Штутгарте таким лицом была Клара Цеткин, выдающийся деятель германской социал-демократической партии, а в Нюрнберге – Филипп Регнер, в Лейпциге – Карл Пинкау, в Лондоне – доктор А.Р. Хазель.

В Россию письма направлялись на «чистые» легальные адреса для последующего вручения адресату.

По способам применения и назначения искровские посреднические адреса можно подразделить на четыре группы: личные и прямые адреса В.И. Ленина и членов редакции «Искры», адреса общего назначения, специализированные и открытые адреса «Искры».

Личные и прямые адреса В.И. Ленина и членов редакции «Искры». 16 июля 1900 г. В.И. Ленин выехал за границу для переговоров с группой «Освобождения труда» о совместном редактировании газеты «Искра» и научного журнала «Заря». В июле-августе он переписывался только с родными по парижскому адресу русского эмигранта М. Жуковского. В деле Московского жандармского управления в выписках из писем В.И. Ленина к родным сохранился этот адрес:

«Письмо того же автора (В.И. Ленина [0]) «с датой 18/VIII-1900. Париж», адресованное М.А. Ульяновой, в коем

встречается адрес: M. Dr. Dubon chez... Pour. M. Goukowsky, 8 Boulevard Capucines, Paris [15]. По этому поводу М.И. Ульянова писала: «В первое время пребывания Владимира Ильича за границей в 1900 г., когда он не знал еще, насколько прочно обоснуется там, он, в целях конспирации, не давал нам для переписки своего личного адреса, и, когда он жил в Швейцарии ...мы писали ему на Париж» [16].

Находясь в Швейцарии и желая придать большую правдоподобность своему «пребыванию в Париже», В.И. Ленин в письмах к М.А. Ульяновой подчеркивал: «Удивляюсь я, дорогая мамочка, что не получаю от тебя ни одного письма: я писал тебе уже дважды из Парижа...» [17].

Первые два дня после приезда в Швейцарию В.И. Ленин прожил у П. Б. Аксельрода. По-видимому, адрес П. Б. Аксельрода: Hrn Paul Axelrod, Vogelsangstrs. 9/11. Zurich [18] стал вторым посредническим адресом для переписки его с родными. На этот адрес В.И. Ленину направлялись письма из Парижа.

Через две недели после отъезда В.И. Ленина за границу выехала и А. И. Ульянова-Елизарова. Ее парижский адрес (Rue de la Glaciere, 103. M-lle Loukachevitsch, Paris. Для Бланк) [19] также применялся для связи с В.И. Лениным. В целях конспирации адресата в Париже применялась фамилия матери В.И. Ленина – Бланк. На этот адрес пересылались письма и книги. (А.М. Лукашевич – участница социал-демократического движения в Москве в 1900 г. находилась в эмиграции во Франции) [20]. Получая письма и книги на адрес Лукашевич, А.И. Ульянова-Елизарова направляла их В.И. Ленину в Швейцарию на адрес П.Б. Аксельрода.

После отъезда из Швейцарии по пути в Мюнхен В.И. Ленин встретился в Нюрнберге с одним из руководителей германской социал-демократической партии Адольфом Брауном, через которого был получен первый личный адрес В.И. Ленина в Германии: Herrn Philipp Rogner, Cigarrenhandlung, Neu Gasse, Nurnberg [21]. Об этом адресе 5 сентября 1900 г. В.И. Ленин впервые сообщал в письме неустановленному адресату за границей, а в другом письме вновь его подтвердил: «...спешим по-

слать Вам адрес, по которому могли бы быть посылаемы всякие материалы из России (данным Вам адресом – Rogner, можно пользоваться только из-за границы, и этого адреса Вы, пожалуйста, другим не давайте») [22].

Филипп Регнер, член социал-демократической партии Германии, был владельцем табачной лавки. Его коммерческие связи стали хорошим прикрытием для пересылки нелегальной корреспонденции.

В.И. Ленин просил, чтобы письма по этому адресу посылались «в 2-х конвертах, на втором: для Петрова» и вместе с тем указывал: «Не пишите, пожалуйста, никаких инициалов в письмах – господь их знает, вполне ли здесь надежна почта» [23].

Из Нюрнберга В.И. Ленин на пути в Мюнхен выехал в Прагу, где по рекомендации чешских социал-демократов договорился с рабочим типографии социал-демократом Ф. Модрачиком о пересылке им нелегальной корреспонденции из России в Мюнхен и обратно. Его адрес (Herrn Franz Modracek Smesky, 27 Prag. Австрия) был одним из важнейших для связи В.И. Ленина с Н.К. Крупской, жившей в то время в Уфе, а также с родными. Впервые использование этого адреса В.И. Лениным отмечено в октябре 1900 года [24].

С приездом в Мюнхен В.И. Ленин познакомился с известным польским революционером Ю. Мархлевским, который продолжительное время жил в Германии. Через него был получен второй посреднический адрес доктора К. Лемана. Об этом адресе В.И. Ленин писал: «Вот лучший адрес: Herrn Dr. Med. Carl Lehmann, Gabelsbergerstrabe 20a. Munchen. Внутри на втором конверте: для Петрова» [25].

Этот адрес считался одним из важнейших, прямым и был пригоден для денег, писем и для книг. Специальность врача позволяла Леману иметь большой круг пациентов, вести обширную переписку и обеспечивала прикрытие конспиративных связей. Этим адресом наиболее часто В.И. Ленин пользовался для переписки с членами редакции газеты «Искра», находившимися в Швейцарии – Г.В. Плехановым и П.Б. Аксельродом.

В Мюнхене В.И. Ленин поселился в трактире «Цум гольденен Онкль» [26] владельцем которого был социал-демократ Риттмейер. Его адрес В.И. Ленин также использовал для переписки: Herrn Georg Rittmeyer Kaiserstrabe 53. O.Munchen [27].

При отправке писем в адрес доктора Лемана В.И. Ленин просил на втором конверте писать «fur Meyer» (для Мейера). Если же письмо было написано по-русски, то его можно было отправить в адрес Риттмейера без всякого указания о передаче, видимо, потому, что из русских в трактире жил только он один.

В мае 1901 г. В.И. Ленин и Н.К. Крупская переехали на новую квартиру в предместье Мюнхена – Швабинг. В это время основным адресом стал адрес доктора Лемана.

В марте 1901 г., когда Модрачек сменил место жительства, В.И. Ленин сообщил М.А. Ульяновой измененный адрес: Herra Franz Modracek. Vrsovice bei Prag, №384. Oesterreich.

В предисловии к сборнику «Письма к родным» (издания 1930 г.) М.И. Ульянова отмечала, что «в письме от 2 марта 1901 г. В.И. Ленин сообщил свой новый адрес, прибавляя, что «переехал вместе со своим хозяином квартирным». Франц Модрачек, на адрес которого шли наши письма, действительно, переехал тогда на новую квартиру, но Владимир Ильич продолжал жить в Мюнхене, на старой» [28].

Следовательно, за границей В.И. Ленин продолжил организационную работу, начатую еще в России, по становлению первых искровских связей. В Германии были подобраны личные посреднические адреса, которые обеспечили связь Ленина с соредакторами «Искры» в Швейцарии, социал-демократами за границей и в России.

Адреса Лемана, Риттмейера, Регнера вначале применялись для заграничных связей, а затем по мере расширения искровской переписки стали использоваться агентами «Искры» и наиболее надежными корреспондентами в России. В мюнхенский период деятельности редакции «Искры» (1901-1902 гг.) эти адреса использовались для заграничной переписки В.И. Ленина с Г.В. Плехановым, П.Б. Аксельродом, а такке с агентами газеты в России – В.П. Ногиным, Н.Э. Бауманом, М.А. Сильвиным,

В.Н. Крохмалем, Г.М. Кржижановским, Ф.В. Ленгником, Е.Д. Стасовой, А.С. Енукидзе, К.И. Захаровой, П.Н. Лепешинским, И.И. Радченко и другими.

12 апреля 1902 года В.И. Ленин и редакция «Искры» переехали в Лондон. Там первым личным посредническим адресом В.И. Ленина для переписки с родными, Г.В. Плехановым и П.Б. Аксельродом стал адрес жившего тогда в эмиграции врача социал-демократа Н.А. Алексеева. Об этом адресе В.И. Ленин заранее, чтобы не прерывать связь, 10 апреля сообщил А.И. Ульяновой-Елизаровой в Берлин: «Пиши пока, если что спешно, на адрес: Mr. Alexejeff; 14, Frederick Str, 14. Gray's Ynn Road; London W. C. (для Ленина – внутри)» [29].

В письме от 17 апреля 1902 года этот же адрес был передан для связи Г. В. Плеханову, а затем и П.Б.Аксельроду [30].

После смены местожительства Алексеева его новый адрес: Mr. Alexeyeff 22, Ampton Street, Gray's Ynn Road, W.C. стал также использоваться в прежних целях. В частности, Н.К. Крупская в письме от 30(17) октября 1902 г. в Одессу просила Д.И. Ульянова передать этот адрес К.И. Захаровой (Теодорке) и сообщить ей, что в случае побега (в это время К.И. Захарова была арестована) для нее у Алексеева есть 100 рублей [31].

Через неделю после приезда и устройства на место вторым личным и прямым адресом В.И. Ленина стал адрес: Mr. Jacob Richter (Holford) 30. Holford Square. Pontonville. London W.C., который впервые В.И. Ленин сообщил 23 апреля 1902 г. в письме П.Б. Аксельроду: «...вот Вам новый адрес (который просил бы очень не сообщать никому, даже из членов Лиги, кроме самых близких лиц...: остальные пусть пользуются попрежнему адресом Алексеева, а сторонние – адресом Дитца». Далее, в целях конспирации переезда из Германии В.И. Ленин просил: «...постарайтесь и в разговорах употреблять систематически Мюнхен вместо Лондона и мюнхенцы вместо лондонцы» [32].

В истории развития искровских конспиративных связей это был первый случай, когда действительный адрес В.И. Лени-

на, по которому он и Н.К. Крупская проживали до начала мая 1303 г. в Лондоне, применялся для непосредственного получения писем. Этот адрес использовался для связи с узким кругом лиц – Г.В. Плехановым, П.Б. Аксельродом, В.Д. Бонч-Бруевичем.

Затем область применения В.И. Лениным личных немецких и английских посреднических адресов расширилась. Они стали использоваться для важных и экстренных связей. Так, 16 апреля 1901 г. Н.К. Крупская в конспиративном письме в Россию шифром сообщила адрес доктора К. Лемана, которому следовало направлять деньги, собранные для «Искры» [33]. Финансовый вопрос всегда беспокоил В.И. Ленина, так как потребность в деньгах была большой.

В другом случае, в письме, направленном Н.К. Крупской в Петербург 21 февраля 1902 г. для агента «Искры» М.А. Сильвина, излагался план нелегального перехода границы в Восточной Пруссии и по прибытию в Мюнхен указывался как явка адрес доктора Лемана [34].

С приездом в Мюнхен Н.К. Крупской переписка с ней В.И. Ленина по адресу Модрачека была прекращена, но адрес был сохранен для связей и продолжал успешно действовать. Им стали пользоваться искровские группы в России. Так, в феврале-марте 1902 г. Московский комитет РСДРП отправил по адресу Модрачека посылку и деньги, а по адресу доктора Лемана две бандероли [35]. Успешно использовался также адрес Ф. Регнера. В январе 1902 г. на этот адрес для редакции «Искры» Московский комитет РСДРП выслал революционные прокламации [36]. Этот же адрес в апреле того же года, незадолго до ареста использовал М.А. Сильвин, который должен был доставить в русскую типографию «Искры» в Кишиневе текст прокламации Харьковского комитета РСДРП. Однако до Кишинева М.А. Сильвину доехать не удалось и он вынужден был отправить текст прокламации почтой для редакции «Искры» [37].

Адреса общего назначения. С развитием массовых искровских связей большое значение приобрели посреднические адреса общего назначения, используемые редакцией «Искры»

для повседневных сношений как с Россией, так и с заграницей. Заграничные посреднические адреса для связи с ленинской «Искрой» имелись в большинстве западноевропейских государств: в Германии (Мюнхен, Штутгарт, Гамбург, Нюрнберг, Лейпциг, Кенигсберг, Берлин, Шарлотенбург, Веймар, Дармштадт, Ширвиндт, Вюрцен); Швейцарии (Цюрих, Женева, Берн); Франции (Париж); Бельгии (Льеж, Брюссель); Швеции (Стокгольм); Австро-Венгрии (Прага, Лемберг); Англии (Лондон). В Мюнхене, например, в период 1901-1903 гг. действовало 5 известных нам посреднических адресов общего назначения: M. Bley, Dietrich Buchbinder, Richard Etzold, проживавшие в разное время по адресам: Kaiserstrasse 42-1, Pundterplatz, 4, Kaiserstrasse 33III; Frau Wind, St. Paulstrasse 3III; Max Ettinger, Amalienstrasse, 38. В Лейпциге в связи с тем, что там до начала июня 1901 г. находилась нелегальная типография «Искры», посреднические адреса в этом городе для связи с Россией не применялись. С начала июня 1901 года, когда типография готовилась к переезду в Мюнхен, в Лейпциге стало использоваться до семи адресов: Dunsker; Dr. F. Hordnung, проживавшие по двум адресам: Blumnerstrasse, 25, Antonienstrasse, 3; Richard Illge; Muller; K. Pinkau по адресам: Hohenzollernstrasse, 13, Turnsstrasse, II; Karl Arnold; Clara Wehmann.

В исследуемый период по несколько посреднических адресов имелось почти в каждом городе, через которые осуществлялась переписка. Так, в Берлине действовало 11 адресов, Нюрнберге – 5 адресов, в Лондоне – 6 адресов и т.д.

После переезда редакции «Искры» в Лондон с середины апреля 1902 г. в искровские связи были введены бельгийские адреса, обеспечивавшие более быструю пересылку корреспонденции из России в Лондон и обратно. В Льеже действовало 6 адресов, ранее не применявшихся для связи: Alphonse Pire по адресам, – rue Duny, 55 au rue Vivegni, 351; Heinrich Bologne; Joseph Bologne, Mr. Carl, Julien Defraine; Paul Marechal по двум адресам – rue St Jean N 18 и rue Neuvice II.

В Дармштадте (Германия) искровцы в конспиративные целях использовали 5 посреднических адресов и этот город

стал одним из важнейших пунктов обеспечения безопасности связи редакция с Россией: Heinrich Lenges по двум адресам: Liebfrauenstrasse, 37, Tuhrmannstrasse, 12; W. Nsubaur; A. Ettling; Loht.

В целях противодействия «Черному кабинету» и прикрытия переписки от перехвата агенты «Искры» при связи с редакцией рассредоточивали переписку по многим направлениям с применением большого числа посреднических адресов.

Так, например, в 1902–1903 гг. Е.Д. Стасова (Петербургский комитет РСДРП) связь с «Искрой» поддерживала по 18 конспиративным адресам в Германии, Англии, Швейцарии и Бельгии:

Немецкие адреса: Мюнхен – Gabesbergerstrasse, 20a, Dr. K. Lehmann; Pundterplatz, 4, Kaiserstrasse 42-1, Kaiserstrasse 33III, Richard Etzold; Нюренберг – Neue Gasse, Cugarrenhaundlung Herr Philipp Rogner; Лейпциг – Hernn Pinkau Photogaph Turnerstrasse, II; Karl Armold, Kaufmann, Leipzig – Plag; Берлин – Georg Grewling, Sharlottenburg – Berlin Spreostrasse 60; Karl Anders, Salzwedelstrasse 8; Friedlander Thomashewsky, Eldsterstrasse, 25; Herrn Julius Gerson, Burgstrasse, 30; Дармштадт – Herrn W. Weubauer, Hainheimerstrasse, 50; Herrn A. Ettling, Liebfrauenstrasse, 45, Bierhaille; Loth.

Английские адреса: Лондон – A. P. Hazell, 85, Avenall Rd, Highbury, Elfort Road, Aldert Park; W. A. Woodroff, 26, Barsett Road Nunhead.

Шведские адреса: Стокгольм – Strandvagen, Herr C. A. Andersson (Cafe), Hubersgarten, 8; Fr. Andersson H. Tegnersgarten II (Hidur).

Бельгийские адреса: Льеж – Alphonse Pire, rue Dany, 55a; Paul Merechal rue Neuvice, II.

Специализированные адреса. По мере развития конспиративных искровских связей посреднические адреса тоже дифференцировались по узкому направлению конспиративной работы. Специализация адресов проявилась как одна из форм повышения конспирация переписки. Так, например, в августе 1902 года Московский комитет РСДРП переписывался

с «Искрой» по двум адресам: Herrn Richard Illge, Eisenbahnstrasse, 3, Leipzig. Этот адрес применялся для присылки писем и корреспонденции, а второй – Herrn Jacob Betsch, Senefelderstrasse, 50 b. IV, Stuttgart (специализированный) использовался только для пересылки денег [38], в этих же целях применялся искровскими группами в России берлинский адрес – Herrn Julius Gerson Burgtrasse, 30II, а адрес Heinrich Lenges, Liebfrauenstasse, 37, Darmstadt был сообщен в начале января 1903 г. Н.К. Крупской – Г.М. Кржижановскому в Самару для присылки за границу паспортов, по которым изготовлялись в Берлине их копии, используемые при поездках в Россию [39].

Своеобразный порядок связи установила в середине июля 1905 г. редакция «Искры» с социал-демократом Емельяном, работавшим в Одессе и передавшим газете адрес для денег: «Одесса, Куяльницкий лиман, Гавриле Петровичу Иваненко. Для присылки новых номеров «Искры»: Куяльницкий лиман, городское лечебное заведение; Одесса, редакция «Одесских Новостей». З.К.У. Адрес для писем: Польская, Бирнбаум... фамилию подчеркнуть» [40].

Открытые адреса «Искры». Помимо конспиративных адресов редакция «Искры» для широкой связи со своими корреспондентами и читателями имела три открытых адреса, один из которых принадлежал социал-демократу, руководителю издательства Германской социал-демократической партии И.Г. Дитцу в Штутгарте. В типографии издательства печатались журнал «Заря», работа В.И. Ленина «Что делать?» и другая социал-демократическая литература. По своему применению этот адрес также был посредническим и в ряде номеров газета «Искра» извещала об этом читателей: «По поводу многократных обращений к нам с вопросами о том, как сноситься с «Искрой» людям, попадающим за границу, мы повторяем, что из-за границы следует посылать все и всякие письма, материалы и деньги на адрес Дитца в Штутгарте – Verl. S. H. Dietz Nachfolger, Stuttgart для редакции «Заря». Редакция «Заря» всегда будет немедленно пересылать все получаемое ею для «Искры». Убедительно просим всех пользую-

щихся этим адресом на внешнем конверте писать только адрес Дитца, указания же о передаче (для ред. «Заря») должны делаться на внутреннем конверте» [41].

Этим же адресом пользовался В.И. Ленин в случаях, когда необходимо было установить тесные связи с руководителями западноевропейских социал-демократических партий. Так, в письме к лидеру социал-демократической партии Швеции К.Я. Брантингу 19 апреля 1901 г. в целях привлечения шведских и финских социал-демократов к сотрудничеству в газете «Искра» В.И. Ленин сообщил этот адрес для связи с ними [42].

Два других адреса применялись для пересылки материалов, рукописей и денег (из-за границы) и принадлежали: один в Цюрихе (Швейцария) – П. Б. Аксельроду (Hrn Paul Axelrod, Vogelsangstrasse 9/II, Zurich), а второй в Париже (Франция) – группе содействия «Искре» – Bibliotheque du Parti Ouvrier Francais, 36, rue Hall, Paris [43].

Значительную сложность при организации связи представлял подбор держателей конспиративных адресов как за границей, так и в России. Редакция газеты должна была полностью быть уверена в том, что переписка осуществляется через надежные руки.

Агентам «Искры» и социал-демократическим организациям приходилось испытывать значительные трудности в подборе конспиративных адресов, а их требовалось большое количество. Во-первых, конспиративные адреса должны были обеспечивать регулярное получение и сохранность получаемой из-за границы корреспонденции, а их владельцы по своему социальному положению не должны были вызывать подозрений у полиции своими связями с адресатами в заграничных городах. Во-вторых, владельцы адресов – это лояльные люди, стоящие в стороне от революционного движения. По этому поводу в одном из писем к В.П. Ногину, который имел связь с Полтавой, В.И. Ленин писал: «Дайте, пожалуйста, 2-3 адреса вполне надежных людей (сторонних, не революционеров) для того, чтобы явиться к ним в Полтаве...» [44].

За границей, как правило, держателями конспиративных адресов являлись местные социал-демократы, люди массовых профессий или дюди из «общества», не связанные с революционным движением, но обладавшие безукоризненной честностью. Среди них были владельцы трактиров, пивных баров – Rittmeyer, Ettling; врачи – K. Lehmann M. Bley, A.P. Hazell, F. Hordnung; книгоиздатели – Dietrich; владельцы кафе – C.A. Andersson; книжных магазинов – Muller; торговых лавок – Rogner, Clara Wehmaan; коммерсанты – K. Arnold; члены рейхстага – K. Pinkau. После переезда редакции и типографии газеты «Искры» в Лондон свой домашний адрес передал для использования «Искрой» коммерческий директор типографии Максимуса Эрнста в Мюнхене – Рихард Этцольд.

В России конспиративные адреса подбирать было сложно, так как значительная часть русской интеллигенции боялась преследования полиции. Владельцы этих адресов должны были обладать большим мужеством. Так, в письме в «Искру» 13 ноября 1901 г. ее представитель в Одессе К.И. Захарова просила помочь ей достать необходимые адреса для связи: «...Нет адресов. Здесь немыслимо прямо-таки достать, все трусят смертельно» [45].

В качестве конспиративных адресов в России использовались адреса владельцев различных магазинов, служащих учреждений (земских управ, консерватории в Москве, Статистического комитета, банков), адвокатов, а также адреса врачей, медицинских сестер, студентов и др. Так, например, в адрес Международного торгового банка в Москве (для Алексея Никитича Дементьева) 7 июля 1902 г. было отправлено письмо В.И. Ленина с подписью «Мейер». [46].

«Избранный нами способ сношений, – отмечала редакция «Искры», – представляющий на первый взгляд многие неудобства, оказался вполне целесообразным. Если соблюдать все меры предосторожности, материал доставляется скоро и аккуратно» [47]. Следовательно, почтовая связь была положительно оценена редакцией «Искры», но при этом необходимо было изыскивать способ, каким бы она «могла сноситься с каждым корреспондентом».

Письма из России за границу нередко отправлялись непосредственно в почтовых вагонах скорых и пассажирских поездов. Это давало возможность избегать вскрытия писем на почте и таким образом миновать местную цензуру. Кроме того, «Черный кабинет» не всегда мог определить, из какого именно города было послано опущенное в почтовый вагон письмо, чтобы начать розыск его автора. Еще в 1901 г. в переписке с социал-демократами в Самаре, Выборге и других городах Н.К. Крупская настоятельно рекомендовала отправлять письма таким способом. Так, например, письмо В.И. Ленину от 12 февраля 1902 г. о съезде искровских агентов в Самаре и его решениях, написанное З.П. Кржижановской, было опущено в почтовый вагон пассажирского поезда №64 (Самара-Ряжск) по адресу: Frau Posa Beeken Wilhelmsburgerstrasse, 43, Hamburg [48]. Аналогичным способом из Нижнего Новгорода с пассажирским поездом №12 (Нижний Новгород-Москва) 12 июля 1902 г. было направлено «Искре» конспиративное письмо без подписи на адрес Karl Pinkau, Turnerstrasse,II,Leipzig [49].

В случае крайней необходимости в искровских конспиративных связях использовался телеграф. Однако при выборе средств связи для пересылки корреспонденция В.И. Ленин предпочитал почту телеграфу. В письме, отправленном в августе 1901 г. Л.Е. Гальперину в Баку, он указывал: «Мы послали телеграмму, – смысл ее понятен – согласие. Но имейте в виду, что сношения телеграфом очень опасны, с телеграмм ведь снимаются копии. Старайтесь ограничиваться почтой» [50], в связи с этим телеграф в деятельности «Искры» и социал-демократических организаций использовался крайне редко. Если же возникала необходимость что-либо телеграфировать, то обычно передавался короткий заранее обусловленный текст. Так, для получения чемодана с искровской литературой из Берлина группа содействия «Искре» в Полтаве должна была послать своего человека в Бреславль как ближайший к границе город и оттуда по имеющемуся адресу телеграфом передать условную фразу в Берлин: Heinrich, schickt zwei (oder drei) [51]. (Генрих, присылай два или три.) Телеграмму следо-

вало подписать фамилией владельца паспорта отправителя, так как при получении на почте чемоданов, высланных из Берлина до востребования, необходимо было предъявить на указанную фамилию документ.

Успешная работа редакции «Искры» зависела от устойчивости связей с агентами газеты и ее корреспондентами. В этом отношении был предпринят ряд мер.

Для проверки надежности того или иного адреса, а также звеньев (цепочек) связи практиковалась посылка обыкновенных писем самого невинного содержания. Адресат извещал об их получении, после чего завязывалась регулярная переписка. В другом случае, по договоренности посылка такой открытки являлась сигналом о том, что «Искра» выслала конспиративное письмо, а поэтому надо быть готовым к его приему. О посылке таких открыток просил, например, Г.М. Кржижановский в письме в «Искру» 5 августа 1902 г. Он писал: «Перед посылкой письма всякий раз присылайте невинную открытку на адрес «Медвежонка» (М.И. Ульянова [0]), с таким расчетом, чтобы она пришла на один-два дня раньше письма» [52]. Кроме того, регулярное получение таких открыток убеждало редакцию газеты в том, что адресат жив и продолжает работу. По этому поводу В.И. Ленин и Н.К. Крупская в письме, отправленном в Смоленск в июне 1901 г., просили следующим образом уведомлять о надежности посреднического адреса и, естественно, сохранности самих адресатов:

«Пусть адресаты, если они дали свой адрес не на один только раз, извещают о получении, чтобы знать, что адресат действителен. Пусть каждый выберет какие-нибудь 2 буквы и пишет на один из немецких адресов (у вас есть таковые?) незначительную открытку, подписывая этими буквами» [53].

С расширением конспиративных связей и переписки редакция «Искры» стала располагать большим количеством посреднических адресов и корреспонденции. В целях упорядочения их учета Н.К. Крупская в конце 1901 г. ввела порядковую нумерацию заграничных адресов. Это мероприятие имело двойной смысл. Во-первых, отпала необходимость каж-

дый раз в переписке указывать полное наименование адреса, и, во-вторых, повышало конспиративность искровских связей в борьбе с «Черным кабинетом».

Одновременно Н.К. Крупская завела тетрадь регистрации входящих и исходящих писем, регулярно отмечая сведения о корреспонденции: когда (дата) отправлена или получена, на какой адрес, кому выслана, исполнение [54]. Как редакция «Искры», так и ее агенты изыскивали различные способы адресования писем. Одним из них была посылка «до востребования» без указания адреса получателя с расчетом, чтобы не привлечь внимания охранки к адресату.

Часто при пересылке корреспонденции уславливались, что, если письмо следует для передачи, то фамилию следует подчеркнуть. Это был внешний сигнал для адресата, который знал, кому в действительности предназначалось письмо. Никаких других пометок о передаче письма в этом случае на конвертах не делалось.

Устойчивость искровских связей определялась также расширением сети корреспондентов. В больших городах «Искра» имела, как правило, по несколько корреспондентов. В случае ареста одного из них другие продолжали поддерживать письменную связь с газетой. Проваленные посреднические адреса немедленно отменялись.

В деятельности агентов «Искры» и ее Русской организации одним из важнейших практических условий устойчивости организации профессиональных революционеров была преемственность, которая достигалась подбором «наследников» – проверенных людей, у которых сосредотачивались не только связи с «Искрой», но и связи внутри социал-демократической организации. Непременное условие при этом – быть нейтральными людьми по отношению к охранке, не заниматься революционной деятельностью и, следовательно, не находиться под наблюдением полиции. Так, Г.М. Кржижановский в апреле 1902 г. писал в редакцию «Искры»: «Имейте в виду, что если я буду изъят, то надо в Самаре отыскать служащего в губернском земстве Николая (Ивановича Соловьева), он совершенно

свой человек, все дела будут переданы ему. Вторым наследником назначаю служащего в коммерче(ском) отдел(ении) Самаро-Златоустовской ж. д. (Конрада Газенбуша); если такой погибнет, надо будет прислать сюда для получения тетрадки, где записаны все наши связи, особого человека, связи зашифрованы там ключом.., она будет храниться у (Александра Дмитриевича Попова) – элеватор... Пароль: «Я от брата» [55]. «Наследников» имели Н. Э. Бауман, Е. Д. Стасова и многие другие агенты «Искры».

Приступая к изданию газеты «Искра», В.И. Ленин вначале сам выполнял техническую работу по связям с Россией потому, что практически лишь к весне 1901 г. мюнхенская часть редакции «Искры» и «Зари» собралась вместе. «Владимир Ильич, – писала А.И. Ульянова-Елизарова, – с жаром взялся за работу, которая вначале, особенно вследствие малого количества работников, была для него в большей мере черновой; приходилось самому вести переписку, шифровку, налаживать транспорт, связи с Россией» [56]. Эта важная, но тяжелая работа отрывала В.И. Ленина от насущных дел и забот издательского дела, а их было немало. Об этом он писал 18 октября 1900 г. П.Б. Аксельроду: «Загорская (И.Г. Смидович [0]) все не едет, а работы по ведению переписки становится все больше и больше. Я временами изнемогаю и совсем отвыкаю от своей настоящей работы» [57].

С октября 1900 г. секретарем редакции «Искры» была И.Г. Смидович (по мужу И.Г. Леман), с апреля 1901 г. – Н.К. Крупская. В.И. Ленин считал, что назначение Н.К. Крупской секретарем редакции было необходимо для дела. Ближайший друг и верный соратник В.И. Ленина Н.К. Крупская проявила большой организаторский талант, упрочивая и развивая связи с агентами «Искры», группами содействия газеты, социал-демократическими организациями, формируя «русскую социалистическую почту». Она внесла выдающийся вклад в организацию, развитие и совершенствование конспиративных искровских связей.

Н.К. Крупская налаживала и поддерживала связи с Россией не только путем конспиративных писем, но и через газету. Начиная с первого номера, в «Искре» был введен специ-

альный отдел – «почтовый ящик». В нем помещались короткие сообщения, предназначенные для адресатов, находящихся в России. В «почтовом ящике» давались указания по вопросам связи («2а3б. Все получаем. Спасибо, пишите»; «307н. Не имели от вас ни писем, ни корреспонденции»); адресов и явок («4ММ. Корреспонденции получены, дайте адрес для писем и явки»; «Адрес № 22 отменяется»; «Адресом № 16 просим пользоваться возможно реже»; «17852. Просим не писать на прежний адрес. Постарайтесь достать другой, или дайте нам адрес, чтобы мы могли написать вам».) [58].

Вопросы техники нелегальных связей, освещаемые в газете, способствовала регулярности переписки с Россией. Каждый корреспондент, имея очередной номер «Искры», мог найти в нем дополнительные указания о связях, способах переписки и конспиративных адресах (только их номерах).

Следовательно, указания, помещаемые в «почтовом ящике», повышали устойчивость искровских связей. «Почтовый ящик» явился средством управления конспиративными искровскими связями с Россией.

Значительную долю труда в развитии «русской социалистической почты», связей «Искры» и переписки внесли ее агенты, профессиональные революционеры. Их обязанности не ограничивались только решением общепартийных вопросов. Одной из важнейших обязанностей, которую практически выполняли они, был поиск и подбор адресов для получения конспиративных сообщений, организация корреспондирования с мест, собирание и восстановление разорванных связей, способы их конспиративного прикрытия.

В.И. Ленин осуществлял повседневное руководство деятельностью агентов. «Владимир Ильич просматривал каждое письмо, – вспоминала Н.К. Крупская. Мы знали очень подробно, кто из агентов «Искры», что делает, и обсуждали с ними всю их работу...» [59].

Следовательно, организация искровской переписки характеризовалась широким применением посреднических адресов, прикрытием связей и мерами, направленными на усиление ее устойчивости и против «Черного кабинета».

Способы конспирации переписки

Условия подпольной работы требовали от искровцев разработки и соблюдения не только способов внешней конспирации нелегальной корреспонденции, но и применения внутренней конспирации передаваемой информации. Поэтому велико было стремление департамента полиции проникнуть в тайну конспиративных писем, чтобы уяснить состояние и развитие революционного движения в России и, руководствуясь полученными сведениями, осуществлять различные мероприятия по борьбе с революционерами. Внутренняя конспирация – обоюдоострое оружие. Одним острием она направлена против охранки, а другим, в случаях расконспирации – против революционных организаций. Именно поэтому возникали взаимоисключающие задача и интересы двух противостоявших сторон.

В связи с создавшимся положением ответственные задачи и обязанности легли, на плечи революционеров, ибо проникновение в тайны революционного движения розыскных органов наносило непоправимый урон организационной работе искровцев, подчас сводя на нет все усилия, предпринимаемые в этом направлении. С другой стороны, с установлением прочных нелегальных связей количество получаемых и отправляемых редакцией «Искры» писем значительно увеличилось, что повышало вероятность их перехвата «Черным кабинетом». Все это в конечном счете определило тот размах незримой борьбы, которая развернулась между революционными социал-демократами И «Черным кабинетом» по вопросам нелегальной переписки.

Социал-демократическая мысль в вопросах противодействия происками политической полиции непрерывно занималась усовершенствованием способов конспирации информации, содержащейся в нелегальной переписке. При организации конспиративных связей с Россией «Искра» разрабатывала приемы конспирации переписки, добиваясь чтобы ее содержание не могло стать достоянием не только полиции, но и

любого постороннего человека, в руках которого по каким-либо причинам могло оказаться конспиративное письмо.

Обычно содержание каждого нелегального письма состояло из открытой и конспиративной части. Открытая часть содержала сведения, которые не только не раскрывали существа революционной работы, но и вообще не касались даже отдаленно этой области деятельности. Конспиративную же часть составляли сообщения, характеризующие подпольную работу комитетов РСДРП, групп содействия и агентов «Искры», установление нелегальных связей и распространение литературы, транспортировку «Искры» и другие вопросы. В ней указывались посреднические адреса, пароли для установления личных связей, открытые и условные названия городов, ключи шифров, фамилии лиц, содержащих явочные квартиры, и другие важные сведения.

Техника составления конспиративного письма была сложной, трудоемкой, требовала определенных навыков, аккуратности и точности.

Чтобы подготовить конспиративное письмо, надо было его написать с учетом характера содержащихся в нем сведений, затем подчеркнуть в тексте все те предложения и слова, которые являлись конспиративными и их следовало зашифровать, потом произвести шифрование текста, проверить правильность шифровки во избежание пропусков и искажений при использовании того или иного заранее обусловленного ключа шифра. После этого необходимо было подготовить внешнее, фиктивное письмо, которое было вполне обычным и по содержанию не могло бы вызвать подозрения у цензоров. Далее, подобрать соответствующий сорт бумаги и между строк внешнего письма химическими чернилами написать конспиративное сообщение.

Примером может служить письмо, отправленное Н.К. Крупской 13 ноября 1901 г. из Мюнхена (через Нюрнберг) в Одессу К.И. Захаровой.

Внешне письмо было вполне безобидным. В нем сообщалось:

«12.XI.1901. Дорогая моя! Получила ли ты мое последнее письмо. Я сильно сомневаюсь, верен ли адрес. Повтори его

еще раз. Как ты живешь? От тебя что-то давно нет уже писем. Хорошо ли ты устроилась? Не сырая ли у тебя комната? У меня к тебе еще просьба. Пришли несколько открыток с видами Одессы, одна моя знакомая очень хотела бы иметь таковые. Тут мода собирать коллекцию открыток и мне очень хотелось бы доставить удовольствие моей знакомой. Если ты еще не послала биографию Ибсена, то мне ее больше не надо, пришли только Спинозу. Раздобудь, пожалуйста, ту книжку (Херс. губ. и пр.), о которой я тебя просила. Очень она нужна.

Сейчас тороплюсь и поэтому кончаю письмо, крепко целую. Всего хорошего. Твоя (подпись не разборчива)» [60].

Между строк этого внешнего письма химическими чернилами было написано бесцветное письмо следующего содержания: «Письмо от 25/X получено, но предыдущее, очевидно, не получено, в котором Вы сообщали адрес для писем; также не получено письмо новой группы. Дайте адрес для писем и явки. Это ведь чрезвычайно важно. Вы сами это знаете. Адрес для денег получен... Деньги, посланные Вам, вернулись обратно. Ставьте на письмах номера, только не путайте. Я буду делать то же. Это письмо №I. Грач (Н.Э. Бауман [0]) меняет адрес для явки. Новый адрес: Мещанская, Старо-Екатерининская больница, спросить фельдшерицу Рукину, сказать ей; «я от Зои». Впрочем, если воспользоваться старым, то беды особенной нет. ...Посылаю на всякий случай хороший адрес для писем: Hermann Schneider, ob Wohrdstrasse, 21II, Nurnberg [61].

При составлении конспиративных писем Н.К. Крупская придерживалась большой осторожности. Подготовив основу письма, его конспиративные элементы, как-то: посреднические адреса, ключи шифров, фамилии лиц или их псевдонимы вписывались в текст непосредственно перед отправкой письма. Этот вывод основывается на сопоставлении некоторых подлинников писем и их перлюстраций. Поэтому в редакционном архиве многие подлинники писем отложились в первоначально исполненном виде, а в архиве охранки в несколько ином более полном, в таком, как они были отправлены по почте. Редакция «Искры», опасаясь возможного напа-

дения тайной полиции, стремилась раньше времени не доверять конспиративных тайн бумаге. Вместе с тем следует полагать, что Н.К. Крупская отдельно вела учет ключей шифров, паролей, который можно было легко уничтожить в случае возникшей опасности.

При подготовке писем в Россию Н.К. Крупская вначале определяла степень конспиративности сведений, помещаемых в письме, затем волнистой чертой подчеркивала слова и предложения, которые необходимо было зашифровать и, кроме того, ослабить с помощью шифра логические связи в предложении. Это значительно затрудняло охранке в случае перлюстрации или захвата писем выявление содержания зашифрованных участков текста и, следовательно, повышало степень конспирации переписки.

Помимо писем, непосредственно написанных В.И. Лениным или Н.К. Крупской, многие из них содержали правки, добавления или изменения в первоначально подготовленном тексте, внесенные В.И. Лениным, Н.К. Крупской или другими членами редакции газеты. Редакция с большой тщательностью относилась к ведению своей конспиративной переписки.

Очень часто внешнее письмо готовилось измененным почерком на языке той страны, куда оно направлялось или откуда исходило. Чаще всего это был немецкий, французский или английский язык.

Довольно часто как само письмо, так и адрес, надписанный на конверте, исполнялись печатными буквами. Кроме того, письма выполненные лицами мужского пола, иногда имитировались как письма, направляемые якобы от женщин. Это был один из видов конспиративного прикрытия, преследующий цель затруднить охранке проведение экспертизы почерков и определение по ним автора письма.

Другая особенность искровской переписки заключалась в том, что в ней применялось много условностей, отдельные письма или их части приобретали иносказательную форму о событиях, предмете переписки, известных только адресату. Так, в письме к Н.К. Крупской от 16 июля 1902 г., выступая

против преждевременного созыва съезда искровцев, работавших в России, В.И. Ленин писал: «Л. Гр. теперь и сам откладывает это «до осени». Пожалуйста, постарайся и сама «разнести» эту ерунду со «съездом». Надо видеть теперь же Лаптя: он повидает и швейцарцев и сам к нам приедет. Чего еще? Затем Повар, видимо, нуждается еще в ученье, – и пусть поучится в Цюрихе; это отлично. Может быть, он, как И Б. Н., еще месяцы просидит за границей??? Чего же торопится видеть? «А когда захочет ехать, он сам должен приехать к нам, и нечего его тащить теперь. И какую это чепуху пишет Бергу Б.Н. и З.Б.: «нельзя разговаривать без П.Б. «С кем? с Поваром – он у П.Б.С тремя лицами – они у П.Б. С Лаптем – он будет у П. Б. Посоветуй Бергу хорошенько выбранить В.В. и Б.Н. за эту чепуху и напиши мне, как Берг смотрит, и есть ли надежда, что он им ответит так, чтобы отбить охоту блажить» [62]. Псевдонимы и сокращения в этом письме означали: «Л. Гр.» – Л.Г. Дейч, «Лапоть» – П.Н. Лепешинский, «По-вар» – Ф.И. Шеколдин, «Б. Н.» – В.А. Носков, «Берг» – Ю.О. Мартов, «П. Б.» – П.Б. Аксельрод.

Псевдонимы и сокращения, применяемые в переписке, значительно усиливали ее конспирацию, были чрезвычайно разнообразны и часто менялись. 9 псевдонимов имел В.И. Ленин (Ильин, Ленин Н., Мейер, Петров, Старик, Тяпкин, Фрей, Meyer, Richter J.), 5 – Н.К. Крупская (Катя, Мария, Рыбка, Рыбочка, Тоня), 5 – Д.И. Ульянов (Андрей, Подопечный, Стар, Фит, Юноша), 7 – Н.Э. Бауман (Грач, Григорьев, Макс, Орлов, Николай Петрович, Полетаев, Мах), 4 – Г.В. Плеханов (Дядюшка, Дядя, Дядя Юра, Жорж), 9 – В.И. Засулич (В.И., В. Ив., Велика, Велика Дм., Велика Дмитриевна, Карелин, Сестра, Старшая сестра, Kiroff) и др.

Среди псевдонимов можно встретить названия животных, птиц: Теленок (П.Б. Струве), Медведь, Медвежонок (М.И. Ульянова), Грач (Н.Э. Бауман), Лошадь (Л.Б. Красин), Лань, Суслик (Г.М. Кржижановский), Мышь (П.И. Кулябко). Иногда псевдонимы применялись в виде отдельных букв латинского алфавита: zz (И.Х. Лалаянц), х (Л.М. Книпович) и др. Русские буквы В.И. Ленин и редакция «Искры» употребляли реже и в

каком-нибудь сочетании, например, ъ/з (Л.Е. Гальперин), 2а3в (П.Н. Лепешинский). Изредка встречались псевдонимы в виде имен литературных героев, например, Рахметов (А. Богданов), Инсаров (П.И. Кулябко).

Довольно часто в качестве псевдонимов употреблялись имена собственные: Катя (редакция «Искры»), Нина (Бакинская типография), Юрий («Южный рабочий»), Аркадий (И.И. Радченко), Андрей (Д.И. Ульянов), Соня (Бюро Русской организации «Искры»). При обозначении названий городов первая буква имени соответствовала первой букве названия города, например, Маша (Москва), Паша (Псков), Осип (Одесса).

Одним из основных способов внутренней конспирации переписки искровцев являлись шифры. С ростом революционного движения в России и расширением искровских связей шифрованная переписка революционных социал-демократов значительно увеличилась,

В.И. Ленин уделял большое внимание шифрам и шифрованной нелегальной переписке. Он сам умел шифровать, расшифровывать сообщения, применять тайнопись, разрабатывал шифры, учил революционеров приемам шифрования, проявлял большую осторожность в передаче конспиративных сведений [63]. Так, например, 24 января 1901 г. В.И. Ленин писал В.П. Ногину: «Мне сообщили фамилию того петербуржца, который делал (в провинции и довольно глухой) предложение издать перевод Каутского. Боюсь доверить фамилию почте – впрочем, передам Вам ее таким образом. Напишите имя, отчество (на русский лад) и фамилию Алексея и обозначьте все 23 буквы цифрами по их порядку. Тогда фамилия этого Петербуржца составится из букв: 6-й, 22-й, 11-й, 22-й (вместо нее читайте следующую по азбуке букву), 5-й, 10-й и 13-й» [64].

Настоящее имя, отчество и фамилию «Алексея» (Мартова) – Юлий Осиповичъ Цедербаумъ – В.П. Ногин знал, поскольку он с ним в то время переписывался. Его фамилия и цифры 6, 22, 11, 22, 5. 10, 13 послужили ключом для сообщения В.И. Лениным фамилии петербуржца. Чтобы ее узнать, необходимо было пронумеровать каждую букву (по старому

русскому алфавиту). В первой строке написать цифры, а под ними текст следующим образом:

I	2	3	4	5	6	7	8	9	10	11	12
ю	л	и	й	о	с	и	п	о	в	и	ч
13	14	15	16	17	18	19	20	21	22	23	
ъ	ц	е	д	е	р	б	а	у	м	ъ	

Теперь по цифрам (ключу), который указал В.И. Ленин, можно расшифровать фамилию: 6, 22, 11, 22, 5, 10, 13 – с м и м о в ъ. В фамилии Смирнов В.И. Ленин опустил букву «р», чтобы не передавать ее полностью и не подвергать риску Смирнова, а буква «н» была передана как «м», так как в ключе шифра ее не было. В.П. Ногин должен был догадаться, о ком идет речь, поскольку он был знаком с Б.М. Смирновым по совместной работе в группе «Рабочее знамя» в Петербурге.

Каждый профессиональный революционер должен был уметь пользоваться шифрами, правильно составлять текст писем, зашифровывать и расшифровать их, применять тайнопись. Овладение искусством нелегальной связи с применением шифров для каждого из них считалось обязательным, ибо незнание приемов конспирации связи, неумение и ошибки, допускаемые в шифрованной переписке, усложняли связь и в конечном итоге могли привести к ее утрате, создали бы возможность проникновения охранки в среду социал-демократических организаций. Без овладения этим искусством конспиративная связь была бы невозможна. Так, например, в письме к Фиту (Д.Я. Ульянову) от 16 декабря 1902 г. В.И. Ленин писал: «Ваше письмо от 15/XI получено. 1. Написано оно неизвестным нам ключом, впрочем, мы расшифровали все, за исключением адресов. (Не шифруйте иначе, как целыми фразами, иначе очень легко раскрыть ключ). Адреса повторите...» [65].

В искровской переписке, поскольку она в основном велась с применением тайнописи, зашифровывался, как правило, не весь текст, а только наиболее конспиративные сведения. В письмах В.И. Ленина и редакции «Искры» зашифровывались названия городов, фамилии, посреднические адреса для

писем, денег, корреспонденции, пароли, ключи шифров, сведения, непосредственно относящиеся к практической деятельности по устройству типографий, распространению нелегальной литературы и др. Это положение подтверждается некоторыми примерами, которые дают представление о сведениях, подлежащих шифрованию.

Так, Н.Э. Бауман в письме к В.И. Ленину 12 июня 1901 г. сообщал: «...Получил Ваше письмо на новый адрес. У меня есть человек, который желает посвятить все свои силы и средства на постановку типографии («Чайная фирма»). Есть очень удобная земля для дома и средства на постройки» [66]. В другом письме И. И. Радченко 17–19 февраля 1902 г. в редакцию «Искры» говорилось: «...Получили ли вы все это. Свой адрес сообщит сам, будет писать ключом «Брожу ли я вдоль улиц» Пушкина, начиная с пятой строки... Еду в Воронеж и к Паше... Четвертого должен выехать к вам Бродяга... По ключу «Три пальмы» пишите по адресу: Таганка, дом Сергия ТРОЦЫ, кв. 29, Елизавете Анисимовне СМИРНОВОЙ» [67]. В обоих письмах были зашифрованы выделенные слова в предложении.

Шифры, применяемые В.И. Лениным, редакцией «Искры», агентами газеты и социал-демократическими организациями в России, усложнялись по мере развития связей и овладения профессиональными революционерами техникой нелегальных связей.

Как показало проведенное исследование в искровской переписке наибольшее применение нашли следующие виды шифров [68]. (Название шифров приводится в соответствии с принятой терминологией, которой пользовались революционные социал-демократы в 1900–1903 гг.)

Шифр по слову. Для построения шифра этого вида в качестве ключа бралось одно (например, Собакевичъ, Александръ и др.) или несколько слов, заключенных подчас в предложения (например, За немощь побили Франца и др.). По этому ключу строился шифр. Ключ записывался вертикально в прямоугольник, размеры которого определялись по вертикали количеством букв, входящих в состав слов (предло-

жений), а по горизонтали – 28 и 30-ю буквами старого русского алфавита. Начиная с каждой буквы слова, по горизонтали выписывался алфавит. Таким образом, в прямоугольнике были выписаны несколько полных алфавитов. Шифрованные знаки писались в виде дробей, числителем которых служил номер строки, а знаменателем – место буквы в строке. Например, 3/1, 3/3, 6/2 и т.д.

Пример 1.

	1	2	3	4	5	6	7	8	9	10	11
1	С	т	у	ф	х	ц	ч	ш	щ	ы	ъ
2	О	п	р	с	т	у	ф	х	ц	ч	ш
3	Б	в	г	д	е	ж	з	и	к	л	м
4	А	б	в	г	д	е	ж	з	и	к	л
5	К	л	м	н	о	п	р	с	т	у	ф
6	Е	ж	з	и	к	л	м	н	о	п	р
7	В	г	д	е	ж	з	и	к	л	м	н
8	И	й	к	л	м	н	о	п	р	с	т
9	Ч	ш	щ	ы	ь	ю	я	а	б	в	г
10	Ъ	ю	я	а	б	в	г	д	е	ж	з
…	21	22	23	24	25	26	27	28	29	30	…
…	и	й	к	л	м	н	о	п	р	с	…
…	д	е	ж	з	и	к	л	м	н	о	…
…	ц	ч	ш	щ	ы	ь	ю	я	а	б	…
…	ф	х	ц	ч	ш	щ	ы	ь	ю	я	…
…	а	б	в	г	д	е	ж	з	и	к	…
…	ы	ь	ю	я	а	б	в	г	д	е	…
…	ч	ш	щ	ы	ь	ю	я	а	б	в	…
…	ю	я	а	б	в	г	д	е	ж	з	…
…	н	о	п	р	с	т	у	ф	х	ц	…
…	с	т	у	ф	х	ц	ч	ш	щ	ы	…

Приведенной в качестве примера табличкой шифра по ключу «Собакевичъ» в 1901 г. пользовалась Н.К. Крупская для связи с социал-демократическими организациями в России [69]. Если, например, следовало зашифровать сообщение: «адрес для явки: Москва, Кузнецкий мост, 21», то, пользуясь правилами шифрования, текст выглядел так: 4/1 3/4 1/29 3/5 8/10 8/27 3/10 3/28 9/7 4/3 5/1 8/1 1/25 2/1 2/4 4/10 3/2 4/1

5/1 2/6 4/8 1/25 3/5 2/9 3/9 1/21 6/2 5/3 2/1 5/3 9/26 21. При этом способе шифрования возможны и другие варианты, важно было не повторять одни и те же буквы из одной строки, встречающиеся в предложении. Цифры, означающие номера домов, писались в тексте открыто.

Текст расшифровывается в обратном порядке: вначале отыскивалась строка (числитель), а затем столбец (знаменатель).

Этот вид шифра был характерен для начального этапа развития искровских связей и по мере их совершенствования применялся все реже. Начиная с 1902 года, он больше в искровской переписке не встречался.

Простой квадратный шифр. В квадрат (10 × 10) вписывались произвольно взятые слова, короткие предложения или буквы. Колонки и строки шифра нумеровались. Иногда в квадрат вписывался книжный текст. Тогда шифр носил наименование квадратный книжный. Буквы алфавита, которые ни разу не встречались в тексте, вписывались в конец квадрата. Столбцы и строки квадрата нумеровались двойным или тройным рядом цифр. В этом виде шифра при умелом шифровании уменьшалась частота повторяемости шифрзнаков, но как и в предыдущем виде шифра оставалась частота повторяемости знаков, заложенная в русском языке.

Пример 2.

			1	2	3	4	5	6	7	8	9	10
			11	12	13	14	15	16	17	18	19	20
			21	22	23	24	25	26	27	28	29	30
1	11	21	з	в	е	з	д	ы	у	с	ы	п
2	12	22	в	ъ	с	у	м	р	а	к	е	
3	13	23	к	а	к	ъ	б	е	з	м	я	т
4	14	24	б	л	е	щ	е	т	щ	ъ	и	
5	15	25	т	у	ч	к	и	п	ъ	ю	т	
6	16	26	ф	т	о	т	о	о	м			
7	17	27	д	е	н	а	д	о	е		д	
8	18	28	н	е	т	н	а	р	а			
9	19	29		о	г	р	д	а	р		о	
10	20	30	в	ъ	м	е	с	я		ц	и	

Приведенным в качестве примера шифром пользовался в мае-октябре 1901 г. для переписки с В.И. Лениным и редакцией «Искры» Н. Э. Бауман [70]. В этом шифре каждый знак имел девять различных обозначений. Например, буква «в» могла быть зашифрована следующими цифрами: 1.2 1.12 1.22 11.2 11.12 11.22 21.2 21.12 21.22.

30 октября 1901 года Н.Э. Бауман писал в «Искру»: Сижу с пустыми руками (у Н. Э. Баумана в то время не имелось нелегальной литературы для распространения [0]). Положение мучительное. Со всех сторон требования. Пожалуйста, сообщите немедленно, установлены ли у Вас сношения со следующими пунктами: 2.3 3.2 2.5 9.6 9.7 13.2 3.1 8.6 1.1 19.6 8.1 18.1 5.5 3.12 18.11 15.5 4.9. Даны ли Вами все необходимые условия для правильных сношений (адреса для писем, явки и т.п.)?» [71].

С использованием таблички шифра МОЖНО прочитать зашифрованный текст. Н. Э. Бауман спрашивал о связи редакции «Искры» со следующими пунктами: «Самара Казан(ъ) Нижний». Для усложнения конспирации вертикальная и горизонтальная стороны квадрата были занумерованы цифрами от 1 до 30 по порядку, образовав трехрядный ключ. Шифрзнаки записывались без знака дроби, через точку. Шифрование производилось так же, как и в первом примере.

Стихотворный шифр. Имел наибольшее распространение в искровской переписке в 1901–1903 гг. Ключом шифра служило стихотворение. Шифрзнаки обозначались через дробные числа по всему стихотворению или части его, числитель – строка, знаменатель – номер буквы в строке. Например, 2/1, 2/3 и т.д.

Пример 3.

	1	2	3	4	5	6	7	8	9	10
1	н	у	п	о	ш	е	л	ж	е	р
2	н	е	б	о	е	л	ь	н	и	к
3	н	е	в	е	с	е	л	а	я	л
4	э	й	с	а	д	и	с	ь	к	о
5	н	о	г	и	б	о	с	ы	г	р
6	и	е	д	в	а	п	р	и	к	р
7	н	е	с	т	ы	д	и	с	ь	ч
8	э	т	о	м	н	о	г	и	х	ъ
9	в	и	ж	у	я	в	к	о	т	о
10	т	а	к	у	ч	и	т	ь	с	я

В качестве примера приведен шифр по ключу стихотворения Н.А. Некрасова «Школьник». В письме В.И. Ленина к Л.Н. Радченко, написанном в июле 1901 года, рукой Н.К. Крупской была сделана приписка следующего содержания: «Паше. Отчего давно нет писем? Как дела с техникой? Отчего никогда не присылаете корреспонденции? Имейте в виду, что скоро получите письмо за подписью Яблочков (В.П. Ногин – *авт.*), ключом «У лукоморья дуб зеленый» (или «Школьник»)» [72]. Как следует из этого сообщения, В.П. Ногин должен был прислать Л.Н. Радченко письмо, зашифрованное по одному из указанных ключей. В данном примере часть стихотворения вписана в квадрат 10 × 10.

Выбор стихотворного шифра для конспиративных связей был не случаен. Во-первых, стихотворение можно было выучить наизусть, а затем составить табличку шифра и, во-вторых, революционер-подпольщик ничем не рисковал, перевозя с собой томик стихотворений, который на самом деле является сборником ключей для конспиративной переписки.

В качестве ключей больше всего употреблялись стихотворения поэтов-демократов, чья литературная деятельность была ближе по духу революционной молодежи в борьбе за светлое будущее. Так, редакция «Искры» в ноябре 1900 года переписывалась с Ю. Мартовым, который находился в то время в Полтаве, по стихотворению А.С. Пушкина («Брожу ли я вдоль улиц шумных...») [73]. Д.И. Ульянову ключом для переписки с «Искрой» служило стихотворение С.Я. Надсона «Мгновение» («Пусть нас давят угрюмые стены тюрьмы, мы сумеем их скрыть за цветами...»). И.И. Радченко в 1901–1902 гг. – «Дума» М.Ю. Лермонтова, «Меж высоких хлебов затерялося...» – Н.А. Некрасова, для связи с Киевским комитетом РСДРП – стихотворение «Я вчера еще рад был отречься от счастья...» С.Я. Надсона. И.И. Радченко для внутрироссийской переписки имел второй ключ: «Маша» – стихотворение Н.А. Некрасова, а для непосредственной связи с Баку (нелегальная типография «Нина») применял ключ такой же, как и для переписки с «Искрой» – «Дума» М.Ю. Лермонтова. Для связи с

Одесской группой РСДРП – «Мать» С.Я. Надсона, Екатеринославской – «Два горя» С.Я. Надсона, Е.Д. Стасовой – «Колыбельная» Н.А. Некрасова и басня И.А. Крылова «Дуб и трость». Г.И. Окуловой – басня И.А. Крылова «Крестьянин в беде». Тульскому комитету РСДРП для связи с Московским комитетом по подготовке II съезда партии – «Памятник» А.С. Пушкина. Казанскому комитету РСДРП – «Парадный подъезд» Н.А. Некрасова. Московскому комитету РСДРП для связи с Самарой – «Несчастные» Н.А. Некрасова. А.П. Паромовой – «Мцыри» М.Ю. Лермонтова и «Маша» Н.А. Некрасова. И.Г. Леман – «Мать» С.Я. Надсона. В.И. Трелиной – «Молитва» («В минуту жизни трудную...») М.Ю. Лермонтова и др.

Впоследствии наблюдалось стремление искровцев избегать применения в качестве ключей к шифрам произведения известных поэтов и писателей, а использовать произведения малоизвестных поэтов, народные песни, революционные сатирические стихотворения. Так, в ноябре 1901 г. из Киева И.Г. Леман и в январе 1902 г. из Пскова П.Н. Лепешинский переписывались с редакцией «Искры», применяя распространенное в то время в революционных кругах стихотворение «Гимн новейшего русского социалиста» [74].

Иногда в целях усложнения одно письмо шифровалось по нескольким ключам с различных строк. Так, И.Г. Леман во время поездки в Россию в конце 1901 г. письмом от 18 января 1902 г. предупредила Н.К. Крупскую о том, что «2а3в (П.Н. Лепешинский [0]) меняет для себя ключ. Он берет тот же, что и мой с Вами, позднейший, но будет считать не с первой строки, а со второй, первую строку совсем отбросить. Он будет ждать, пока Вы перемените ключ, а потом уже и сам перейдет на новый» [75].

Книжный шифр (страничный). Этот вид шифра широко вошел в практику искровских конспиративных связей с 1902 г. После того, как редакции «Искры» стало известно о том, что конспиративная искровская переписка перехватывается «Черным кабинетом», этот шифр стал основным. Шифрзнаки составлялись из номера строки и номера буквы в этой строке и писались в виде дробей. Ключ шифра обозначался номером

страницы и проставлялся среди шифрзнаков текста. Номер страницы образовывался путем произведения или суммы цифр числителя и знаменателя. Ключ шифра вначале проставлялся в тексте на первом, а затем на любом условленном месте. Дроби, предшествовавшие указателю, были фиктивными. Текст конспиративного письма мог шифроваться по одной или по нескольким страницам.

В качестве шифра применялись книги. Так, у «Северного Союза» находилась книга В.И. Ленина «Развитие капитализма в России», у Л.М. Книпович, Харьковского и Николаевского комитетов РСДРП – «Биография Спинозы» издания Павленкова, у Рижской искровской группы – рассказ С.Г. Скитальца «Сквозь строй» и «Композитор», П.Ф. Куделли – «Челкаш» с пятой строки и т.д. Во всех случаях было важно, чтобы стихотворные и страничные шифры использовались революционерами по книгам одного и того же года издания.

Шифр «Гамбетта» (гамбеттовский шифр) [76] получил широкое применение в искровской переписке. (Гамбетта Леон Мишель (1839–1882) французский политический и государственный деятель, один из лидеров буржуазных республиканцев. Применял этот вид шифра для конспиративной переписки.) Техника использования этого шифра была следующая. Для того, чтобы зашифровать сообщение, бралось одно или несколько слов, известные только лицам, которые вели переписку. Например, «НЕБО ЛАЗУРНОЕ В МОРЕ...». Каждая четная или нечетная буква в предложении подчеркивалась, получался набор, состоящий из следующих букв: «НБЛЗРОВОЕ». Имели место случаи, когда использовался бессмысленный набор букв определенной длины. Впоследствии такой набор букв для краткого произношения стал называться гаммой.

Буквы открытого текста и гамма нумеровались цифрами в порядке их расположения в 28-ми или 30-ти буквенном русском алфавите. Затем из цифр открытого текста вычитались по модулю 28 или 30 цифры гаммы. В результате этих действий сообщение было зашифровано. Для отделения одного предложения от другого в начале каждого из них могла проставляться

трехзначная цифровая группа вида 127, 267, 311 и т.д. Эта группа была условной и при расшифровании текста сообщения не учитывалась. Например, необходимо было зашифровать следующий текст: «Сообщите адрес, явки, пароли».

В цифровом обозначении этот текст имел вид: 17 14 14 2 25 9 18 6 1 5 16 6 17 1 29 3 10 9 15 1 16 14 11 9. Бралась гамма – НБЛЗРОВОЕ и согласно принятым правилам шифрования производилось вычитание:

	17	14	14	02	25	09	18	06	01	05	16	06
—	13	02	01	08	16	14	03	14	06	13	02	01
	04	12	13	24	09	25	15	22	25	22	14	05
	17	01	29	03	10	09	15	01	16	14	11	09
—	08	16	14	03	14	06	13	02	01	08	16	14
	09	15	15	00	26	03	02	29	15	06	25	25

В случае, если верхняя цифра была меньше нижней, то к ней прибавлялась цифра 30 и по модулю производилось вычитание. Таким образом получалось: 02 – 08 = 24 (32 – 08 = 24) и т.д. Окончательно зашифрованный текст имел вид: 127 04 12 13 24 09 25 15 22 25 22 14 05 09 15 15 00 26 03 02 29 15 06 25 25. Расшифрование производилось в обратном порядке, т.е. цифры шифрованного текста складывались по модулю 30 с цифрами гаммы.

В своей переписке с «Искрой» гамбеттовский шифр применяла А.А. Кузнецова, С.Н. Афанасьева. Этим же видом шифра 10 апреля 1902 г. было зашифровано и направлено письмо В.И. Ленину об итогах Белостокской конференции представителей комитетов и организаций РСДРП делегата от «Заграничной лиги русской революционной социал-демократии» на этой конференции Ф.И. Дана. Часть согласованных решений нам известна в виде «Резолюции конференции» [77]. Но в Белостоке были приняты важные конспиративные решения, непосредственно относящиеся к вопросам созыва II съезда РСДРП. Эту часть решений по соображениям конспирации участники конференции договорились в виде печатных или рукописных

документов не оформлять и согласовали их между собой устно, чтобы совершенно секретные сведения не стали достоянием охранки. Поэтому они в исторических и архивных материалах не отложились, тем более, что многие участники конференции вскоре были арестованы. И только косвенным путем, по хранящимся в ЦПА ИМЛ и ЦГАОР СССР документам можно судить об их содержании [78].

После окончания конференции представитель «Заграничной лиги русской революционной социал-демократии» из Белостока почтой отправил В.И. Ленину известные резолюции конференции (открытую часть) и частично зашифрованное по двум ключам письмо, в котором описал порядок ее работы [79]. Эти документы «Черный кабинет» не смог обнаружить, и они благополучно были получены редакцией «Искры».

Часть письма, зашифрованное по первому ключу, Н.К. Крупская расшифровала. Вторая же в подлиннике по неизвестным для нас причинам оставалась не расшифрованной.

Не имея сообщения об остальных решениях конференции и подозревая, что представитель Лиги арестован, В.И. Ленин 22 апреля из Лондона обратился к А.К. Крамеру (члену Заграничного комитета Бунда, участнику Белостокской конференции), который находился в Париже, а также к «Союзу русских солиал-демократов за границей» за необходимой информацией. Одновременно В.И. Ленин направил письмо Г.Д. Лейтейзену – представителю группы содействия «Искре» в Париже, поручая ему связаться с «Союзом» для ознакомления с остальными решениями конференции [80]. Из этих источников редакция «Искры», очевидно, неполностью получила интересующие ее сведения.

С момента описываемых событий прошло 78 лет и только тогда при проведения исследования удалось впервые расшифровать вторую часть письма представителя Лиги на Белостокской конференции и получить решения, которые с нетерпением ожидал В.И. Ленин. Эта часть письма начиналась словами: «Кроме того, приняты такие резолюции – во исполнение решений избран орг(анизационный) ком(итет). Выска-

зались за созыв съезда к концу лета. Загр(аничные) представители оповестят комитеты, Место встречи согласуют организации: «Искра», «Лига», «Союз» в короткий срок. Согласованы предложения для образования Загр(аничной) комиссии» [81]. Расшифровано из текста: 215 200 905 12 13 292 802 19 210 81 01 806 01 17 25 27 090 104 26 01 13 17 04 14 08 20 24 26 03 15 23 01 10 10 18 06 27 25 21 25 01 02 09 25 29 15 24 10 02 21 04 12 11 13 19 16 04 190 31 40 82 52 62 70 30 12 0 17 29 28 111 41 207 11 17 24 28 05 200 80 224 26 09 06 14 29 20 12 23 12 07 21 07 02 06 14 19 07 09 24 18 11 18 25 16 25 19 09 2629 17 10 25 01 11 08 25 26 192 31 62 219 20 26 010 50 917 16 11 25 180 30 80 40 91 30 31 63 14 116 2812 27 16 13 17 1926 23 2808 2528 1422 2114 222 116 28 114 29 для образования 18025 25 22 2417 02 20 09 06 02 01 27 23 09 204.

Как видно из письма, Белостокская конференция обсудила важнейшие вопросы подготовки съезда РСДРП. Был избран Организационный комитет, установлен срок созыва съезда, согласованы предложения для образования Заграничной организационной комиссии (Заграничного отдела ОК [0]) и определения места съезда. Кроме того, Белостокская конференция приняла решение о том, что созыв II съезда РСДРП, несмотря на участие в совещаниях представитей Бунда, поручается социал-демократическим организациям, чьи заслуги в развитии революционного движения в России были бесспорны. Эти данные расширяют имеющиеся в историко-партийной литературе сведения о Белостокской конференции и ряде других вопросов, связанных с подготовкой II съезда РСДРП.

Следовательно, применение большого количества шифров, их разнообразие и частая смена ключей подчеркивали стремление редакции «Искры» активно противодействовать работе «Черного кабинета» по дешифрованию переписки и были направлены на обеспечение безопасности своих конспиративных связей.

В.И. Ленин и «Искра» уделяли серьезное внимание шифрам и правилам их использования для конспирации переписки агентов газеты, искровских групп, комитетов РСДРП. В своих письмах В.И. Ленин неоднократно выражал озабочен-

ность безопасностью переписки и требовал строгого соблюдения правил ее ведения. Так, в письме, в июле-августе 1901 г. к Л.Е. Гальперину, который должен был из Баку сообщить конспиративные адреса в Екатеринославе для присылки в этот город искровской литературы, при ответе редакции «Искры» В.И. Ленин рекомендовал правильно составлять первичный текст. «Адреса пишите, разделяя слова, а то не понять, где имя, где город и улица» [82].

Выполняя основную работу по организации и ведений конспиративных связей и переписки с Россией, Н.К. Крупская также давала много ценных советов, учила своих корреспондентов правильно применять шифры и вести нелегальную переписку. Она не только в письмах, но и посредством «Искры» наладила руководство шифрованной связью с Россией. В «почтовом ящике» газеты Н.К. Крупская регулярно сообщала корреспондентам о состоянии шифрованной связи. Например, «М.У.Р. из Сибири. Зашифрованное письмо и шифр получили, но до сих сор не могли прочесть, так как не можем достать указанной книги». «Мирэ. Письмо не разобрано, просим правильно шифровать». «Зайчику». Письмо написано непонятным ключом». «Льву Львовичу. Письмо получено и разобрано» [83].

Помимо тех указаний по организации шифрованной связи, которые давала Н.К. Крупская своим корреспондентам, на страницах «Искры» помещались предостережения о правилах ведения шифрованной переписки. Так, например, в примечании к статье «Внимание революционеров!» редакция сделала важное примечание: «Добавим, со своей стороны, что шифр – оружие обоюдоострое, ибо жандармы лег-ко сумеют раскрыть всякий шифр, если не применять при шифровании особых предосторожностей. Безусловно необходимо: I) не отделять слова от слов; 2) не повторять часто одинаковых знаков, особенно знаков для наиболее употребительных букв; 3) писать шифр так, чтобы нельзя было узнать системы шифра; 4) не употреблять слишком известных стихотворений и книг. Без соблюдения этих правил шифр прямо-таки недопустим. Ред» [84].

Вся конспиративная переписка «Искры» велась в основном тайнописью с применением химических средств, что обеспечивало скрытность связи и создавало значительные препятствия для перлюстрации писем розыскными органами в России и за границей.

В искровский период, ведя обширную переписку с Россией, в одном из писем к А.А. Якубовой от 26 октября 1900 г., В.И. Ленин подчеркивал, что перепиской писем с их заделкой (в переплеты книг [0]) по имеющемуся у него адресу не занимается, а письма направляет только химией [85]. Н.К. Крупская пересылала многие письма В.И. Ленина – агентам «Искры», исполненные им тайнописью.

Имея большой опыт в тайнописи, В.И. Ленин учил своих корреспондентов правильному использованию химических составов. В письме от 4 августа 1902 г. к Картавцеву (псевдоним не раскрыт [0]) В.И. Ленин, в частности, писал; «Получили еще 2 Ваших письма и ничего не могли разобрать. Вы пишите слишком слабым составом.

Прежде чем написать – делайте каждый раз опыт. Ужасно досадно бывает получить письмо и быть не в состоянии его прочесть» [86].

По своим свойствам химические составы, применяемые для переписки, делились на две группы: I) проявляющиеся при нагревании и 2) проявляющиеся другими химическими веществами. Отбор химических средств для тайнописи был результатом многолетнего опыта русских революционеров. При нагревании бумаги с «химическим» текстом (например, над керосиновой лампой) происходила реакция и обычно обугливались те места, которые были написаны химическими чернилами. Текст письма, проявленный таким образом, приобретал коричневую окраску. К первой группе относились все кислоты, которые составляли основу химических чернил (слабые растворы серной и соляной кислоты, сок лимона, лук, молоко и др.).

Очень часто растворы кислот, содержащиеся в химических чернилах, воздействуя на бумажную массу, оставляли на

бумаге след. Если раствор кислот был слишком крепок, то под воздействием химической реакции через некоторое время наступало самопроявление, и конспиративный текст становился видимым. В этом случае «Черному кабинету» не представляло большого труда обнаружить конспиративное письмо. Чтобы этого не произошло, надо было предварительно приготовить раствор определенной концентрации. Делалось это опытным путем: раствор разбавлялся водой до тех пор, пока проявленный над лампой текст не был слишком ярким, ни слишком бледным, затрудняющим чтение.

Опытным путем также подбирался сорт бумаги и писчее перо, которое не должно было оставлять механических следов. От выполнения этих необходимых рекомендаций определялось качество писем, исполненных химическими чернилами, а это было крайне важно, чтобы сохранить непрерывность связи.

Н.К. Крупская в переписке со своими корреспондентами неоднократно указывала на необходимость соблюдения этих правил. Так, в письме к М.Г. Вечеслову 27 апреля 1901 г. она писала: «...Ваше письмо разобрали с трудом, бумага никуда не годится, сплошная мазня, берите такую, на которой мы пишем вам» [87]. О подборе качества бумаги, писать на более плотной, Н.К. Крупская советовала многим своим корреспондентам. В одном из писем к К.К. Газенбушу от 19 мая 1901 г. она давала рекомендацию о химической переписке: «Можно также писать... химией в обыкновенных письмах между строк, надо брать только толстую английскую бумагу, это наилучший способ сношений» [88].

После того как письмо было написано, ему давали высохнуть и мягкой белой резинкой подчищали участки бумаги, на которых был нанесен конспиративный текст, для устранения механических повреждений, сделанных писчим пером.

Применение сока лимона или лука ввиду неоднородности раствора имело определенные недостатки. Перед употреблением его необходимо было тщательно готовить, чтобы избегать самопроявления текста. Поэтому если в начальном периоде развитая искровских связей в качестве химических

чернил использовались в основном слабые растворы кислот, то в последующем они стали заменяться химическими составами, которые устранили недостаток – самопроявление. К этой группе относились соли свинца (азотносвинцовая соль, соль двууглекислого свинца и др.). Соли растворялись до получения насыщенного раствора, из которого при добавлении воды в соотношении 5:1 получался рабочий раствор чернил. Дальнейшая техника подготовки писем оставалась прежней. Эти средства тайнописи были очень просты в использования, но основной их недостаток заключался в том, что все конспиративные письма, исполненные такими химическими чернилами, проявлялись при нагревания.

Ко второй группе химических составов относился, например, уксуснокислый никель, а в качестве «проявителя» брался раствор диметилглиоксила или синеродистый калий, растворяемый в малой дозе в воде с «проявителем» полуторахлористого железа. Другим «проявителям» эти вещества не поддавались. Такие рецепты чернил с большей надежностью гарантировали тайну сообщений.

Для конспиративной переписки с «Искрой» изыскивались и другие химические растворы. Так, З.П. Кржижановская в письме от 21 мая 1902 г. в «Искру» предпочла следующий рецепт химических чернил: «Вот новый способ для переписки: писать 1%-м спиртовым раствором **В**-нафтола; чистить резинкой. Для проявления растворить немного паранитранилина в разведенной соляной или серной кислоте, прибавить туда несколько капель раствора азотно-натриевой или азотисто-калиевой соли и тотчас по приготовлении влить эту смесь в большой объем крепкого раствора уксуснолатриевой соли» [89].

В искровских связях тайнопись широко применялась в книгах, периодических изданиях, а иногда и в газетах. Текст писем исполнялся непосредственно между печатных строк. Этим способом связи пользовался В.И. Ленин в переписке с И.И. Радченко и другими агентами газеты. Так, в одном из писем он писал в Петербург:

«Посылайте непременно еженедельную газету правильно на адресе Rogner'a: нам необходима аккуратнейшая

переписка. И мы хотели бы посылать еженедельный специальный журнал: дайте скорее адрес врача, техника, велосипедиста, артиста и т. п.…» [90].

Стремясь избежать перлюстрации, В.И. Ленин, конечно, не мог прямо написать, что конспиративные письма будут помещаться в журналах, а поэтому он применил выражение «специальный журнал» в зависимости от профиля работы адресата, чтобы не привлечь внимание охранки.

В целях предупреждения адресата о том, что в книге имеется конспиративное письмо, на полях одной из страниц ставился условный знак (сигнал). К номеру страницы знака необходимо было прибавить заранее обусловленное число, чтобы определить страницу конспиративного письма. В другом случае страница начала корреспонденции указывалась «химией».

Иногда на страницах книг пересылались прокламации. Так, в письме от 20 декабря 1901 г., направленном из Харькова В.Н. Крохмалю, Харьковский комитет РСДРП просил разложить текст прокламации в искровской типографии в Кишиневе: «Одновременно посылаем в книге текст прокламации, о коей вам писано. Надо напечатать в типографии «Искры» тысячу штук, прошу употребить все усилия, чтобы ускорить печатание. Напишите, когда будет готово. Дайте адрес для явки. Мы пришлем человека» [91].

Впоследствии Н.К. Крупская так охарактеризовала применение тайнописи: «Пятнадцатилетний опыт убедил нас, что только правильно поставленная химическая непосредственная переписка гарантирует правильность сношений. И товарищи рабочие в свое время широко пользовались этим способом. Питерский рабочий Бабушкин ...ночи просиживал над химическими письмами, несмотря на свои больные глаза, и благодаря ему удалось тесно связать «Искру» не только с питерскими и московскими, но ивано-вознесенскими, ореховозуевскими и другими рабочими.

Писали нам «химией» екатеринославские, николаевские, одесские, уральские рабочие... Брались за дело сами, понимания, что это такая же обязанность революционера, как всякая другая» [92].

Одним из распространенных способов маскировки нелегальной корреспонденции, пересылаемой по почте, служили тайники в переплетах и корешках книг, куда тщательно заделывалась нелегальная корреспонденция. В.И. Ленин применял этот способ еще при переписке с группой «Освобождения труда». Так, в письме к П. Б. Аксельроду (середина ноября 1895 г.) он писал: «Получили Бреславльский отчет. Расклеили с несказанными усилиями, причем большую часть изорвали (письмо благодаря хорошей бумаге получилось целым). ...Во всяком случае способ годен, и его следует практиковать» [93]. Этим способом впоследствии пользовались редакция газеты «Искра» и социал-демократические организации в России для пересылки газет, листовок и другой нелегальной корреспонденции. Его сложность заключалась в том, что после сделанного вложения надо было очень тщательно переплести книгу, чтобы «Черный кабинет» не заметил в ней тайника. Кроме того, при вскрытии тайника необходимо было иметь соответствующие условия, чтобы извлечь из него содержимое. Как раз на это указывал Н.Э. Бауман в августе 1901 г. в письме из Москвы в редакцию «Искры»: «Ваш переплет получил... Только он причинил массу хлопот, несмотря на то, что этот способ я знал и имею опыт. Нужны слишком хорошие квартирные условия, чтобы без отлагательства добыть содержимое. Поэтому прибегайте к нему в крайнем случае» [94].

Используя этот способ пересылки нелегальной корреспонденции, Н.К. Крупская в то же время учила агентов газеты правилам пользования им. Так, в письме П.Н. Лепешинокому Н.К. Крупская подробно описала технику вскрытия тайника: «На днях пошлем Вам книгу в переплете. Переплет надо опустить в теплую воду, и, когда он станет расслаиваться, начать отделять листы, подставляя под кран с кипящей водой, надо только не спешить. Отделенные таким образом листы вытереть губкой, чтобы снять клей, потом дать высохнуть и сыроватыми положить под пресс» [95].

Тайнопись с применением химических средств для пересылки нелегальной корреспонденции являлась одним из основных способов внутренней конспирации искровских связей.

Она совершенствовалась по мере организационной работы, проводимой редакцией «Искры», как показал анализ, из 1392 документов, сохранившихся в архиве редакции газеты, охранкой было перехвачено, перлюстрировано и расшифровано лишь 119 (8,5%) [96].

Таким образом, организационная и практическая работа, проведенная В.И. Лениным, Н.К. Крупской, редакцией «Искры» и ее Русской организацией по широкому применению шифрованной связи и тайнописи в основном обеспечили надежность искровской конспиративной переписки.

В условиях нелегальной деятельности революционных социал-демократов конспиративная переписка была важнейшим средством связи, без которой немыслима была вся работа, проводимая В.И. Лениным, редакцией «Искры», профессиональными революционерами по созданию пролетарской партии нового типа. Переписка В.И. Ленина, редакции «Искры» с социал-демократическими организациями в России и за границей была чрезвычайно разнообразной и касалась многих проблем, относящихся к деятельности «Искры» и ее Русской организации. В письмах нашла отражение конспиративная постановка всего дела «Искры».

В.И. Ленин приложил немало сил для создания опорных пунктов общерусской нелегальной марксистской газеты в России, подбора ее первых корреспондентов, организации конспиративных связей с редакцией газеты.

Пересылка писем, книг, посылок осуществлялась, главным образом, посредством почты. В целях противодействия перехвату и перлюстрации корреспонденции связь между адресатами состояла из отдельных звеньев (цепочек) с использованием многочисленных посреднических адресов за границей. По способам назначения и применения искровские посреднические адреса подразделялись на личные и прямые адреса В.И. Ленина и членов редакции «Искры», адреса общего назначения, специализированные и открытые адреса «Искры». Устойчивость конспиративных связей достигалась путем применения «наследников» – держателей связей, явок и

паролей, а также через «почтовый ящик» (специальный раздел, введенный в газете «Искра»).

В целях конспирации содержания писем широко практиковались химические средства тайнописи шифры («шифр по слову», «простой квадратный шифр», «стихотворный шифр», «книжный шифр» (страничный), шифр «Гамбетта». Конспиративные письма очень часто исполнялись на страницах книг, журналов. Наиболее важные сведения, содержащиеся в письмах, шифровались, В качестве ключей искровских шифров применялись стихотворения и произведения поэтов и писателей-демократов: А.С. Пушкина, И.А. Крылова, М.Ю. Лермонтова, Н.А. Некрасова, С.Я. Надсона, А.М. Горького и др.

Для пересылки корреспонденции широко использовались тайники, в качестве которых, например, применялись переплеты книг, куда заделывалась корреспонденция.

Все эти меры, применяемые редакцией «Искры», профессиональными революционерами, значительно усилили защиту корреспонденции от проникновения в ее содержание «черного кабинета» и Особого отдела, способствовали устойчивости конспиративных связей и безопасности социал-демократических организаций.

Список рекомендуемой литературы

[0] Уральский Ю.С. Конспирация в деятельности Ленинской «Искры». – М., 1980.
[1] Ленин В.И. Полн. собр. соч., т. 47, с. 12.
[2] См.: там же, т. 46, с. 399.
[3] См.: там же, с. 406.
[4] Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т, I, с. 194.
[5] Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 22.
[6] Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 354.

[7] Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с, 318-320, 325-329. 350-351, 392-407, 413-415.
[8] См.: там же, с. 346.
[9] Таблица составлена на основании материалов Переписки В.И. Ленина и редакции газеты «Искра»... – М., 1969, 1970, т.т. I, 2, 3.
[10] См.: Степанов. В.И. Ленин и Русская организация «Искры». – М., 1968, с. 25 (примечание).
[11] Воспоминания о Владимире Ильиче Ленине. – М., 1979, т. I, с. 65.
[12] Большевики Смоленщины до октября 1917 года. Сб. документов. – Смоленск, 1961, с. 51.
[13] См.: Материалы по истории связи в России XVIII – начало XX в. – Л., 1966, с. 164.
[14] По данным советских исследователей к концу 1903 года в Германии и Бельгии редакция имела 30 посреднических адресов. (См.: Степанов В.И. Ленин и Русская организация «Искры», 1900-1903. М., 1968, с. 135). Новиков В.И. в кн.: Ленин и деятельность искровских групп в России. 1900-1903. – М., 1978, с. 116, со ссылкой на немецкого исследователя Wuttke Irmtraund считает, что искровцы для конспиративных связей в тот период имели 84 адреса.
[15] Ленин В.И. Полн. собр. соч., т. 55, с. 386.
[16] Там же, с. XV.
[17] Там же, с. 189.
[18] См.: Листовка редакции «Искры». К русским за границей. – Красный архив, 1934, т. 1(62), с. 141.
[19] Ленин В.И. Полн. собр. соч., т. 46, с. 52.
[20] См.: Ленинский сборник III, с. 74.
[21] См.: Ленин В.И, Полн. собр. соч., т. 46, с. 44, 49.
[22] Там же, с. 41, 45.
[23] См.: Ленин. Полн. собр. соч., т. 46, с. 49, 57.
[24] Там же, т. 55, с. 386.
[25] Там же, т. 46, с. 47.
[26] См.: Муравьева Л.Л. Сиволап-Кафтанова В.И. Ленин в Мюнхене. – М., 1976, с. 31.

[27] См.: Ленин В.И. Полн. собр. соч., т. 46, с. 72.
[28] Ленин В.И. Полн. собр. соч., т. 55. с. XV. с. 205. Иванов М. Ленин в Праге. – М.. 1963, с. 26-28.
[29] Ленин В.И. Полн. собр. соч., т. 55, с. 220.
[30] См.: там же, т. 46, с. 178, 179.
[31] См.: Переписка В. И. Ленина и редакции газеты «Искра»... – М., 1969, т. 2, с. 393.
[32] Ленин В.И. Полн. собр. соч., т. 46, с. 180.
[33] См.: Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. 1, с. 61.
[34] См.; Переписка В. И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 429.
[35] См.: ЦГАОР, ф. ДП. 00. 1901 г., д. 825, ч. 4. л. 55.
[36] Там же, ч. 6, л. 14.
[37] Там же, ч. 7, л. 60.
[38] См.: Переписка. В. И. Ленина и редакции газеты «Искра»... – М., 1969. т. 2, с. 174.
[39] См.: там же, т. 3, с. 77.
[40] Там же, с. 423.
[41] Искра, №№7, 9, 14.
[42] См.: Ленин В.И. Полн. собр. соч., т. 46, с. 94.
[43] См.: Листовка редакции «Искры». К русским за границей. – Красный архив, 1934, т. 1(62), с. 141.
[44] Ленин В. И. Полн. собр. соч., т. 46, с. 49.
[45] Переписка В. И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 305.
[46] Так, например, в адрес Международного торгового банка в Москве (для Алексея Никитича Дементьева) 7 июля 1902 года было отправлено письмо В.И. Ленина с подписью «Мейер». (См. Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. 2, с. 60).
[47] Искра, № 2.
[48] См.: Переписка В. И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 425; ЦГАОР, ф. ДП, 00, 1901- г., д. 825, ч. 4, л. 6.
[49] См.: ЦГАОР. ф. ДП, 00, 1901 г., д. 825, ч. 10, л. 139.
[50] Ленин В.И. Полн. собр. соч., т. 46, с. 136.

[51] См.: Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 71, 72.
[52] Там же, т. 2, с. 157.
[53] Переписка В.И. Ленина и редакции газеты «Искра»... – М., т. 1, 1969, с. 125.
[54] Там же, т. 3, с. 483-560.
[55] Переписка В.И. Ленина и редакции газеты «Исктра»... – М., 1969, т. I, с. 492, 493.
[56] Ульянова А. И., Ульянов В.И. (Н. Ленин). Краткий очерк жизни и деятельности. – М., 1934, с. 41.
[57] Ленин В.И. Полн. собр. соч., т. 46, с. 50.
[58] Искра, №№3, 8, 16. 22.
[59] Воспоминания о Владимире Ильиче Ленине. – М., 1979, т. I, с. 259.
[60] ЦГАОР, ф. ДП, 00. 1901 г., д. 825, ч. I, л. 33.
[61] Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 301, 302.
[62] Ленин В.И. Полн. собр. соч., т. 46, с. 199-200.
[63] См.: Сильвин М. А. В.И. Ленин в период зарождения партии. – М., 1958, с. 97.
[64] Ленин В.И. Полн. собр. соч., т. 46, с. 78, 484.
[65] Ленин В.И. Полн. собр. соч., т. 46, с. 239.
[66] Переписка В.И. Ленина И редакции газеты «Искра»... – М.,1969, т. I, с. 118.
[67] Там же, с. 443, 444.
[68] Название шифров приводится в соответствии с принятой терминологией, которой пользовались революционные социал-демократы в 1900–1903 гг.
[69] См.: ЦПА ИМЛ, Ф. 24. оп. 12, н, ед. хр. 1271, л. 1.
[70] См.: Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 243, 268, 269, 287, 288.
[71] Там же, с. 288.
[72] Переписка В.И. Ленина и редакции газеты «Искра»... – М.,1969, т. I, с. 166.
[73] См.: Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 39.

[74] См.: Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 334, 382; т. 2, с. 10. История Коммунистической партии Советского Союза. – М., 1967, т. I, с. 280, 281.
[75] Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, С. 383.
[76] Гамбетта Леон Мишель (1839-1882) французский политический и государственный деятель, один из лидеров буржуазных республиканцев. Применял этот вид шифра для конспиративной переписки.
[77] См.: КПСС в резолюциях и решениях съездов, конференций и пленумов ЦК. – М., 1970, т. I, с. 40-43 об.
[78] См.: Степанов В. Н. Ленин и русская организация «Искры». – М., 1968, с. 317-318.
[79] См.: Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 468.
[80] См.; Ленин В.И. Полн. собр. соч., т. 46, с. 182-184.
[81] См.: Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 471. Расшифровано из текста: 215 200 905 12 13 292 802 19 210 81 01 806 01 17 25 27 090 104 26 01 13 17 04 14 08 20 24 26 03 15 23 01 10 10 18 06 27 25 21 25 01 02 09 25 29 15 24 10 02 21 04 12 11 13 19 16 04 190 31 40 82 52 62 70 30 12 0 17 29 28 111 41 207 11 17 24 28 05 200 80 224 26 09 06 14 29 20 12 23 12 07 21 07 02 06 14 19 07 09 24 18 11 18 25 16 25 19 09 2629 17 10 25 01 11 08 25 26 192 31 62 219 20 26 010 50 917 16 11 25 180 30 80 40 91 30 31 63 14 116 2812 27 16 13 17 1926 23 2808 2528 1422 2114 222 116 28 114 29 для образования 18025 25 22 2417 02 20 09 06 02 01 27 23 09 204.
[82] Ленин В.И. Полн. собр. соч., т. 46, с. 137.
[83] Искра, №№29, 33.
[84] Искра, № 13.
[85] См.: Ленин В.И. Полн. собр. соч., т. 46, с. 53.
[86] Ленин В.И. Полн. собр. соч., т. 46, с. 215.
[87] Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 71.
[88] Там же, с. 89.

[89] Переписка В.И. Ленина и редакции газеты «Искра»... – М., 1969, т. I, с. 530.
[90] Ленин В.И. Полн. собр. соч., т. 46, с. 188.
[91] ЦГАОР, ф. ДП, 00, 1901 г., д. 825, ч. 2, л. 22.
[92] Степанов В. Н. Ленин и Русская организация «Искры». – М., 1968, с. 149, 150.
[93] Ленин В.И. Полн. собр. соч., т. 46, с. 10.
[94] Переписка В.И. Ленина и редакции газеты» «Искра»... – М., 1969. т. I, с. 197.
[95] Там же, с. 181.
[96] Там же, т. I, 2, 3.

Глава 6.

Криптография в России накануне и в период Русско-японской войны

Русско-японская война, начавшаяся 27 января 1904 г., стала одним из первых крупных конфликтов XX в. Война носила особый характер. Отчетливо обозначилось перерастание отдельных непродолжительных сражений в крупномасштабные и длительные военные операции (как новое явление в военном искусстве). В ходе боевых действий в массовом порядке стали применяться новые виды вооружений, например, пулеметы, броненосцы. Россия впервые применила подводные лодки[1]. Большое значение для переброски войск на Дальний Восток и снабжения действующей армии играл железнодорожный транспорт. Для управления войсками на огромных театрах военных действий и непосредственно в бою были использованы все средства связи, как применявшиеся на протяжении всей истории военной связи, так и созданные в конце XIX и начале XX вв. Война стала суровой проверкой состояния связи в оперативно-стратегическом звене управления войсками Российской Империи, значительно возросла роль телеграфа и телефона. С точки зрения истории криптографии главным событием русско-японской войны стало активное использование обеими сторонами радио. Россия стала пионером в новых видах боевых действий – радиоразведке и радиоэлектронной борьбе.

Военная угроза со стороны Японии в отношении России возникла еще в конце XIX в. В связи с этим была создана сеть

[1] Справедливости ради надо отметить, что русские подводные лодке в этой войне не потопили ни одного вражеского корабля, но во время боевых действий регулярно выходили в море на патрулирование. Само наличие подводного флота у России на Дальнем Востоке послужило серьезным сдерживающим фактором для Японии от расширения районов боевых действий, в частности нападения на Владивосток.

агентурной разведки против Японии. У одного из российских агентов был осведомитель – немецкий подданный К.Э. Маукиш, занимавший должность дратомана (переводчика) китайского адмиралтейства. С его помощью были добыты секретные сигнальные (кодовые) книги Японии. Сведения, полученные с помощью этих книг, оказались весьма значительными. В частности, были раскрыты планы Японии по завоеванию провинций Китая и Кореи. Всей агентурной операцией руководил полковник русской разведки К.И. Вогак.

До начала войны русской разведке удалось получить довольно значительные сведения о состоянии дел в японской армии и на флоте и о подготовке Японии к войне. С началом войны российская разведка сумела обзавестись значительным количеством агентов на территории Японии и Китая. В основном это были жившие там европейцы: журналисты, коммерсанты и др. Вербовать японцев и китайцев мешало отсутствие специалистов по Дальнему Востоку, знающих японский и китайский языки. Для связи с агентурой использовалось шифрование. Так, отправившийся в Японию англичанин Коллинз (он в инициативном порядке предложил свои услуги российской разведке, и они были приняты, так как Коллинз долгое время жил в Японии и Китая и знал специфику региона) должен был поддерживать связь с центром по телеграфу с помощью «особого шифра». К сожалению, авторам не известно, что за шифр использовал Коллинз, Возможно, это был один из агентурных шифров, описанных в статье [Бабаш, 2004].

Некоторые разведывательные данные поступали от дипломатов, морских атташе, чиновников Министерства финансов. Однако несмотря на некоторые успехи, в целом разведывательная служба России работала бессистемно. Общей программы не было. Такая ситуация имела место по всем разведывательным линиям, в том числе, и по линии против Японии. К тому же следует отметить, что хотя накануне войны Япония считалась серьезным противником, многие в руководстве Российской Империи, включая Николая II, считали японцев отсталой нацией и не верили в возможность развязы-

Николай II

вания Японией войны с Россией. Вследствие этих причин нападение японцев оказалось внезапным для России. Эти недостатки не замедлили сказаться в самом начале войны с Японией. Например, ко дню высадки японской армии на материк 1 апреля 1904 г. Россия не имела никакой информации о возможном времени и месте высадки.

Наряду с разведывательной деятельностью, военное и политическое руководство России в начале XX в. стало уделять внимание контрразведывательной работе. В начале 1903 г. было образовано разведочное отделение главного штаба Российской Империи (фактически первая официально созданная структура военной контрразведки в России). Оно сразу же начало активно противодействовать деятельности иностранных разведок в России. Одним из первых успехов новой спецслужбы был арест в феврале 1904 г. японского шпиона ротмистра Ивкова.

Некоторые эпизоды деятельности российских военных контрразведчиков напрямую связаны с криптографией. Так, в 1902 г. было установлено наблюдение за мелким чиновником Департамента торговли и мануфактур С. Васильевым, которого подозревали в шпионаже. В частности, было установлено, что Васильев продал одной иностранной державе чертежи из конструкторского бюро главного артиллерийского управления Военного ведомства. Чтобы убедиться в своих подозрениях, у него провели негласный обыск и обнаружили «секретный шифр». Уже одна эта находка послужила доказательством того, что Васильев – шпион. Следует отметить, что само наличие шифра у подозреваемого, часто служит поводом для обвинения в шпионаже.

Занимался разведывательной и контрразведывательной деятельностью и департамент полиции. В частности, в Санкт-Петербургском охранном отделении в начале 1904 г. было создано «специальное отделение о разведке военного шпионства» для наблюдения за иностранными военными атташе и сбора сведений в интересах русского военного командования. Образование этого подразделения произошло в результате бурной деятельности сотрудника департамента полиции И.Ф. Манасевича-Мануйлова (о нем подробно читайте в гл. 10). Он организовал агентурную сеть для разработки японских миссий в ряде европейских государств. Здесь удалось добиться некоторых успехов.

Однако донесения Манасевича-Мануйлова чуть не привели к серьезному дипломатическому скандалу между Россией и Великобританией. Осенью 1904 г., в связи с начавшейся войной с Японией, российская эскадра под командованием вице-адмирала Рожественского готовилась к переходу из Кронштадта на Дальний Восток в зону боевых действий. В это же время Манасевич-Мануйлов, находясь в заграничной командировке, сообщил, что он сумел добыть японский дипломатический шифр. Это якобы помогло ему проникнуть в замыслы японцев. В России ему поверили. В официальном документе МВД России отмечалось: «Этим путем были получены указания на замысел Японии причинить повреждения судам эскадры на пути следования на Восток». Эти сведения были переданы в генштаб и сообщены Рождественскому. К чему это привело рассказывает министр иностранных дел России А. Извольский: «В ночь на 21 октября 1904 г., когда флот адмирала Рожественского, направляясь на Дальний Восток, проходил Северное море, произошел серьезный инцидент в районе Доггер-банки. Повстречавшись с флотилией английских рыбаков и предполагая, что он окружен японскими кораблями, о пребывании которых в этих водах было сообщено русским бюро информации, адмирал приказал открыть огонь. Один из английских траулеров затонул, несколько других получили серьезные повреждения. Один из русских крейсеров – «Аврора» – тоже пострадал. Адмирал Ро-

жественский, несомненно, узнал на следующее утро о своей ошибке, но тем не менее, продолжал без остановки свой путь и настаивал на версии о японской атаке. Этот инцидент вызвал громадное негодование в Англии и едва не повлек за собой разрыв с Россией».

И вот как комментируется этот эпизод в [Лебедев, 2000]: «Какой-либо реальной угрозы эскадре Рожественского со стороны японцев в европейских водах, конечно, не было и быть не могло. «Информация» Мануйлова, по всей видимости, представляла собой его собственную выдумку или ловко подсунутую ему дезинформацию противника, которая чуть не привела к разрыву дипломатических отношений с Великобританией, что могло бы значительно ослабить и без того незавидное положение России в тот период». Интересно отметить, что в августе 1916 г. Манасевич-Мануйлов был арестован полицией за финансовые махинации, но суд над ним так и не состоялся по личному указанию Николая II.

К сожалению, жертвой агентурной деятельности по добыче шифров становилась и Россия. Накануне Русско-японской войны в Порт-Артуре были выкрадены планы укреплений крепости и шифры, использовавшиеся русским военным командованием. Кража была совершена под руководством небезызвестного Сиднея Рейли (о нем подробно читайте в гл. 10).

В основном дешифровальная работа против японцев была сосредоточена в министерстве иностранных дел. Некоторую работу непосредственно на театре военных действий проводили военные специалисты (об этом будет рассказано далее). Во время русско-японской войны шел очень оживленный обмен шифрованными сообщениями между Японией с одной стороны, и Англией и Германией с другой. При этом использовался код, который был составлен на английском языке и имел пять различных ключей. Одному из крупнейших специалистов дешифровальной службы царской России Владимиру Ивановичу Кривошу-Неманичу удалось раскрыть три ключа, с помощью которых «разбиралось» большинство перехватываемых телеграмм.

Заметим, что Кривош-Неманич активно занимался не только криптографией, но и стенографией. Изучил все известные системы письма – иероглифы, майское письмо, иератические, армянское, грузинское, еврейское и финикийское. В 1893 г. он опубликовал учебник стенографии по системе Гадельсберга, а в 1895 – собственный самоучитель стенографии. Позже он получил орден Александра Невского, а затем стал Главным цензором газет и журналов Российской Империи.

При работе по дешифрованию японской переписки большую помощь России оказала Франция, которая в то время была союзницей России. В Париже также работали над раскрытием упомянутого ранее пятиключевого кода. И небезуспешно. Были раскрыты два ключа. Правда один из них был уже известен Кривошу-Неманичу, зато другой – нет. Дешифрованные японские телеграммы французы пересылали в Россию. Таким образом, неизвестным для дешифровальщиков России и Франции оставался один ключ. Тогда министерство иностранных дел командировало Кривоша-Неманича в Париж для совместной работы с французами. Французы приняли российского криптографа как своего человек. Они ввели его в святая святых своей секретной службы – в «Surete generale». Там он проработал около 10 дней, пока не была раскрыта пятая составляющая японского кода.

Кроме того, Кривошу-Неманичу удалось подробно ознакомится с работой французской криптографической службой. Оказалось, что парижский «черный кабинет» был устроен аналогично петербургскому. Он располагался в частном доме с вывеской какого-то землемерного института. Один из служащих «черного кабинета» разбирался в вопросах лесоводства и землеустройства, и всегда давал квалифицированную справку частным лицам, интересовавшихся этими вопросами. В переднюю комнату мог зайти с улицы кто угодно. Здесь на стенах висели карты, планы лесов, земельных участков, имений и др., а столах лежали свежие газеты, вырезки из них, письменные принадлежности. Из этой комнаты была дверь в следующую, в которой также не было ничего секретного, но был шкаф, слу-

живший дверью в третью комнату. Чтобы попасть в третью, секретную, комнату, нужно было наступить одновременно на две дощечки на полу и нажать одно из украшений шкафа. «Дверь» открывалась перед входящим и закрывалась за ним автоматически. В третьей комнате, имевшей с помощью пневматической почты сообщение с главным телеграфом, проводилась регистрация поступивших телеграмм, их разбор по странам и передача по принадлежности в кабинеты дешифровальщикам. Дешифровальщики работали по двое. У них были подлежащие раскрытию коды, которыми они пользовались, и книга, в которую заносились все результаты их работы.

Эта книга передавалась в следующую комнату, там все сведения сортировались «по вопросам», содержащимся в сообщений. Из одной телеграммы делались несколько разных выписок, если она содержала информацию по разным вопросам. Один экземпляр таких выписок оставался в «черном кабинете», а другой отправлялся соответствующему руководителю (министру иностранных дел, военному или морскому министрам), а в наиболее важных случаях – и президенту Франции.

Кроме раскладки материалов «по вопросам», в «черном кабинете» делались еще и сводки «по вопросам». Это позволяло в любой момент времени получить информацию о ходе развития данного вопроса. При этом вопрос всесторонне освещался с разных точек зрения, если о нем писали представители разных правительств. Для президента ежедневно выпускался «листок» со всеми полученными за 1 сутки сведениями.

Почти все коды французы добывали агентурным путем. Так, французы активно использовали подкупленных служащих иностранных посольств для добывания криптоматериалов (включая порванные черновики секретных телеграмм, отправляемых в зашифрованном виде из этих посольств). Имелись у них и все русские коды, что не скрыли от Кривоша-Неманича. Однако он с удовольствием заметил, что один очень простой способ пользования кодом, изобретенный им самим и сообщенный министру, в Париже известен не был.

Интересно отметить следующий факт. По сообщению Кривоша-Неманича, все работники криптографической служ-

бы Франции (включая технический персонал – секретарей, машинисток, посыльных и др.) должны были быть заинтересованными в своей работе и не бояться ее потерять. В секретной части довольно часто работали жены, сестры служащих. Таким образом, целые семьи сплачивались одной идеей сохранения доверенных им тайн. От этого существенно зависело их семейное материальное благосостояние.

Владимир Иванович Кривош-Неманич стал первым русским криптографом, подробно познакомившимся с работой дешифровальной службы Франции того времени. Полученные полезные сведения были использованы русскими криптографами в практической деятельности.

После революции Кривош-Неманич сотрудничал с советской криптографической службой, передавая свой опыт молодым специалистам.

Перейдем к вопросу организации связи в российской армии на театре военных действий. К началу военных действий были сформированы управления армий, фронтов и ставка верховного главнокомандующего. Штабы фронтов координировали боевые действия нескольких армейских объединений, решавших задачи на различных стратегических направлениях. Планирование военных операций становилось все сложнее, усложнялось руководство боевыми действиями. Это приводило к необходимости высокой централизации управления и предъявляло новые повышенные требования к связи, особенно в оперативно-стратегическом звене управления.

Использование телеграфа, телефона и радио коренным образом меняло способы управления войсками и облегчало работу верховного главнокомандования по объединению усилий больших масс войск для достижения единой цели во время боевых действий.

Принципы организации связи и способы поддержания ее в ходе боевых действий определялись введенными в 1904 г. «Уставом полевой службы» и «Наставлением для действия в бою отрядов из всех родов оружия». Организация связи в оперативно-стратегическом звене основывалась на принципе «снизу вверх».

Основой связи в стратегическом звене оставался телеграф. Сеть правительственного телеграфа связывала театры военных действий с административными центрами. На театре военных действий работа по строительству телеграфных линий в тылу возлагалась на полевое управление почт и телеграфов, а от главной квартиры – на телеграфные батальоны и роты.

После того, как были сформированы три Маньчжурские армии и введена должность главнокомандующего, уже после начала войны в районе сосредоточения действующей армии было учреждено почтово-телеграфное управление при главнокомандующем. Оно осуществляло общее руководство почтово-телеграфной частью как в ближнем общем тылу трех армий, так и в районах сосредоточения каждой армии, где действовали почтово-телеграфные учреждения.

Связь главнокомандующего вооруженными силами на Дальнем Востоке с империей обеспечивалась через центральное отделение телеграфа с помощью быстродействующих телеграфных аппаратов Уитстона. Для связи главнокомандующего с армиями использовались буквопечатающие телеграфные аппараты Юза (рис. 6.1).

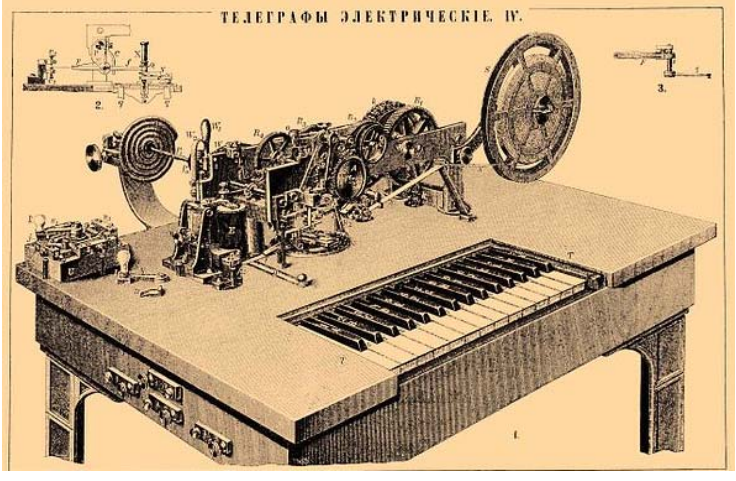


Рис. 6.1. **Телеграфный аппарат Юза**

В целях лучшего использования местной сети связи и средств военного телеграфа в июне 1904 г. при штабе Маньчжурской армии было учреждено телеграфное отделение. Оно передвигалось по железной дороге вслед за командующим и его штабом и представляло собой центральную станцию. При переводе Главной квартиры в Мукден вагоны с телеграфным отделением передвигались 2 суток, и в это время связи главной квартиры с Петербургом не было. Чтобы избежать подобных перерывов связи в дальнейшем, телеграфное отделение было разбито на два: центральное телеграфное отделение и телеграфное отделение при главнокомандующем. Перемещение осуществлялось поэшелонно. Центральное телеграфное отделение, таким образом, стало первым подвижным узлом связи армейского типа.

Первые же боевые действия русских войск показали, что полевой (правительственный) телеграф не в состоянии в полном объеме обеспечить связью войска. В распоряжении штаба армии должны были быть собственные полевые средства связи. В этих целях генерал А.Н. Куропаткин добился решения о формировании военно-телеграфного батальона. Формирование первого восточно-сибирского военно-телеграфного батальона было завершено в мае 1904 г. В конце сентября 1904 г. батальон прибыл по железной дороге в район Мукдена. Он стал использоваться штабами главнокомандующего и армий. Военно-телеграфный батальон стал первым в русской армии подразделением, обеспечивающим организацию связи в оперативно-стратегическом звене управления.

В ходе русско-японской войны важное значение для управления войсками приобрела телефонная связь. Преимущества этого вида связи по сравнению с телеграфной связью заключались в ее большей мобильности, что играло немаловажную роль в условиях позиционной войны. Появление на театре военных действий микротелефонных аппаратов и телефонных коммутаторов выдвинуло телефонную связь на первое место среди других видов связи. Так, уже в июне 1904 г. в одном из вагонов телеграфного отделения при штабе мань-

Адмирал Макаров С.О.

чжурской армии был установлен телефонный аппарат командующего. После завершения войны в руководящих армейских кругах неоднократно отмечалось, что телефон принес громадную пользу и работал превосходно.

Но самым перспективным видом связи на театре военных действий явился беспроволочный телеграф (радио). Главное его преимущество – это быстрота установления связи (в то время – до 40 мин.), и возможность организации связи через недоступные пространства и территорию, занятую противником.

Специфический характер дальневосточного театра военных действий потребовал применения радиосвязи для управления войсками. До русско-японской войны развитию радиосвязи на Дальнем Востоке не уделялось должного внимания, и лишь назначение выдающегося русского флотоводца вице-адмирала Макарова командующим 1-й тихоокеанской эскадрой в корне изменило ситуацию. После его вступления в должность 24.02.1904 г. были предприняты энергичные шаги по внедрению радиосвязи в управление флотом. К марту 1904 г. почти все корабли оснастили радиостанциями. Тогда же началась реализация сделанного Макаровым еще в феврале 1904 г. предложения о создании цепи радиостанций на побережье Тихого океана. В сухопутных войсках действующей армии внедрение радиосвязи началось несколько позже. В апреле 1905 г. в Петербурге были сформированы 1-я и 2-я восточно-сибирские искровые (радиотелеграфные) роты. Это были первые полевые радиочасти русской армии. Они имели на вооружении по 8-ми радиостанций «Маркони» (рис. 6.2). Искровыми они назывались потому, что применявшиеся в них передатчики создавали электромагнитные колебания высокой

частоты с помощью искрового разрядника. Одна из рот (первая) стала обеспечивать радиосвязь штаба главнокомандующего со штабами всех трех маньчжурских армий.

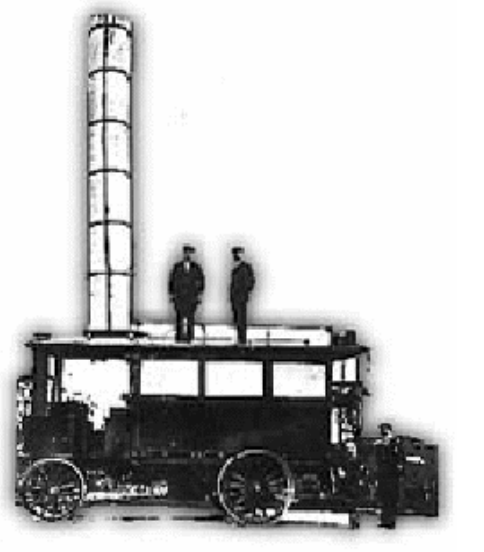


Рис. 6.2. **Автомобильная радиостанция «Маркони»**

При организации радиосвязи применялись два варианта, которые назывались радионаправление и радиосеть. С помощью первого варианта связь обеспечивалась только между двумя штабами, а при втором – связь осуществлялась между несколькими штабами. При главнокомандующем русскими войсками было создано управление начальника радиотелеграфа.

Таким образом, русская армия не только первой в мире использовала радио для управления сухопутными войсками непосредственно на театре военных действий, но и выработала способы организации радиосвязи, не утратившие значения и до настоящего времени.

Непосредственное участие в организации стратегической связи в русско-японской войне принял и фельдъегерский

корпус, который с началом военных действий повелением Николая II был приведен в «усиленный вариант». Фельдъегеря, откомандированные на Дальний Восток (около 35% штатного состава), не только обеспечивали доставку приказаний и распоряжений командующих в пределах действующей армии, но и доставляли в столицу наиболее срочные и важные донесения, адресованные непосредственно императору.

Приведем примеры российских шифров времен русско-японской войны. Русский словарный ключ №349 введен в действие в 1868 г. на линиях связи министерства финансов для телеграфной шифрпереписки. Изъят из употребления в 1879 г. вследствие утраты двух экземпляров. В 1901 г. вновь введен в действие для сношений министерства финансов с таможнями. Кроме того, этот шифр был введен в действие в 1900 г. в министерстве государственных имуществ, в 1902 г. – в Порт-Артуре, Харбине, Мукдене; в 1904 г. он был направлен в действующую армию.

«Ключ военного министерства №7 1905 г.» – алфавитный трехзначный цифровой код на 900 словарных величин, размещенных на 18 таблицах. Использовался императором и высшим военным руководством.

К сожалению, в организации шифрсвязи в действующей армии имелись серьезные недостатки. Если донесения в осажденный Порт-Артур посылаемые с фельдъегерями шифровали, то по телеграфу информация довольно часто передавалась в открытом виде. При этом уже в 1904 г. японские спецслужбы, впервые в истории радиотехнической разведки, реализовали на практике схему дистанционного съема информации с телеграфного кабеля. В российской прессе лишь в 1915 г. прошло сообщение о том, что во время боевых действий в период Русско-японской войны были случаи перехвата телеграфных сообщений, которыми обменивалась Ставка главнокомандующего и войска. Во время войны проводной телеграф, особенно аппараты Юза, русское командование считало абсолютно надежными для передачи секретных телеграмм в незашифрованном виде.

Наиболее важным с точки зрения истории криптографии является то, что в Русско-японскую войну впервые в мире начала применятся радиоразведка (наблюдение за радиосетями противника, перехват и дешифрование вражеских радиограмм) и радиоэлектронная борьба (постановка помех для срыва радиосвязи противника). Приоритет в использовании этих новых видов боевых действий принадлежит российскому военно-морскому флоту. Фактически, русские моряки начали войну в новом измерении – радиоэфире. Первые радиостанции поступили на вооружение русского флота в мае 1900 г. Почти сразу же после изобретения радио морское министерство Российской Империи начало работу по его использованию для добывания информации о военно-морских силах (ВМС) вероятных противников, выяснения характера их боевой деятельности в открытом море, что было невозможно агентурными методами. Кроме, собственно, обеспечения связи выявились другие направления использования радиостанций: радиоразведка; перехват и последующее дешифрование радиограмм иностранных флотов и баз; создание в эфире радиопомех в целях подавления деятельности радиостанций противника в случае начала военных действий.

Начало активной деятельности в этих направлениях, также как и радиофикация флота, было положено вице-адмиралом Макаровым. После его вступления в должность 24 февраля 1904 г. были предприняты энергичные шаги по ведению радиоразведки. К марту 1904 г. организовано постоянное несение вахт радиоразведки, а 7 марта издан приказ №27, явившийся законодательной базой дальнейшего развития радиоразведки и радиомаскировки. Приведем выдержку из этого приказа: «Приемная часть телеграфа должна быть все время замкнута так, чтобы можно было следить за депешами, и если будет чувствоваться неприятельская депеша, то тотчас же доложить командиру и определить, по возможности, заслоняя приемный провод, приблизительное направление на неприятеля и доложить об этом. При определении направления можно пользоваться, поворачивая свое судно и заслоняя

своим рангоутом приемный провод, причем по отчетливости можно судить о направлении на неприятеля. Минным офицерам предлагается провести в этом направлении всякие полезные опыты». Следует отметить, что в этом же приказе впервые в мире был введен режим радиомолчания (без разрешения командира корабля или командующего флотилией запрещалось отправлять в эфир любые радиограммы). Из этого следует, что Макаров понимал, что вместе с ведением радиоразведки в отношении противника следует уделять внимание защите информации на собственных радиолиниях.

К сожалению, гибель адмирала 31 марта на броненосце «Петропавловск», подорвавшемся на японской мине, существенно замедлила воплощение этих планов в жизнь. Важно отметить, что при анализе обстоятельств потопления «Петропавловска» выяснилось: именно недостаточная работа радиоразведки, которая не смогла выявить факт постановки японцами мин на внешнем рейде Порт-Артура накануне рокового дня, и стала основной причиной трагедии.

Тем не менее, ведение радиоразведки продолжалось, и ее роль при вскрытии планов противника была весьма важной. Так, в начале апреля 1904 г. японское командование приняло решение о проведении очередной боевой операции под Порт-Артуром силами 12 кораблей. Уже 9 апреля морской походный штаб царского наместника на Дальнем Востоке адмирала Алексеева известил штаб крепости:

«Сегодня утром на эскадре были разобраны (дешифрованы – *авт.*) японские телеграммы по беспроволочному телеграфу, из которых можно предположить, что намечается новая атака...». Русское командование сразу же усилило бдительность. 15 апреля японцы, закончив необходимые приготовления, провели в акватории порта-крепости рекогносцировку с целью ознакомить капитанов кораблей с районом предстоящих действий. В эту же ночь радиотелеграфисты броненосца «Полтава» перехватили и дешифровали телеграмму противника, подтвердившую его планы, и операция, состоявшаяся в ночь на 20 апреля, закончилась для японцев неудачно.

Апрель 1904 г. отмечен ещё одним достижением российских моряков. 2 числа они впервые смогли нарушить радиосвязь противника. В результате помех, созданных радиостанциями эскадренного броненосца «Победа» и берегового радиопоста «Золотая гора», была сорвана корректировка по радио артиллерийского огня японских кораблей, обстреливавших гавань Порт-Артура. Контр-адмирал Ухтомский доложил адмиралу Алексееву: «Неприятелем выпущено более 60 снарядов большого калибра. Попаданий в суда не было». Таким образом, этот день следует считать днем рождения нового вида боевых действий – радиоэлектронной борьбы. Стало ясно, что если не обеспечена скрытность связи, то оказывается уязвимой ее надежность.

Опыт русско-японской войны показал, что в условиях боевой обстановки невозможно обеспечить устойчивое управление войсками без улучшения работы штабов за счет применения всего комплекса средств связи. Важнейшим средством связи в стратегическом и оперативном звеньях в этой войне стал телеграф. Традиционно использовался для организации документальной шифрованной связи фельдъегерский корпус. Полностью оправдали себя телефон и радиосвязь как средства управления вооруженными силами.

Русско-японская война, в числе прочего, продемонстрировала необходимость широкого использования общегосударственной связи для управления многочисленными армиями в военный период. На рубеже первых 2-х десятилетий XX в. в ряде городов России уже существовали крупные для того времени радиостанции.

Учитывая опыт русско-японской войны, в 1909–1914 гг. военное ведомство построило ряд мощных радиостанций на Дальнем Востоке, в Арктической зоне, стали сооружаться приемно-передающие радиоцентры на радиомагистрали Москва–Владивосток. Была создана сеть рейдовых радиостанций по побережью Балтийского моря. Кроме того, стала действовать линия радиотелеграфа на юге России, соединившая форт Александровский (ныне г. Махачкала) с центром.

Итак, можно сделать вывод, что боевое применение средств радиосвязи в 1904–1905 гг. ознаменовало собой появление нового вида боевого противоборства – радиовойны. Получение сведений о вероятном противнике с помощью радио значительно расширяло разведывательные возможности. Но для этого нужна была эффективная служба наблюдения. В проекте закона «Об императорском российском флоте» 1911 г. в 27-й статье так определено содержание и направление дальнейшего развития службы наблюдения и связи: «Побережье Балтийского, Черного морей и Тихого океана должны быть оборудованы сооружениями для наблюдения за прилегающим водным пространством и для связи с флотом соответствующим числом береговых наблюдательных постов и радиотелеграфных станций».

Радиоразведка получила развитие в последующие годы. Так, служба наблюдения и связи (СНИС) Балтийского флота объединила в себе функции связи и радиоразведки, с безусловным преобладанием последней. Ее первым руководителем стал капитан 1 ранга Андриан Непенин. Он развернул активную деятельность и уже к 1909 г. сформировал стройную систему наблюдения морского побережья Балтийского моря, состоявшую из трех линий: 1-я – агентура на неприятельской территории; 2-я – пункты дальнего наблюдения (морские 1-го класса); 3-я – пункты ближнего наблюдения (сухопутные 2-го класса).

Основной задачей береговых наблюдательных пунктов 1-го класса являлось слежение за действиями неприятельского флота и их оценка. Личный состав этих пунктов комплектовался из чинов морского ведомства. В задачу пунктов 2-го класса входило наблюдение за побережьем и отражение возможного десанта. Персонал для них набирался преимущественно из чинов местной пограничной стражи. Там, где отсутствовали пункты обоих типов, создавался негласный агентурный аппарат, находившийся на связи у местного руководства. При СНИС имелись отделы дешифрования, информации и шифрования. В дальнейшем она сосредоточила в своем ведении все средства разведки, приняв, таким образом, на себя функции разведотдела штаба Балтийского флота. В 1912 г. во время штурманских походов в южную часть Балтийского мо-

ря, где передачи радиостанций иностранных флотов прослушивались особенно хорошо, на нескольких русских кораблях была специально организована тренировка радиотелеграфистов по обнаружению и перехвату радиопереговоров береговых и корабельных станций вероятного противника. Все эти мероприятия положительно повлияли на ход боевых действий на Балтике во время Первой мировой войны, но это тема для отдельной статьи.

В заключение отметим, что внедрение различных новшеств в Российской Империи часто затруднялось из-за отсталости мышления некоторых государственных деятелей, а также бюрократическим аппаратом, преодолеть сопротивление которого было очень трудно. Для иллюстрации приведем один пример, не относящийся к истории криптографии. В войне 1904–1905 гг. японцы применяли взрывчатое вещество «шимоза», обладающее высоким поражающим эффектом. Российские армия и флот использовали более слабые взрывчатые вещества, хотя еще в 1890 г. Д.И. Менделеев обращал внимание морского министра на высокие боевые характеристики «шимозы». Несмотря на обращения русского ученого, производить новое взрывчатое вещество не стали, и применение «шимозы» японцами оказалось для русских очень неприятным сюрпризом.

Японцы же наоборот активно интересовались новинками в разных областях науки и техники. В конце XIX в. они создали целую систему промышленного шпионажа в Европе и Америке, в интересах японской промышленности за секретами охотились дипломаты, коммерсанты, туристы, студенты. Добыча промышленных секретов и технологий сделала Японию одной из крупнейших индустриальных держав мира. Среди украденных секретов, в частности были технологии производства бездымного пороха, торпед, высококачественных оптических линз, используемых в производстве фотоаппаратов и электрических прожекторов большой мощности, новейшие способы литья стали и многое другое.

Подобные проблемы и стали основной причиной тяжелого поражения России в русско-японской войне.

Список рекомендуемой литературы

1. Ваннах М. «Черная месса» на слова пророка Исайи // Компьютера. – 2004. – с. 44–47.
2. Востоков К. У истоков радиовойны // Независимое военное обозрение 14-20 июля, 2000, с. 7.
3. Дамасскин И.А. Сто великих операций спецслужб. – М., 2004.
4. Крамар В. Энциклопедия радиоэлектронной борьбы на море // Независимое военное обозрение.– 2004. – №21. – с. 8.
5. Крамар В. Контрразведчик эпохи войн и революций // Независимое военное обозрение. – 2004.– №41, с. 7.
6. Куропаткин А. «Полагалось бы учредить…» // Сборник «Разведчики и шпионы»». – М.: Издательский дом «XXI ВЕК – СОГЛАСИЕ», 2000. – с. 19–24.
7. Лебедев В. Разведка виновна менее всех // Независимое военное обозрение. – 2001. – №42. – с.7.
8. Лебедев В. В ногу с прогрессом // Независимое военное обозрение. – 2002. – №1.– с.7.
9. Мерзляков В. Русская контрразведка: на заре в. тотального шпионажа // Сборник «Легион «Белой смерти»». – М., 2002. – с. 3–25.
10. Разведдаты марта // Независимое военное обозрение. – 2004. – №7. – с. 7.
11. Разведдаты апреля // Независимое военное обозрение. – 2003. – №11. – с. 7.

Глава 7.

Криптография в годы гражданской войны

После Октябрьской революции 1917 г. судьба России круто изменилась. Необходимость организации новой системы государственного управления потребовала коренной перестройки всех государственных служб и институтов. Не составила исключения и криптографическая служба России, которая в молодой Советской республике создавалась, фактически, заново. Необходимость организации службы, которая осуществляла бы централизованное управление шифровально-дешифровальным делом, стала очевидной для руководителей государства в годы Гражданской войны. Опыт Гражданской и Первой мировой войн красноречиво свидетельствовал, что умение держать в тайне информацию о себе и получать информацию о противнике является одним из важнейших факторов победы. В данной главе будут рассмотрены основные этапы развития связи в молодом советском государстве в период Гражданской войны и описано противостояние обеих сторон конфликта – красных и белых – в области шифрования, радиоперехвата и дешифрования.

Рассмотрим сначала *особенности организации связи и криптографическую деятельность в белых армиях*. Белые армии унаследовали от царской армии шифровальные и радиотехнические средства. Кадры опытных специалистов криптографической службы царской России, в основном, оказались на стороне белых.

Организации радиосвязи у белогвардейцев уделялось серьезное внимание. Радиосвязь поддерживалась между армиями А.В. Колчака, Н.Н. Юденича, А.И. Деникина и внутри армий для управления войсками. Белые применяли радиосвязь и для переговоров со своими представителями за рубежом. Для обеспечения радиосвязи использовались многочисленные во-

енные и гражданские радиостанции бывшей Российской Империи, среди которых имелись и довольно мощные. Приобретались радиостанции и за рубежом. Так, во Владивостоке действовала радиостанция, переданная американцами, а в Омске работала станция французского производства. Для управления войсками использовались стационарные и полевые радиостанции. Последними были снабжены армии, корпуса, дивизии, конные отряды, военные корабли.

Передаваемые по радио сообщения в обязательном порядке шифровались. Краткие сообщения шифровались целиком. В длинных сообщениях иногда шифровались лишь отрывки, содержащие важные сведения. Такое «частичное» шифрование отрицательно сказывалось на стойкости.

При передаче сообщений часто возникали помехи, которые не позволяли адресатам расшифровать получаемые ими телеграммы. Помехи появлялись при передаче сообщений на большие расстояния из-за сравнительно малой мощности основного количества радиостанций, а также из-за невысокой квалификации шифровальщиков, которые нередко допускали ошибки. Это приводило к необходимости повторной передачи радиограмм. Типичными для 1919–1920 гг. являются телеграммы о том, что какие-то слова или целые телеграммы не поддаются расшифрованию. Помимо радиосвязи широко использовалась отправка сообщений с курьерами, для доставки шифрованных сообщений применялась авиация. Так, в декабре 1918 г. представитель Всевеликого Войска Донского[1] в Украинской Державе[2] генерал Александр Черячукин

[1] Всевеликое Войско Донское – независимая республика, провозглашенная на Дону, восставшими против Советской власти казаками. Это образование поддерживало связи с другими частями Белого движения и воевало против красных, впоследствии Дон должен был войти в состав единой белой России. Главой этого государства (Атаманом) стал генерал-майор Петр Краснов.

[2] Государственное образование на Украине, возглавляемое гетманом П. Скоропадским. Гетман сотрудничал с представителями Белого движения.

направил из Киева, к тому времени занятого воевавшими с белыми войсками Украинской директории (петлюровцами), на Дон два самолета под управлением капитана Гринева и поручика Башкатова. Они доставили атаману шифрованный отчет о положении на Украине, составленный Черячукиным.

Благодаря тому, что большая часть шифровальщиков и криптографов царской России перешла на сторону белых, шифровальное дело в белых армиях было на более высоком уровне, чем в Красной Армии. Министерство иностранных дел колчаковского правительства включало цифирное отделение, сохранившее свое название, традиции, техническую базу царской шифровальной службы.

Белые широко использовали шифры и коды, разработанные еще до революции. Вместе с тем они создавали и новые шифры. Так, 2 февраля 1919 г. управляющий цифирным отделением писал, обращаясь к начальству: «…ввиду скомпрометированности старых ключей Министерства иностранных дел, цифирное отделение приступило к составлению новых секретных ключей для телеграфных сношений заграничных представителей с центральными установлениями министерства и между собой» [Соболева, 2002]. В феврале 1919 г. цифирным отделением Министерства иностранных дел были изготовлены два «перешифровальных ключа» (№560 и №570), введение которых в действие, по мнению изготовителей, «вполне обеспечивало бы сохранение тайны секретной корреспонденции министерства» [Соболева, 2002]. В июле 1919 г. цифирным отделением была завершена работа над изданием нового «секретного ключа» (кода), объемом 8000 словарных величин, а вскоре еще одного – новой буквенно-слоговой таблицы.

Ключевая документация печаталась в типографии военной газеты «Русская армия», где соблюдались соответствующие условия для сохранения тайны издания. Денег не хватало, поэтому типография определяла сметную стоимость издания. Эти данные сообщались типографией в цифирное отделение, и его управляющий составлял прошение об отпуске денег.

Для шифрования сообщений белогвардейцы использовали буквенно-слоговые разнозначные таблицы замены. Срок действия таких шифров определялся в полгода. Как известно, их криптографическая стойкость невелика. Такие шифры раскрываются на материале в несколько десятков знаков. Кроме того, в белых армиях использовались коды объемом в несколько тысяч словарных величин. Коды были в основном алфавитные, редко использовались неалфавитные небольшого объема, в которых имелось некоторое количество пустышек. Даже при соблюдении всех правил использования такие коды не обладают высокой стойкостью и могут раскрываться на материале достаточного объема. При организации регулярного перехвата их раскрытие становилось сравнительно простой задачей. Дешифрование облегчалось еще и тем, что часто шифровалась не вся телеграмма целиком, а только отдельные ее куски, хотя еще в период Первой мировой войны это было категорически запрещено. В качестве агентурных шифров белые использовали шифры перестановки, а именно, лозунговые шифры вертикальной перестановки.

Определить виды использовавшихся шифров в значительной степени помогают ошибки в ведении секретного делопроизводства. В начальный период войны ошибки в работе с шифрдокументами белыми почти не допускались. Однако по мере ухудшения военной обстановки, допускалась все большая небрежность.

В руках белогвардейцев оказалась значительная часть средств радиоперехвата. В белых армиях существовали специальные подразделения радиоразведки, которые перехватывали радиограммы, анализировали их, составляли ежедневные сводки и строили схемы радиосвязи советских военных частей. В частности, активную радиоразведку вели Западная и Уральская армии Колчака. Большое количество радиостанций действовало в районах Уфы, Уральска, в Астрахани, Гурьеве, Красноводске и Баку. Против организованного в августе 1919 г. Туркестанского фронта под командованием М.В. Фрунзе велась радиоразведка в Гурьеве, форте Александровском. Пере-

хваченные сообщения красных легко дешифровывались. Например, генерал-майор Дентервиль, командовавший экспедиционными войсками Антанты в Персии и Баку в 1918 г., в своих воспоминаниях писал, что благодаря использованию красными на Каспийском море старого царского кода, копия которого имелась в его штабе, английским войскам удалось получить важную информацию о действиях Красной Армии. Эта информация существенно повлияла на ход боевых действий и позволила англичанам занять Баку и другие районы Кавказа. Известно, что в период с 1918 по 1920 гг. почти все шифровальные сообщения РККА и советской дипломатии успешно читались белогвардейцами, поляками, англичанами, шведами. На деятельности англичан и поляков остановимся подробнее.

В ноябре 1919 г. в Англии была создана государственная служба радиоразведки и криптоанализа – правительственная школа кодов и шифров (ПШКШ), позднее переименованная в штаб-квартиру правительственной связи (ШКПС).

До революции 1917 г. в дешифровальной службе России работал Эрнст Феттерлейн. Среди его заслуг было дешифрование британской дипломатической почты. По иронии судьбы после революции он сбежал в Англию и возглавил там русскую секцию английской дешифровальной службы. За первые 10 лет после революции его главным достижением стало дешифрование русской дипломатической почты, на этот раз для англичан. О деятельности Феттерлейна мы более подробно расскажем в гл. 10.

В начале 1920-х гг. англичане регулярно дешифровали советскую дипломатическую переписку. Они использовали дешифрованные телеграммы в политических целях. В частности, они серьезно повредили проводимой в Китае советской политике. Англичане пошли на опубликование дешифрованных сообщений с целью дискредитировать СССР и продемонстрировать коварство его замыслов. Министр иностранных дел Великобритании и министр внутренних дел в своих выступлениях цитировали указанные документы. В России имелись серьезные подозрения, что используемые шифры не являются

Нарком иностранных дел Г.В. Чичерин

стойкими. Вот выдержка из докладной записки наркома иностранных дел Георгия Чичерина

В. И. Ленину от 20 августа 1920 г.: «Иностранные правительства имеют более сложные шифры, чем употребляемые нами. Если ключ мы постоянно меняем, то сама система известна многим царским чиновникам и военным, в настоящее время находящимся за границей. Поэтому чтение наших шифровок я считаю вполне допустимым» [Лайнер, 2004]. Однако имелось мнение, что возможное чтение наших шифртелеграмм связано не со слабостью шифров, а с агентурной утечкой информации. Вот что об этом пишет Ленину тогдашний полномочный представитель Советской России в Англии Леонид Красин 10 сентября 1920 г.: «Владимир Ильич! Еще в мае в бытность в Копенгагене по некоторым признакам я начал подозревать, что с шифрованной перепиской через Наркоминдел не все обстоит благополучно. В Англии мои подозрения укрепились, и в последующий мой приезд в Москву я обращал внимание тов. Чичерина на необходимость коренной чистки в соответствующем отделе… Дело не в провале шифра или ключа, а в том, что в Наркоминделе неблагополучие, так сказать, абсолютное, и лечить его надо радикально» [Соболева, 2002].

Ленин соглашается с Красиным и 25 ноября того же года направляет Чичерину следующее указание: «Тов. Чичерин! Вопросу о более строгом контроле за шифрами (и внешним и внутренним) нельзя давать заснуть. Обязательно черкните мне, когда все меры будут приняты. Необходима еще одна: с

каждым важным послом (Красин, Литвинов, Шейман, Йоффе и др.) установить особо строгий шифр для личной расшифровки, т.е. здесь будет шифровать особо надежный товарищ, коммунист (может быть, лучше при ЦК), а там должен шифровать или расшифровывать лично посол (или «агент»), не имея права давать секретарям или шифровальщикам. Это обязательно (для особо важных сообщений, 1–2 раза в месяц по 2–3 строки, не больше). Ваш Ленин» [Соболева, 2002].

Несмотря на то, что определенные меры по безопасности связи принимались, англичанам удавалось читать большую часть советской дипломатической переписки. Ущерб СССР был нанесен заметный. Были разорваны дипломатические отношения между СССР и Великобританией, дипломатические шифры СССР снова пришлось заменить.

В мае 1927 г. англичане предприняли силовую акцию по захвату документов советско-английского торгового общества «Аркос» в Лондоне. Среди захваченных секретных документов оказались и советские шифры. Эта находка дала англичанам возможность читать шифрпереписку советских дипломатов в Англии, в частности англичанам удалось «расколоть» шифр, которым пользовалось советское посольство в Лондоне. Кстати, после этого Советский Союз ввел систему зашифровки телеграфной переписки с помощью одноразовых гамм-блокнотов и успехи англичан закончились.

Польская военная криптографическая служба, которая получила название «Секция Шифров», была создана 8 мая 1919 г. лейтенантом Йозефом Станслинским (Józef Stanslicki), спустя несколько месяцев она получила название «Бюро Шифров». Практически сразу польские криптоаналитики приступили к вскрытию советских военных шифров. С самого начала 1919 г. поляки вели боевые действия против Красной армии в целях захвата территорий в Белоруссии и Литве. Вскоре молодым математиком Стефаном Мазуркевичем (Stefan Mazurkiewicz), который позже стал вице – ректором Варшавского университета, был вскрыт наиболее часто используемый противостоящими полякам частями Красной армии

шифр. В результате польское военное командование получало важную информацию, которая помогала успешному ведению боевых действий. Информация криптоаналитиков поступала во 2-й (разведывательный) отдел польского Генерального штаба, возглавляемый полковником Тадеушем Шаецелем (Tadeusz Schaetzel), а оттуда поступала к командованию армией и руководителям польского государства, включая Юзефа Пилсудского. Шаецель активно помогал криптоаналитикам в их работе, так при его содействии на варшавском радио был организован пункт радиоперехвата под кодовым названием «Война». Здесь был установлен один из двух, имеющихся на тот момент в Польше радиоприемников дальнего действия.

Наиболее активные боевые действия на Советско-польском фронте имели место весной-летом 1920 г. Несмотря на определенные успехи поляков, Красная армия перешла в решительное наступление и нанесла польским войскам ряд тяжелых поражений. В июле 1920 г. советские войска вышли к Варшаве и готовились к штурму польской столицы. Однако 16 августа поляки нанесли контрудар, в результате которого советские войска понесли тяжелые потери и вынуждены были отступить. В достижении этого успеха немалую роль сыграли польские криптоаналитики. О напряженности их работы говорит следующий факт, только за август 1920 г. они дешифровали 410 секретных телеграмм, подписанных наркомвоенмором РСФСР Л.Д. Троцким, а также советскими военачальниками Тухачевским, Гаем и Якиром. В частности польские криптографы обнаружили разрыв между частями Красной армии на левом фланге фронта, именно туда и был нанесен главный удар. Так же было установлено, что войска 4-й советской армии потеряли контакт со своим штабом, в результате чего продолжали продвигаться в Восточную Пруссию, где 50 тыс. человек были интернированы до конца войны. Во время наступления Красной Армии на Варшаву поляки, используя свои успехи в дешифровании советских сообщений, организовали ложный узел связи; с его помощью удалось заставить армию Тухачевского отступить к Житомиру. Таким образом,

польские дешифровальщики внесли существенный вклад в разгром советских войск под Варшавой.

Белые и иностранные противники советской России тщательно следили за военной и дипломатической деятельностью красных. Так, перехватывалась и дешифровывалась переписка советского правительства с делегацией на переговорах в Брест-Литовске. Тщательно отбиралась и анализировалась информация о деятельности ВЧК. Благодаря радиоперехвату и дешифрованию, руководители белого движения контролировали планировавшиеся Красной Армией операции на Восточном и Туркестанском фронтах, следили за связью командования этих фронтов с Москвой. Весной 1919 г. адмирал Колчак писал русскому посланнику в Греции: «Единственным источником информации нам служат перехваченные большевистские радио» [Соблева, 2002]. Системы шифрования, применяемые войсками Буденного и Куйбышева в Средней Азии, иногда «раскалывались» даже басмачами. Слабая профессиональная подготовка кадровых работников шифрслужбы красных не могла обеспечить должного уровня защиты передаваемой информации. Допускалось множество нарушений, послаблений при шифровании. Также как и белые, для экономии времени красные зачастую шифровали только отдельные участки сообщения текста, а остальная его часть передавалась открыто.

Немалый урон советской шифрслужбе нанесли потери, хищения и многочисленные случаи предательства со стороны шифровальщиков Красной Армии. Например, в 1919 г. в руки противника попало 23 экземпляра шифров, в 1920 г. – 30 экземпляров.

В 1919 г. в самолете, летевшем из Германии в Россию и совершившем аварийную посадку в Латвии, местные пограничники обнаружили три шифрованных сообщения. Не сумев их дешифровать, правительство Латвии передало эти сообщения американскому консулу в Риге, который, в свою очередь, переправил их в США. Там они были довольно быстро прочитаны. К дешифрованию был привлечен знаменитый американский криптограф Герберт Ярдли, успешно вскры-

вавший многие немецкие шифры во время Первой мировой войны. Оказалось, что сообщения послали в Москву немецкие коммунисты, которые применили для их засекречивания шифр вертикальной перестановки, а в качестве ключа использовали строки из стихотворения «Лорелея» Генриха Гейне. В шифровках содержалась просьба прислать побольше денег, обсуждался провал съезда коммунистов в Голландии и говорилось об аресте известной немецкой коммунистки Клары Цеткин. Сам Ярдли в своей книге [Yardley, 1931] утверждает, что были также захвачены послания руководителя одной из советских разведывательных сетей в Западной Европе. Среди них оказался весьма любопытный документ под названием «Инструкция агентам, вербующим шпионов в дипломатических миссиях». Перевод этой инструкции на английский язык Ярдли приводит в своей книге. Также по воспоминаниям Ярдли в том же года шифр вертикальной перестановки использовался для связи во время венгерской революции между В.И. Лениным и видным венгерским коммунистом Б. Куном. Их сообщения также были перехвачены и дешифрованы американцами.

Теперь рассмотрим *криптографическую деятельность молодой советской республики*. Руководители большевиков, в том числе и В.И. Ленин, уделяли особое внимание организации и обеспечению безопасности связи. С криптографией многие из них познакомились еще в ходе подпольной работы. Большую работу по организации связи большевики провели накануне Октябрьского вооруженного восстания. Для руководства вооруженным восстанием Петроградский Совет рабочих и крестьянских депутатов образовал Военно-революционный комитет (ВРК) под председательством Н.И. Подвойского. К 22 октября 1917 г. была создана надежная система управления вооруженными отрядами, имевшимися в распоряжении большевиков. С началом восстания утром 25 октября (7 ноября по новому стилю) большевики овладели центральной телеграфной станцией. Средства телефонной связи также оказались в руках ВРК. Телефоны Зимнего дворца, где находились члены Временного правительства, были отключены. В тот же день около

полудня был занят военно-морской порт с радиостанцией «Новая Голландия». Таким образом, в руках большевиков был сосредоточен практически все средства связи Петрограда. Кроме сетей проводной и радиосвязи большевики широко использовали курьерскую связь на автомобилях и мотоциклах. Столь разветвленная сеть связи ВРК во многом и предопределила победу Октябрьского вооруженного восстания.

В Москве ситуация развивалась похожим образом, захват учреждений связи был в числе первоочередных задач восставших. Московское восстание началось 26 октября (8 ноября) 1917 г. 29 октября (11 ноября) были взяты телеграф и почтамт. Интересно отметить следующий факт. Для связи между группами восставших большевики активно использовали будки стрелочников трамвайного управления, они были разбросаны по всей Москве и имели собственную проводную телефонную связь, с трамвайными депо и между собой. Этот канал связи сыграл существенную роль в управлении вооруженными отрядами в ходе восстания в древней столице России.

С победой восстания Петроградский совет стал главным исполнительным органом нового правительства. Изменилось и назначение средств связи. Они превратились из средств управления вооруженным восстанием в средства управления государственным аппаратом. Связь Смольного превратилась, по существу, в правительственную связь, так как она стала использоваться исключительно для обслуживания высших государственных органов власти. В систему этой связи вошли центральная телефонная станция Смольного, локальные станции, телеграф Смольного и Царскосельская радиостанция.

Председатель Совнаркома В.И. Ленин настаивал на том, чтобы правительственная связь действовала бесперебойно в любых ситуациях, была высокого качества и, самое главное, обеспечивала секретность переговоров. Для выполнения этих требований в основу организации связи были положены следующие принципы: обеспечение связи по проводам; специальный отбор обслуживающего персонала; установление строгого порядка пользования средствами связи; применение шифров и условных сигналов.

После переезда Советского правительства из Петрограда в Москву в Кремле была организована специальная телефонная сеть. Во время Гражданской войны она постоянно расширялась и совершенствовалась, став, фактически, первой сетью правительственной связи.

Так как основная часть специалистов-криптографов после революции перешла на сторону противников советской власти, то победившие вынуждены были применять шифры дореволюционной России, либо разработанные ранее подпольные шифры. И те, и другие шифры были хорошо известны криптографам царской России, работавшим на белых.

Те специалисты-криптографы, которые перешли на сторону советской власти, в большинстве своем оказались разбросанными по различным полевым штабам Красной Армии, возглавляя в них шифровальные группы. Однако в распоряжение Советской власти попали почти все шифрдокументы цифирных отделов царской России. Правда, эти документы были хорошо известны специалистам-криптографам, оказавшимся во вражеском лагере, и поэтому, хотя и стали активно применяться, не могли служить действенным средством защиты оперативной информации. К сожалению, красным досталось не все. Многие ценнейшие материалы Временного правительства России, архивов командующих вооруженными силами белых армий, включающие и документы тайной переписки и шифров, были вывезены из России. То же самое следует сказать об архиве, включающем документы царской охранки с 1895 по 1917 гг. Они были переданы бывшим русским послом в Париже известному американскому разведчику и промышленнику Герберту Гуверу. В настоящее время все эти документы и архивы находятся в Гуверовском институте войны, революции и мира при Стэнфордском университете в Калифонии. Кстати сказать, ведущим экспертом этого института по «русскому вопросу» вплоть до самой своей смерти был А.Ф. Керенский.

Во время Гражданской войны в советской республике активно развивалась военная связь. Был проведен ряд мер с целью обеспечения централизованного руководства военной

связью и четкого взаимодействия органов военной связи с учреждениями Народного Комиссариата почт и телеграфов (Наркомпочтеля, НКПиТ). В мае 1918 г. в состав НКТиП был введен отдел военной и военно-морской связи.

В сентябре 1918 г. для улучшения руководства военной связью была введена должность Чрезвычайного комиссара почт и телеграфов при главнокомандующем Вооруженными силами республики. В это же время при штабах фронтов были созданы почтово-телеграфные отделы Наркомпочтеля, которые отвечали за обеспечение связи главкома, штабов фронтов и армий. Военной связью в высшем звене занимались Центральное управление военных сообщений, НКПиТ и главное военно-инженерное управление.

В ноябре 1918 г. Советом Народных Комиссаров был утвержден высший орган по руководству связью в стране – Верховная комиссия телеграфной связи (Верхкомтель). В 1918 г. активно создавались радиомагистрали, которые связали Москву с крупнейшими административными центрами республики, а также со столицами Франции, Германии и Турции.

20 ноября 1919 г. был издан приказ РВСР о создании Управления связи Красной Армии. На фронтах были сформированы управления связи фронтов, в армиях и дивизиях – отделы связи. Введены должности начальников связи фронта и армии. Этот день считается датой создания войск связи РККА как самостоятельных войск.

К концу 1919 г. в телефонной комнате Кремля появились телефонные аппараты прямой связи с фронтами. В феврале 1920 г. сформирован специальный отряд связи штаба Красной Армии, а в мае того же г. – радиотелеграфный дивизион для обеспечения связи в высшем звене руководства фронтами и армиями.

Фельдъегерская связь оставалась самостоятельной службой, которая была представлена соответствующими органами при главном штабе Красной Армии и полевом штабе РВСР, а 23 ноября 1920 г. по приказу РВСР создан фельдъегерский корпус при Управлении связи Красной Армии. К концу 1920 г.

для управления фронтами, армиями и укрепленными районами имелись: «один специальный поезд связи, 13 отдельных батальонов связи, 18 отдельных телеграфно-телефонных дивизионов, 40 телеграфно-эксплуатационных рот, 75 телеграфно-телефонных рот, 13 отдельных рот связи, 3 радиобазы, 16 отдельных радиодивизионов, 38 отдельных радиостанций, 8 рот летучей почты, 21 склад связи, 25 мастерских связи, 26 дислокаторных почтовых отделений» [Астрахан, 1996].

Для организации связи активно использовалась авиация, особенно это было актуально на окраинах бывшей Российской Империи. Так в начале 1920-х гг. в Туркестане, где Красная Армия вела бои с басмачами, имелась всего одна телеграфная линия, проходившая вдоль единственной железной дороги. Шоссейные дороги с твердым покрытием вовсе отсутствовали, а радиосвязь в условиях гор работала плохо. Поначалу для доставки донесений использовали курьеров из местных жителей, однако надежность и оперативность такой связи была чрезвычайно низкой. Использование самолетов для доставки сообщений резко повысило надежность и оперативность связи, что позволило советскому командованию гораздо более эффективно осуществлять руководство операциями Красной Армии против басмачей.

С образованием в апреле 1920 г. Дальневосточной республики[1] возникла необходимость организации шифрованной связи с советской Россией. Эту задачу успешно решил Меер Абрамович Триллесер, он создал «первую на советском Дальнем Востоке специальную шифровальную службу для связи с Москвой» [Антонов, 2008]. С 1922 по 1929 гг. М. Триллесер был руководителем советской внешней разведки, под его руководством было проведено множество успешных операций, в том числе по добыче криптографических секретов иностранных государств и белоэмигрантских организаций.

[1] Дальневосточная республика являлась «буферным» государством между Советской Россией и Японией, существовала в период 6.04.1920–15.11.1922, после разгрома белогвардейцев и японских интервентов вошла в состав РСФСР.

Меер Абрамович Триллесер

Несмотря на значительное преимущество радиосвязи по сравнению с проводными средствами связи, для которых были необходимы постоянные воздушные линии большой протяженности, почти вся связь высшего военного руководства того времени базировалась на использовании воздушных линий связи и отдельных проводов. Частичный отказ от радиосвязи был обусловлен тем, что красным стало известно об успехах белогвардейских служб радиоперехвата и дешифрования. Именно поэтому в высшем звене руководства Красной Армией применялась в основном проводная связь. Такая связь штаба РВСР со штабами фронтов и армий осуществлялась по отдельным проводам через полевые телеграфные конторы, как правило, с использованием аппаратов Бодо, Юза и Уитстона. Телефонная связь применялась на небольшие расстояния, в основном, в оперативном звене.

Теперь рассмотрим шифры применявшиеся на линиях связи молодой советской республики. В основном применялись шифры простой и пропорциональной замены. В период борьбы с Врангелем советской стороной применялся шифр «Республика», представлявший собой шифр Виженера с чередованием букв алфавита внутри квадрата в соответствии с ключом-лозунгом. Применялись не менее широко известные шифры «Москва» и «Секунда». Шифр «Москва» также представлял собой шифр Виженера, где в качестве лозунга использовался тот же открытый текст, но сдвинутый на один шаг вправо, иначе расшифрование было бы невозможно. При этом первая буква лозунга была заранее оговоренной и менялась в соответствии с расписанием. Шифр «Секунда» был

обычным шифром замены на 9, 2, 13 колонок. В 1919–1920 гг. были разработаны и применялись более стойкие шифры: «Пулемет», «Агитатор», «Советский» и другие лишь незначительно улучшили неблагоприятную в целом ситуацию с обеспечением тайны шифропереписки в Советской республике.

Крайне плохо обстояло дело с дешифрованием иностранной и военной переписки. В Красной Армии не было организованной дешифровальной службы, так как созданные при штабах шифргруппы имели главной задачей создание шифров и защиту ими секретной переписки. Можно сказать, что дешифровальная служба практически отсутствовала. В тот период советская сторона не располагала силами и средствами для успешного проведения такой работы. Советская сторона испытывала острый дефицит в радиоперехватывающих средствах и их оснастке, хотя войсковые соединения и перехватывали радиопереговоры, ведущиеся по линиям связи фронтовых и дивизионных соединений белых армий.

Однако и советские радиоразведчики и криптоаналитики добивались успехов. В конце 1917 г. был обнаружен архив посольства Англии. В нем оказались действующие английские шифры. В результате был дешифрован ряд телеграмм английского посла в России Бьюкенена, а затем и сменившего его дипломатического агента Англии Локкарта. Это помогло ВЧК раскрыть заговор последнего, направленный против большевиков. В этом заговоре участвовали послы ряда западных стран. Его была организация восстания в Москве и физическое устранение руководства молодой советской республики. Среди задержанных по делу Локкарта оказался представитель ряда американских фирм в России Каламатиано. У него при обыске в полой трости был обнаружен шифр, которым пользовались заговорщики, архив заговорщиков и списки участников заговора. В дальнейшем Каламатиано продолжил свою шпионскую деятельность против советской России. При аресте в 1918 г. у него была обнаружена инструкция, в которой указывалось, что в сообщении следует зашифровывать особо важные сведения следующим образом: номера войск обозна-

чаются как количество пудов сахара и патоки, а также цена на них. Дух войск – положение в сахарной промышленности. Номера артиллерийских частей – мануфактура и цены на нее. Дезертирство из Красной Армии – эмиграция из Украины.

Интересно отметить, что все подробности раскрытия заговора Локкарта стали известны белогвардейцам из перехваченных и дешифрованных советских радиопередач.

Таким же образом был обнаружен шифр румынского военного атташе. В результате был раскрыт план Корнилова о сдаче Риги немцам и получены другие важные материалы.

В период Первой мировой войны на Балтийском флоте в составе службы наблюдения и связи была создана достаточно сильная и эффективная радиоразведывательная сеть. Она включала в себя центральную станцию радиоперехвата, 10 периферийных станций радиоперехвата и 10 радиопеленгаторных станций. 18 февраля 1918 г. немецкие войска начали наступление на Петроград, оккупировав Эстонию и Латвию. Личный состав станций отходил вместе с войсками к Ревелю (ныне Таллинн, Эстония). По мере продвижения войск противника на восток российские моряки вынуждены были свернуть западный и северозападный районы СНиС флота. В соответствии с указанием советского правительства в целях спасения кораблей Балтийского флота 12 марта 1918 г. начался знаменитый ледовый переход кораблей из Гельсингфорса в Кронштадт. После этого перехода, стоившего больших потерь, службы наблюдения и связи, а вместе с ними и радиоразведка флота, прекратили свое существование. Однако уже осенью 1918 г. Реввоенсовет Республики принял решение о создании четырех районов связи Балтийского флота: Кронштадского, Петроградского, Шлиссельбургского и Онежского.

Функции этих районов были несколько сокращены. Шифрование передано специальному шифровальному отделению, радиоперехватом занималась только радиостанция «Новая Голландия», откуда все сведения поступали непосредственно в штаб Красной Армии или в Смольный. Также посты радиоразведки на некоторых кораблях эпизодически вели пе-

рехват радиограмм противника. Таким образом, в период Гражданской войны и иностранной военной интервенции радиоразведывательная деятельность на Балтике велась не очень активно. Тем не менее, 2 декабря 1918 г. был достигнут крупный успех, красные радиоразведчики зафиксировали факт прибытия английской эскадры в Ревель. В этот день была перехвачена и дешифрована английская радиограмма из Ревеля, в которой сообщалось: «Командующему союзным флотом в Балтике. Наши летчики будут встречать Вас у Сурупа и Оденсхольма» [Боечин, 2006]. В последствии были перехвачены и дешифрованы еще несколько английских сообщений, из которых удалось определить, что на Балтику прибыло не менее 9 английских кораблей. Эти данные были подтверждены агентурной разведкой. Информация была немедленно передана в Москву. К сожалению, эти сведения не были оценены командованием Балтийского флота, которое организовало набег на Ревель, в результате столкновения с превосходящими силами англичан было потеряно два эсминца. Однако опыт радиоразведывательной деятельности Балтийского флота был успешно использован на других фронтах Гражданской войны. При обработке материалов, полученных радиоразведкой, использовался криптоанализ, так как значительная часть передаваемой информации шифровалась.

Весьма активно велась радиоразведка на Волжско-Каспийской военной флотилии красных. Эпизодический перехват радиограмм противника велся радистами флотилии, которая начала создаваться с весны 1918 г. из отдельных разрозненных отрядов вооруженных буксирных пароходов и барж, где команды состояли преимущественно из моряков Балтийского флота. Во второй половине октября 1918 г. связисты флотилии перехватили несколько радиограмм противника об обстановке в районе населенного пункта Гальяны на Каме. Это дало возможность командованию флотилии успешно организовать поход на Гальяны в целях освобождения пленных красноармейцев, увезенных белыми на барже при отступлении из Сарапула. Большую роль сыграла радиоразведка после выхода флотилии в

Каспийское море. Как на восточном, так и на западном побережье Каспия практически отсутствовала проводная связь, и радиосвязь имела первостепенное значение. Поэтому между белогвардейцами и силами Волжско-Каспийской флотилии развернулась настоящая война за захват и уничтожение радиостанций и добывание шифрматериалов.

Захваченные радиостанции применялись для дезинформации противника. Одной из важнейших задач во время боевых походов кораблей флотилии было уничтожение береговых радиостанций противника. Так, 30 декабря 1918 г. начальник штаба Волжско-Каспийской флотилии Н. Третьяков доложил в штаб Каспийско-Кавказского фронта, что во время похода флотилии 9–12 ноября 1918 г. к Брянской косе и набега на бухту Староречную был произведен обстрел радиостанции белых. Окончательно ее уничтожили 14 ноября 1918 г.

Яркой страницей в историю советской радиоразведки вошел случай захвата радиостанции форта Александровский и использования ее в радиоигре с белогвардейцами. 30 декабря 1919 г. отряд кораблей флотилии подошел к полуострову Мангышлак и внезапным ударом после высадки десанта захватил форт Александровский.

Долгое время белогвардейцы не знали о захвате форта и продолжали передавать через транзитную радиостанцию радиограммы, поступавшие из штабов армии Деникина, из Баку, Красноводска для передачи колчаковцам в Гурьев. Радист с эсминца «Карл Либкхнехт» Н. Чемруков, работавший на радиостанции форта, принял 5 мая 1919 г. радиограмму о переходе из Петровска в Гурьев парового судна «Лейла» с военной миссией А. Деникина во главе с генералом А. Гришиным-Алмазовым. Радиотелеграфист К. Ровков перехватил переговоры между «Лейлой» и английским вспомогательным крейсером «Президент Крюгер». Вскоре после того, как крейсер разошелся с «Лейлой», белогвардейский пароход было захвачено красным эсминцем «Карл Либкхнехт». Генерал и его адъютант застрелились, а сопровождавшие генерала штабные офицеры попали в плен. Среди 29 пленных были английский

и французский военные советники белогвардейцев. В числе захваченных ценных документов были план совместного похода Деникина и Колчака на Москву, их личная переписка и многое другое.

Через радиостанцию форта Александровский проводилась активная дезинформация белых. Все белогвардейские радиограммы немедленно передавались в штаб 11-й армии. Там в них вносились необходимые изменения, чтобы максимально запутать управление войсками противника, после чего радисты передавали их адресатам. Радиоперехватом занимались не только береговые, но и корабельные радиостанции. 5 апреля 1920 г. радисты уже упоминавшегося эсминца «Карл Либкнехт» перехватили радиограмму, предписывающую генералу Толстову со штабом погрузить золото и серебро на корабль и ждать дальнейших приказаний. В штабе на основе добытых ранее данных был сделан вывод о подготовке белыми перехода в иранский порт Энзели. Вышедший к расположению белогвардейских частей эсминец «Карл Либкнехт» после успешного боя с двумя белогвардейскими вспомогательными крейсерами «Милютин» и «Опыт», подойдя к кораблю противника, предложил ему немедленно сдаться. Вскоре в Астрахань была передана радиограмма с эсминца: «Захватили в плен 2 генералов, 77 офицеров и 1088 казаков. Взяли 90 пудов серебра и другие трофеи» [Востоков, 2000].

С января 1919 г. в Красной Армии и на флотах началось формирование пеленгаторных и приемно-информационных радиостанций – первых подразделений фронтовой радиоразведки, на которые возлагалась также задача по контролю над своими радиостанциями. В ноябре 1919 г. радиоразведкой Красной Армии был раскрыт факт поставки военного имущества и продовольствия для уральской белой армии на судах «Астрахань», «Азия», «Европа», «Слава» и «Президент Крюгер», входивших в состав Каспийской флотилии белых. В сентябре 1919 г. для разгрома войск Деникина был создан Юго-Восточный фронт. Радиоразведку в его интересах стали вести приемно-информационные радиостанции и связные радио-

станции армии. Эти станции осуществляли слежение за полевыми радиостанциями противника в районе боевых действий уральской и деникинской армий, а также за судовыми радиостанциями на Каспийском море.

В начале 1920 г. на Черноморском флоте принято решение о формировании службы наблюдения и связи, начальником которой был назначен С. Касаткин. Созданы Одесский, Очаковский, Херсонский и Мариупольский районы. Главное управление СНиС вначале имело в своем составе командование, оперативный отдел с дежурством по связи, четырьмя шифровальщиками и двумя переводчиками. Наличие переводчиков говорит о том, что посты занимались перехватом иностранного радиообмена.

Радиоразведка Юго-Западного фронта вела перехват сообщений радиостанции белых в Севастополе, отправлявшихся в Париж, Варшаву, Константинополь, Будапешт и Афины. В 1920 г. с ее помощью были обнаружены корабли интервентов на Черном море у берегов Крыма и подвоз на судах боеприпасов, продовольствия и снаряжения для войск Врангеля в Крыму, было установлено наличие радиосвязи между штабом Врангеля и странами Антанты. С началом наступления войск Южного фронта 28 октября 1920 г. с помощью радиоразведки была вскрыта передислокация штабов белогвардейцев, были добыты сведения о боевой деятельности войск, о движении боевых кораблей и транспортов противника. Осенью 1920 г. советским дешифровальщикам удалось прочитать переписку врангелевской контрразведки, из которой были получены важные сведения.

В 1920 г. при разгроме Врангелевской армии в Крыму был захвачен начальник станции радиоперехвата Ямченко. Он дал согласие сотрудничать с новой властью и рассказал о практически полном дешифровании белыми перехваченных сообщений. С этими сведениями был ознакомлен знаменитый советский военачальник М.В. Фрунзе. Вот какую оценку состояния дел в области криптографической защиты информации в молодой советской республике он дает: «…Из предос-

тавленного мне бывшим начальником врангелевской радиостанции Ямченко доклада устанавливается, что решительно все наши шифры вследствие их несложности читаются нашими врагами. Вся наша радиосвязь является великолепнейшим средством ориентирования противника. Благодаря тесной связи с шифровальным отделением морфлота Врангеля, Ямченко имел возможность лично читать целый ряд наших шифровок самого секретного военно-оперативного и дипломатического характера; в частности, секретнейшая переписка Наркоминдела с его представительством в Европе и в Ташкенте слово в слово известна англичанам, специально организовавших для подслушивания наших радио целую сеть станций особого назначения. К шифрам, не поддававшимся немедленному взлому, присылались ключи из Лондона, где во главе шифровального отдела поставлен англичанами русскоподданный Феттерлейн, ведавший прежде этим делом в России. Общий вывод такой, что все наши враги, в частности Англия, были постоянно в курсе всей нашей военно-оперативной и дипломатической работы…» [Соболева, 2002].

Иногда знание шифровального дела сильно помогало внедрению агента. Во время Гражданской войны в России в белую армию добровольно вступил П.В. Макаров, который на самом деле был агентом разведки красных. Чтобы проверить лояльность добровольцев, белые посылали всех вновь прибывших на передовую и только после реального активного участия в боевых действиях допускали к работе в штабах. Макаров неплохо знал шифровальное дело, о чем и сообщил белогвардейцам. Так как шифровальщиков не хватало, то в виде исключения он сразу был направлен в штаб Добровольческой армии. Карьера Макарова быстро продвигалась, и вскоре он стал личным адъютантом одного из руководителей Добровольческой армии генерал-лейтенанта В. Май-Маевского. Эта должность открывала Макарову доступ к самой секретной информации. К тому же, пользуясь своим служебным положением, Макаров устроил телеграфистом в штаб Добровольческой армии своего брата, что дало дополнительные возмож-

ности добывать полезную информацию. П. Макаров послужил прототипом главного героя известного кинофильма «Адъютант его превосходительства».

В январе 1921 г. В.И. Ленин был ознакомлен с некоторыми материалами о результатах работы радиоразведки в годы Первой мировой и Гражданской войн. Ленин отметил большую важность этой работы и поручил Реввоенсовету и ВЧК заняться организацией специальной радиоразведки. Как отмечалось ранее, еще будучи в подполье, В.И. Ленин уделял большое внимание шифровальному делу. Став руководителем советского государства, он продолжал уделять внимание защите информации криптографическими методами и вопросам добывания информации с помощью радиоразведки и криптоанализа. Ленин несколько раз лично давал рекомендации по совершенствованию системы пользования шифрами, повышению шифрдисциплины, излагал свое мнение о принципах построения шифровальной службы. Приведем цитату по этому поводу. В 1922 г. Ленин писал: «Сообщают об английском изобретении в области радиотелеграфии, передающем радиотелеграммы тайно. Если бы удалось купить это изобретение, то радиотелеграфная и радиотелефонная связь получила бы еще более громадное значение для военного дела» [Лекарев, 2004]. В Советской России началось критическое осмысление состояния безопасности отечественных линий связи и определение организационных форм будущей шифровальной службы страны. В начальный период этой деятельности руководители страны уделяли этой службе должное внимание. В результате был создан специальный отдел при ВЧК как единый центр криптографической службы страны. А еще в сентябре 1920 г. Политбюро рассмотрело предложение Ленина принять меры к усложнению шифров и к более строгой охране шифрованных сообщений. Политбюро постановило поручить наркому по военным и морским делам Л.Д. Троцкому организовать комиссию из представителей Наркомвоен, Наркоминдел, ЦК РКП(б) и Наркомпочтеля. В.И. Ленин, изучив досконально вопрос, зная мнение различных заинтересованных ведомств, поручает изыскать пути наведения порядка в шифровальном

деле руководству ВЧК, хотя шифровальные службы по традиции сохранялись и во внешнеполитическом ведомстве, и в военном наркомате. Возможно, на выбор базового ведомства по осуществлению криптографической деятельности в Советском государстве повлияла сложность обстановки, а также то обстоятельство, что главной функцией ВЧК уже в тот период было обеспечение государственной безопасности в целом. Именно на обеспечение государственной безопасности направлена и деятельность криптографической службы. Во второй декаде января 1921 г. Коллегия ВЧК принимает решение о созыве совещания представителей заинтересованных ведомств для подготовки соответствующих предложений по воссозданию криптографической службы. В обсуждении вопроса принимали участие представители ЦК РКП(б), ВЧК и наркоматов. 12 апреля на заседании Малого Совнаркома был заслушан проект создания специального отдела при ВЧК. В проекте говорилось о том, что «в республике отсутствует центр, объединяющий и направляющий деятельность шифровальных органов различных ведомств, в связи с чем постановка шифровального дела бессистемна и случайна, а следовательно, у врагов рабоче-крестьянского государства существует возможность проникнуть в его тайны» [Красная книга ВЧК, 1990]. Далее в проекте предлагалось «создать при ВЧК специальный отдел, задачами которого в числе прочих являлись бы постановка шифровального дела в РСФСР... и подготовка кадров необходимых специалистов» [Красная книга ВЧК, 1990]. 5 мая 1921 г. постановлением малого Совнаркома при ВЧК был создан Специальный отдел, начальником его и одновременно членом коллегии ВЧК назначен Г.И. Бокий.

К сожалению, в тяжелые годы Гражданской войны и послевоенной разрухи существенным образом усилить защиту передаваемой информации оказалось невозможно. После окончания Гражданской войны Советское правительство приложило значительные усилия для становления и развития шифровальной службы как отдельной структуры во всех ведомствах и звеньях государства.

Список рекомендуемой литературы

1. Антонов В. Семь лет во главе советской внешней разведки // Независимое военное обозрение. – 2008. – №24.– с. 12–13.
2. Водитель первого «бронепоезда» // Октябрьский прорыв. – 2007. – Ноябрь. – с. 2.
3. Востоков К. Рождение радиоразведки // Независимое военное обозрение. – 2000. – №30.– с. 7.
4. Боечин И.А. Фиаско «красного лорда» // Независимое военное обозрение. – 2006. – №47. – с. 5.
5. «Зашифрованная война», документальный фильм реж. И. Сахаров, эфир на ОРТ 2.12.2003 и 9.12.2003 в 22 ч. 40 мин.
6. Котельников В. Красные звезды Туркестана // Авиамастер. – 2006. – №4. – с. 32–38.
7. Красная книга ВЧК / под ред. А.С. Велидова. т. 1, 2. – М, 1990.
8. Лайнер Л. Погоня за «Энигмой». – М.: Молодая гвардия, 2004.
9. Лекарев С., Порк В. Радиоэлектронный щит и меч // Независимое военное обозрение. – 2002. – №2. – с.7.
10. Мараев В. Гетманские аэропланы для Всевеликого Войска Донского // Авиация и время. – 2007. – №5. – с. 38–39.
11. Меркачева Е. От мертвого посла уши // Московский комсомолец. – 2006. 20 июня. – с. 7.
12. Николенко А. Умные машины // Воздушно-десантные войска. Спецназ. – 1998. – №4-6(9-11).
13. Разведка. Версия для кино. «Адъютант его превосходительства» документальный фильм, эфир на ОРТ 9.11.2003 в 12 ч. 10 мин.
14. Хроника революции в Москве // Октябрьский прорыв. – 2007. – Ноябрь. – с. 2.
15. Yardley H. O. The american black chamber. – Indianapolis, Bobbs Merrill, 1931.
16. Режим доступа: http: //www.criptograf.narod.ru
17. Режим доступа: www. cryptography.ru
18. Режим доступа: http://en.wikipedia.org/wiki/Biuro_Szyfrów

Глава 8.

Криптографическая деятельность в СССР накануне и во время Второй мировой войны

8.1. Спецотдел ВЧК. Рождение советской криптографической службы

Важнейшей датой в истории отечественной криптографии является 5 мая 1921 г., когда был создан Спецотдел ВЧК, родоначальник криптографической службы Советской России. Впервые в нашей стране была создана единая криптографическая организация. Современные российские криптографические службы являются наследниками этой организации.

После Октябрьской революции 1917 г. судьба России круто изменилась. Необходимость организации новой системы государственного управления потребовала коренной перестройки всех государственных служб и институтов. Не составила исключения и криптографическая служба России, которая в молодой Советской республике создавалась, фактически, заново. Необходимость организации службы, которая осуществляла бы централизованное управление шифровально-дешифровальным делом, стала очевидной для руководителей государства в годы Гражданской войны. Опыт Гражданской и Первой мировой войн красноречиво свидетельствовал, что умение держать в тайне информацию о себе и получать информацию о противнике является одним из важнейших факторов победы.

В январе 1921 г. В.И. Ленин был ознакомлен с некоторыми материалами о результатах работы радиоразведки в годы Первой мировой и Гражданской войн. Ленин отметил большую важность этой работы и поручил Реввоенсовету и ВЧК заняться организацией специальной радиоразведки. Ёще будучи в подполье, В.И. Ленин уделял большое внимание шиф-

ровальному делу. Став руководителем советского государства, он продолжал уделять внимание защите информации криптографическими методами и вопросам добывания информации при помощи радиоразведки и криптоанализа. Ленин несколько раз лично давал рекомендации по совершенствованию системы пользования шифрами, повышению шифрдисциплины, излагал свое мнение о принципах построения шифровальной службы. Приведем цитату по этому поводу. В 1922 г. Ленин писал: «Сообщают об английском изобретении в области радиотелеграфии, передающем радиотелеграммы тайно. Если бы удалось купить это изобретение, то радиотелеграфная и радиотелефонная связь получила бы еще более громадное значение для военного дела» [Лекарев, 2002]. В Советской России началось критическое осмысление состояния безопасности отечественных линий связи и определение организационных форм будущей шифровальной службы страны. В начальный период этой деятельности руководители страны уделяли этой службе должное внимание. В сентябре 1920 г. Политбюро рассмотрело предложение Ленина принять меры к усложнению шифров и к более строгой охране шифрованных сообщений. Политбюро постановило поручить наркому по военным и морским делам Л.Д. Троцкому организовать комиссию из представителей Наркомвоен, Наркоминдел, ЦК РКП(б) и Наркомпочтеля. В.И. Ленин, изучив досконально вопрос, зная мнение различных заинтересованных ведомств, поручает изыскать пути наведения порядка в шифровальном деле руководству ВЧК, хотя шифровальные службы по традиции сохранялись и во внешнеполитическом ведомстве, и в военном наркомате. Возможно, на выбор базового ведомства по осуществлению криптографической деятельности в Советском государстве повлияла сложность обстановки, а также то обстоятельство, что главной функцией ВЧК уже в тот период было обеспечение государственной безопасности в целом. Именно на обеспечение государственной безопасности направлена и деятельность криптографической службы. Во второй декаде января 1921 г. Коллегия ВЧК принимает решение о созыве

совещания представителей заинтересованных ведомств для подготовки соответствующих предложений по воссозданию криптографической службы. В обсуждении вопроса принимали участие представители ЦК РКП(б), ВЧК и наркоматов.

12 апреля на заседании Малого Совнаркома был представлен с проект создания Специального отдела при ВЧК. С данным проектом выступил один из руководителей ВЧК Глеб Иванович Бокий. Вот текст этого документа:

«Имея в виду:

1) Отсутствие в Республике центра, объединяющего и направляющего деятельность шифровальных органов различных ведомств, и связанные с этим бессистемность и случайность в постановке шифровального дела,

2) Возможность, благодаря этому при существующем положении широкого осведомления врагов Рабоче-Крестьянского государства о тайнах Республики, Совет Народных эмиссаров постановил:

Образовать при Всероссийской Чрезвычайной комиссии «Специальный отдел», штаты в коем утверждаются Председателем ВЧК. Начальник Специального отдела назначается Совнаркомом.

В круг ведения Специального отдела при ВЧК включить:

I. Постановку шифровального дела в РСФСР:

А. Научная разработка вопросов шифровального дела:

а) анализ всех существующих и существовавших русских и иностранных шифров;

б) создание новых систем шифров;

в) составление описаний шифров и инструкций по шифровальному делу и пользованию шифрами;

г) собирание архивов и литературы по шифровальному делу для концентрирования такового при Спецотделе;

д) составление и издание руководств по вопросам шифрования.

Б. Обследование и выработка систем шифров:

1. Обследование всех действующих в настоящее время шифров и порядка пользования ими шифрорганами;

2. Окончательная обработка инструкций по шифровальному делу и пользованию шифрами и выработка правил работы шифрорганов;

3. Распределение вновь выработанных систем шифров между всеми ведомствами,

В. Организация учебной части:

1. Выработка программы школы шифровальщиков;

2. Создание школы шифровальщиков;

3. Укомплектование школы преподавателями и учениками.

Г. Учет личного состава шифровальных органов. Наблюдение за закономерной постановкой шифровального дела. Инструктировка и инспекция шифровальных органов:

1. Учет и проверка всех сотрудников всех шифрорганов;

2. Распределение всяких сотрудников всех шифрорганов между последними в зависимости от индивидуальных качеств каждого работника и фактической потребности в работниках в том или ином шифроргане, а также зависимо от государственной важности каждого учреждения;

3. Чистка неблагонадежного и неспособного элемента из всех шифрорганов;

4. Наблюдение за закономерной постановкой шифровального дела во всех шифрорганах;

5. Инструктировка и инспекция всех шифрорганов и проведение в жизнь Инструкции и правил по шифровальному делу.

Постановка расшифровального (имеется ввиду дешифрование – *прим. авт.*) дела в РСФСР:

1. Изыскание способов повсеместного улавливания всех радио, телеграмм и писем неприятельских, иностранных и контрреволюционных;

2. Открытие ключей неприятельских, иностранных и контрреволюционных шифров;

3. Расшифровка всех радио, телеграмм и писем неприятельских, иностранных и контрреволюционных.

Все распоряжения и циркуляры Специального отдела при ВЧК по всем вопросам шифровального и расшифроваль-

ного дела являются обязательными к исполнению всеми ведомствами РСФСР» [Соболева, 2002].

Оценивая этот документ сегодня, можно утверждать, что в функциях спецотдела уже с самого начала были предусмотрены по существу все направления криптографической, которые в совокупности обеспечивают решение задачи обеспечения информационной безопасности государства.

Отдел стал единым центром криптографической службы страны, назывался 8-й спецотдел при ВЧК.

Кадровому составу спецотдела, на взгляд авторов, следует уделить особое внимание. И здесь нельзя не остановиться на личности его первого руководителя Глеба Ивановича Бокия. Этому человеку предстояло стать главным организатором криптографической службы страны и ее первым руководителем, он возглавлял спецотдел с 1921 по 1937 гг.

Глеб Иванович Бокий родился в 1879 г. в старинной дворянской семье. В 1897 г. вступил в петербургский «Союз борьбы за освобождение рабочего класса» и вскоре стал видным революционером, с 1900 г. он член РСДРП, на протяжении 20 лет с 1897 по 1917 год он являлся одним из руководителей петербургского большевистского подполья. В конце 1916 – начале 1917 г. Глеб Иванович был членом Русского бюро ЦК РСДРП, в октябре 1917 г. он член Петербургского военно-революционного комитета, один из руководителей вооруженного восстания. На протяжении своей революционной карьеры Бокий активно использовал шифры, мало того, он разрабатывал и собственные шифрсистемы. Так, при аресте Г.И. Бокия сотрудники правоохранительных органов нередко обнаруживали на первый взгляд самые обычные ученические тетради, исписанные математическими формулами. В действительности это были конспиративные записи, зашифрованными изобретенным Бокием математическим шифром. Ключ к нему был известен только автору. Дешифровальщики департамента полиции подозревали, что за этими «формулами» скрывается шифр.

Для разработки и реализации проекта создания спецотдела Г.И. Бокий пригласил ряд специалистов-криптографов –

В.И. Кривоша-Неманича, И.А. Зыбина и И.М. Ямченко, Г.Ф. Булата, Е.С. Горшкова, Э.Э. Картали, Е.Э. Морица работавших ещё до революции. Они внесли большой вклад в становление советской криптографической службы.

К дешифровальной работе в качестве экспертов-аналитиков в то же время или немного позже (1923 г.) были привлечены Б.А. Аронский, Ф.А. Блох-Хацкелевич и др. В создании основ новой криптографической службы приняли участие и те, кто ранее не работал в этой области. Как мы уже говорили, это были люди, которых лично пригласил Бокий для работы в отдел, исходя из их деловых качеств: А.Г. Гусев, А.М. Плужников, Ф.И. Эйхманс, В.Х. Харкевич и др.

Структура отдела, кадровый состав, задачи и методы его работы во многом продолжали традиции криптографической службы дореволюционной России. В начале 1920-х гг. отдел включал шесть, а позднее семь отделений. Однако собственно криптографические задачи, в строгом понимании, решали только три из них:

2-е, 3-е и 4-е.

В целом распределение задач, стоящих перед отделениями было таким [Соболева, 2002]:

1-е отделение – «наблюдение за всеми государственными учреждениями, партийными и общественными организациями по сохранению государственной тайны»;

2-е отделение – так же сотрудники 2-го отделения спецотдела занимались теоретической разработкой вопросов криптографии, выработкой шифров и кодов для ВЧК (ГПУ – ОГПУ – НКВД) и всех других учреждений страны (включая МИД, военное ведомство и др.). Отделение в первые годы работы состояло из семи человек, его начальником являлся Ф.Г. Тихомиров;

3-е отделение. Перед этим отделением стояла задача «ведения шифр-работы и руководства этой работой в ВЧК (ГПУ – ОГПУ – НКВД). Состояло оно вначале всего из трех человек, руководил отделением старый большевик, бывший латышский стрелок Ф.И. Эйхманс, одновременно являвшийся

заместителем начальника спецотдела. Эйхманс организовывал шифрсвязь с заграничными представительствами органов безопасности СССР, направлял, координировал их работу;

4-е отделение. Сотрудники данного отделения, а их было восемь человек, занимались «открытием иностранных и антисоветских шифров и кодов и дешифровкой документов». Начальниками этого отделения были: с мая по декабрь 1921 г. – Ященко, с января по август 1922 г. – Горячев, с августа1922 по сентябрь 1923 гг. – Эльтман, с сентября 1923 по январь 1938 гг. был А.Г. Гусев, который одновременно выполнял обязанности помощника начальника спецотдела;

5-е отделение. «Перехват шифровок иностранных государств; радиоконтроль и выявление нелегальных и шпионских радиоустановок; подготовка радиоразведчиков»;

6-е отделение – «изготовление конспиративных документов»;

7-е отделение – «химическое исследование документов и веществ, разработка рецептов; экспертиза почерков, фотографирование документов» [Соболева, 2002].

Работа Спецотдела началась с детального изучения архивов дешифровальных служб дореволюционной России. Среди архивных документов были обнаружены подлинники и копии шифров Болгарии, Германии, Китая, США и Японии, а также отчеты о работе по их вскрытию, учебные пособия. Этот факт сыграл важную роль в подготовке специалистов-криптографов в послереволюционной России. Успехи советской специальной службы в создании систем шифров, системы радиоперехвата, в подготовке кадров специалистов-криптографов свидетельствуют о большой целенаправленной и продуманной работе, которая велась в стране в области развития криптографической службы. Подготовке новых кадров для шифровальной работы уделялось большое внимание: при ВЧК еще в 1921 г. были созданы курсы шифровальщиков, где именитые профессионалы делились опытом с молодежью.

Вопрос об организации радиоперехвата, в том числе и зашифрованной информации, был решен путем создания станций особого назначения. Для этого использовались все

имевшиеся в войсках приемные, приемно-контрольные и пеленгаторные радиостанции. Таким образом, была создана и начала функционировать служба специальной радиоразведки, работавшая в интересах ВЧК. Кроме телеграмм, поступавших с телеграфа, часть шифрованной иностранной переписки и переписки белой гвардии по заданиям ВЧК и военных органов перехватывалась на Серпуховской приемной радиостанции Реввоенсовета и Шаболовской радиостанции Наркомпочтеля [Востоков, 2000], [Гольев, 2008].

25 августа 1921 г. Спецотдел ВЧК издал приказ, в соответствии с которым все подразделения в центре и на местах должны были направлять в отдел обнаруженные при обысках и арестах шифры, ключи к ним и шифрованные сообщения.

Одним из первых успехов сотрудников спецотдела стало дешифрование немецкого дипломатического кода, и с июля 1921 г. вся переписка между Москвой и Берлином благополучно становилась достоянием ВЧК. В августе 1921 г. были дешифрованы шифры турецких дипломатических телеграмм. При этом следует отметить интересный факт. С 1927 по 1931 гг. ОГПУ поддерживало негласный, но официальный контакт с турецкой контрразведкой. Турки, по их собственному утверждению «получили … от ОГПУ очень важную помощь в организации шифровального и дешифровального дела» [Очерки, 1997, т. 2]. Из Турции приходила и криптографическая информация, касающаяся других стран. В первой половине 1930-х гг. советской резидентуре в Турции удалось приобрести несколько хорошо информированных источников. Так, в 1932 г. начал сотрудничать с советской разведкой агент «Пижама», служащий посольства Японии в Турции. В течение нескольких лет он передавал важные шифрматериалы посольства Японии [Гольев, 2008].

Успехи советских криптоаналитиков продолжались. В 1924 г. – вскрыты два шифра польского разведотдела генерального штаба, которые использовались для связи с военными атташе в Москве, Париже, Лондоне, Вашингтоне и Токио. В 1927 г. началось «чтение» японской шифрпереписки, в 1930 г. – американской.

Возможность читать зашифрованную переписку противника имеет большое значение и для оперативной деятельности

внешней разведки. Вот пример. В 1921 г. ИНО (иностранный отдел ВЧК, занимавшийся внешней разведкой) добыл шифры антисоветских организаций в Лондоне и Париже. Перехваченные и дешифрованные телеграммы этих центров оказали серьезную помощь в выявлении и обезвреживании врагов молодой советской республики [Гольев, 2008], [Очерки, 1997, т.2].

В 1922 г. в ГПУ СССР (бывшей ВЧК) был создан контрразведывательный отдел (КРО). В первые же годы своего существования сотрудники КРО добыли ряд шифров и кодов, на основании которых большинство телеграфных сообщений иностранных посольств в Москве контролировалось советскими криптоаналитиками. В последующие годы был проведен еще ряд операций по добыче иностранных шифров [Мерзляков, 1999].

Так, в 1920-х гг. советская разведка провела операцию по проникновению в китайское посольство в России в целях добычи шифров. Руководил операцией разведчик-самоучка П.Л. Попов, по профессии судовой механик, работавший в царское время в области охраны рыболовных промыслов России на Камчатке. Пользуясь авторитетом у китайских властей, Попов получил свободный доступ в китайское посольство в Москве. Он сумел получить слепки ключей от сейфов посольства. В результате шифры посольства оказались в руках нашей разведки.

В начале 1924 г. резидентом советской разведки в Ковно (в то время столица Литвы) стал И.К. Лебединский. Он завербовал курьера французского военного атташе в Литве. Через этого курьера советская разведка получала черновики секретной переписки атташе с Парижем, что помогло в раскрытии французских шифров. Работа курьера, получившего псевдоним «Василий», продолжалась до начала 1940-х гг. [Очерки, 1997, т. 2].

В середине 1920-х гг. советский военный атташе в Персии (ныне Иран) Бобрищев (бывший офицер царской армии) завербовал себе на службу практически всех шифровальщиков главного штаба Персии. В результате был получен богатый материал, проливавший свет на внутреннюю и внешнюю политику этой страны. В 1927 г. советская разведка завербовала эксперта по шифрам кабинета министров Ирана. К этому времени на СССР

также работал шифровальщик одной из бригад иранской армии, дислоцировавшейся вблизи русской границы. Кроме того, советская разведка сумела получить ключ к шифрам дашнаков (дашнаки – члены националистической партии «Дашнакцутюн», правившей в армянской буржуазной республике в 1918–1920 гг.; в феврале 1921 г. они организовали антисоветский мятеж, а после его подавления действовали за границей СССР). Деятельностью дашнаков руководили из города Тебриза, расположенного на территории Ирана, советский резидент в Тебризе установил связь с одним из чиновников почтовой службы Ирана и скоро имел в своем распоряжении достаточную информацию, позволявшую ему своевременно узнавать обо всех планируемых мероприятиях дашнаков. К сожалению, в этом же году произошел провал, персидская контрразведка арестовала четырех шифровальщиков, работавших на СССР. Трое из них были расстреляны, а один получил 15 лет тюрьмы. Этот факт был придан огласке и из-за боязни разоблачения многие источники в Персии прекратили сотрудничество с советской разведкой [Гольев, 2008], [Очерки, 1997, т. 2].

Большой интерес спецотдела продолжали вызывать шифры различных антисоветских организаций. В 1920–1930-е гг. было взломано немало таких шифров. Так были вскрыты шифры организации Б.В. Савинкова «Народный союз защиты Родины и свободы», которая из-за рубежа вела активную террористическую деятельность на территории СССР. Напомним, что до октябрьской революции Б.В. Савинков был активным членом организации социалистов-революционеров (эсэров). Савинковцы, в основном, использовали так называемые шифры по слову с перешифровкой с помощью гаммы. Шифры по слову в XIX – начале XX вв. активно применяли российские революционеры [Соболева, 2002] [Бабаш, 2004]. В результате чекисты получили информацию о паролях и явках савинковцев на территории СССР. Эта информация в немалой степени способствовала успешному проведению в 1924 г. операции «Синдикат-2», в результате которой Савинков и несколько других руководителей его организации оказались на территории СССР и были арестованы. В 1922–1924 гг. спецотделом было дешифровано около 38 шифрсообщений меньшевитских организаций, зашифрован-

ных на 17 ключах. В результате было установлены 65 конспиративных адресов, а также пароли и явки меньшевиков. Также в это десятилетие был раскрыт ряд шифров различных монархических организаций. Полученная в результате дешифрования их переписки информация оказалась крайне полезной для советских органов госбезопасности. Интересно отметить, что помимо шифров, монархисты использовали и код на 1000 величин, который тоже был вскрыт сотрудниками спецотдела. В начале 1920-х гг. спецотдел провел криптоанализ шифрматериалов царских правоохранительных органов. Эта работа позволила выявить большое количество сотрудников и агентов полиции и жандармерии, затесавшихся в различные советские организации [Гольев, 2008], [Соболева, 2002].

В дальнейшем тайные операции советской разведки и контрразведки по добыче криптографических секретов оказывали существенную помощь дешифровальщикам. Ряд из них будут рассмотрены в следующих подразделах.

Одновременно со криптоанализом чужих шифров шла напряженная работа по созданию своих. В 1924 г. на основе 52 различных шифров был создан знаменитый «русский код», расшифровать который не удалось никому. Была создана единая инструкция по шифровальной службе, сотрудники спецотдела начали проводить инспекторские проверки в центральных и периферийных органах.

В связи с реорганизацией советских органов безопасности с 6 февраля 1922 г. по 2 ноября 1923 г. отечественная криптографическая служба называлась – спецотдел при ГПУ, а со 2 ноября 1923 по 10 июля 1934 гг. – спецотдел при ОГПУ [Астрахан, 1996], [Ганин, 2001], [Гольев, 2008], [Соболева, 2002].

8.2 Шифровальная служба

Уже в годы Первой мировой войны появились первые предложения по автоматизации шифрования и расшифрования. Наступала эпоха машинных шифров. В межвоенный период на смену ручным шифрам стали приходить шифрмашины

(механические и электромеханические устройства для шифрования). Противостояние государственных интересов, масштабные военные конфликты в первых десятилетиях XX-го в., появление проводной и эфирной телеграфной и телефонной связи, сопровождавшиеся резким возрастанием скорости и объемов передачи информации, потребовали новых методов и техники шифрования секретных сообщений.

Создание и развитие собственной шифровальной службы СССР началось после окончания Гражданской войны. Так называемые «ручные» системы кодирования и шифрования не могли справиться со все возрастающими потоками информации по причине неизбежно низкой скорости её обработки. Кроме того, армейские и дипломатические службы Германии, Японии, США, России и других стран пользовались довольно простыми шифрами. Актуальность разработки механических и электромеханических машин для шифрования текстов, а также электрических шифраторов для радио и телефонных переговоров стала исключительно высокой.

В СССР пионерами машинного шифрования стали специалисты, работавшие в области криптографической защиты речевого сигнала. С начала XX-го в. уже открытые принципы однополосной модуляции электрических звуковых сигналов, гетеродинного преобразования частоты, регистрации речевых сигналов на магнитный носитель (проволоку) и другие изобретения для своей практической реализации в приборах шифрования телефонных переговоров нуждались в эффективных усилительных электрических приборах. Технологические успехи в изготовлении электровакуумных ламп с приемлемыми характеристиками позволили разрабатывать телефонную шифртехнику уже в 1920-х гг.

М.А. Бонч-Бруевич

В 1920 г. М.А. Бонч-Бруевич (Михаил Александрович Бонч-Бруевич (1888–1940) советский ученый, один из пионеров радиотехники, член-корреспондент Академии наук СССР (1931). Организовал первое отечественное производство электронных ламп (1916–1919). В 1918–1928 гг. руководитель Нижегородской радиолаборатории. Под руководством М.А. Бонч-Бруевича создана первая в мире мощная радиовещательная станция им. Коминтерна в Москве (1922). М.А. Бонч-Бруевич является автором многочисленных трудов в области радиотехники [Словарь, 1984], усовершенствовал временную перестановку. Принцип этого засекречивающего преобразования весьма прост. Представим себе, что речь записана на магнитную ленту. Эта лента разрезается на мелкие фрагменты, которые затем «склеиваются» по заранее заданному закону перестановки «отрезков». В этом склеенном виде информация поступает в канал телефонной связи. На приёмном конце, зная правило перестановки, восстанавливается исходное сообщение. Бонч-Бруевич предложил кадровую структуру преобразований, когда в каждом сегменте из нескольких отрезков перестановка осуществлялась по своему правилу [Бабаш, 2003].

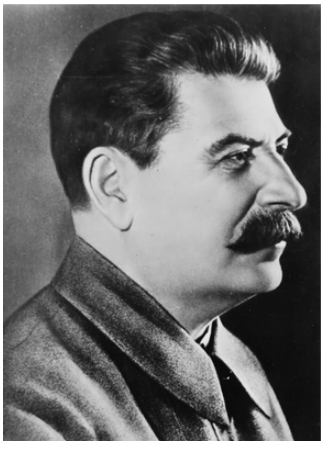
Первые разработки аппаратов секретного телефонирования в СССР относятся к 1927–1928 гг., когда в НИИС (научно исследовательский институт связи) РККА были изготовлены для погранохраны и войск ОГПУ шесть аппаратов ГЭС (конструктор Н.Г. Суэтин) и проведены работы, направленные на создание усовершенствованного секретного полевого телефона ГЭС-4 [Астрахан, 2001]. В 1930-х гг. в области секретной телефонии вели работы семь организаций: НИИ НКПиТ (наркомата почт и телеграфа), НИИС РККА, завод имени Коминтерна, завод «Красная Заря», НИИ связи и телемеханики ВМФ, НИИ №20 НКЭП, лаборатория НКВД.

В 1930 г. были сданы в эксплуатацию первые линии междугородной правительственной высокочастотной связи (ВЧ-связь) Москва-Ленинград и Москва-Харьков. В 1931 г. была создана первая отдельная сеть междугородной ВЧ-связи с применением специальных средств защиты. В 1934 г. на заводе

«Красная Заря» (Ленинград) начался крупносерийный выпуск трехканальной аппаратуры высокочастотного телефонирования СМТ-34, работающей в диапазоне 10,4-38,4 кГц и обеспечивающей удовлетворительное качество связи на расстоянии до 2000 км [Свирский, 2001]. В начале 1941 г. на линии связи Москва-Ленинград была установлена 20-тиканальная аппаратура ВЧ-телефонирования. К началу Отечественной войны ВЧ-связь была организована между Москвой и большинством столиц союзных республик, многими областными центрами, военными округами [obereg]. В мае 1945 г. (конец войны с Германией) протяженность обслуживаемых войсками линий ВЧ связи составила 32944 км, а в августе 1945 г. (во время боевых действий против Японии) достигла 36854 км.

При этом следует отметить, что сама технология ВЧ-связи, без применения аппаратуры шифрования, могла защитить только от прямого прослушивания. Дело в том, что по проводам передавался ток высокой частоты, модулированный звуковым сигналом от мембраны телефона. Такой сигнал не воспринимается человеческим ухом без соответствующей обработки, так как человеческое ухо электромагнитные колебания не улавливает. А вот если его пропустить через простейший детекторный приемник, то разговор восстанавливался в первозданном виде. Любой техник на междугородней станции наркомата связи мог прослушать разговоры правительства по ВЧ.

Впервые об уязвимости ВЧ-связи можно прочесть в рапорте старшего техника-инженера М. Ильинского на имя начальника 13-го отделения оперативного отдела ГУГБ НКВД СССР И. Воробьева. Документ датирован 8 августа 1936 г. Основные источники угроз – агентура иностранных спецслужб среди обслуживающего персонала и использование различных портативных и простых в обслуживании технических средств. В ходе испытаний вблизи Минска в 1936 г. была выявлена возможность перехвата разговоров на радиоприемники с длинноволновым диапазоном при помощи антенны, подвешенной на расстоянии ближе 50 м от междугородной цепи. В другом документе, появившемся в феврале 1937 г., есть фраза о том, что



И.В. Сталин

разговоры могут подслушиваться (и слушаются) нашими работниками ВЧ, а им также полностью доверять нельзя. При этом отметим, что эти люди работали в системе НКВД, а не НКС (Наркомат связи), поэтому и требования при приеме на работу должны быть строже. В 1937 г. первая информация о возможности перехвата поступила от агентуры НКВД БССР, которая в 1,5 км от границы на территории Польши обнаружила специальное подключение к линии связи Москва – Варшава. В 1938 г. начальник отделения правительственной ВЧ-связи СССР И. Воробьев в одном из рапортов указал, что спецсвязь НКС, которой пользуются абоненты Кремля, не обеспечивает никакой секретности разговоров, так как эта связь предоставляется Кремлю в известные часы и разговор членов правительства проходит через ту же аппаратуру НКС, обслуживаемую техническим составом, который обслуживает и коммерческие разговоры. Поэтому в срочном порядке пришлось проложить специальный кабель, соединяющий станцию ВЧ-связи с АТС Кремля. Много еще в столице было правительственных зданий, которые пользовались услугами городской телефонной сети. С целью обеспечения конфиденциальности и предотвращения перехвата разговоров по ВЧ в исследовательской лаборатории НКС были изготовлены специальные защитные фильтры, которыми оборудовались все междугородние телефонные линии, уходившие за границу. Позднее в начале 1941 г. в Таллинне была установлена изготовленная в лаборатории оригинальная аппаратура «шумовой завесы», которая практически предотвращала возможность перехвата переговоров по ВЧ на специальную радиоаппаратуру. Уже в первом полугодии было налажено производство «аппаратуры шумов» для Москвы, Ленинграда, Риги [Астрахан,

2001]. К сожалению, случаи недисциплинированности технического персонала и халатного отношения к своим служебным обязанностям отмечались и во время войны. При этом в одном из документов того времени указывалось, что войска правительственной связи комплектовались в общем порядке и в них могли попасть агенты германской или финской разведки. Кстати отметим, что 5 мая 1941 г. было утверждено «Положение о правительственной связи»; засекреченная ВЧ-связь отнесена к категории правительственной связи [Астрахан, 1996].

Исходя из вышеизложенного, задача разработки и внедрения шифртехники на линии советской правительственной связи была чрезвычайно актуальной. Поскольку потребность в аппаратуре засекречивания телефонных разговоров была очень велика (состояние работ неоднократно докладывалось наркомом внутренних дел руководству ВКП(б) и СНК, а также лично И.В. Сталину), органы госбезопасности сочли возможным одновременно обратиться к зарубежным фирмам-производителям подобной аппаратуры.

К тому времени отечественным специалистам уже были известны некоторые иностранные аналоги проектируемых в СССР «секреток». Так, американская установка с однократным инвертированием спектра использовалась в московском радиотелефонном центре, а шифратор фирмы Siemens был в 1936 г. испытан на магистрали Москва – Ленинград; имелось также краткое рекламное описание переносного телефонного шифратора Siemens. Однако была необходима полная и достоверная информация по зарубежным шифраторам: рассматривалась возможность размещения заказов на разработку новой аппаратуры или приобретения готовой продукции. Через Технопромимпорт и Наркомат внешней торговли в начале 1937 г. было запрошено более десятка европейских фирм, производивших аппаратуру надтонального телефонирования, в том числе Siemens&Halske и Lorenz (Германия), Bell Telephone (США) и Automatic Elektric (Бельгия), Standart Telephone and Cables (Великобритания) Hasler (Швейцария), а также Ericsson (Швеция). К запросам, как правило, прилага-

лись технические требования к аппаратуре: фирме не нужно было гарантировать невозможность расшифрования разговора посредством аналогичной установки – достаточно было обеспечить защиту от дешифрования с помощью радиоприемника с дополнительными простыми устройствами. Тем не менее, большинство фирм ответили на запрос прямым отказом. Некоторые потребовали за разработку шифраторов очень высокую цену (в пределах 40–45 тыс. долл. США – в то время это была весьма существенная сумма). Среди немногих приемлемых предложений заслуживал внимания только ответ английской фирмы «Стандарт Телефон энд Кэблз», чьи шифраторы могли быть использованы как дополнительное оборудование магистрали Москва–Хабаровск.

Тем временем разработка «секреток» в отечественных лабораториях подходила к концу. В 1935-1936 гг. на заводе «Красная Заря» было создано устройство автоматического засекречивания телефонных переговоров – инвертор ЕС (по фамилиям разработчиков К.П. Егоров и Г.В. Старицын) и налажен его выпуск для каналов телефонной высокочастотной связи. Через год ленинградский завод «Красная Заря» наладил выпуск шифратора ЕС-2. Шифратор ЕС-2 при раздельной читке текста обеспечивал разборчивость всего 20–30% слов, цифры при этом понимались полностью. Несмотря на то, что смысл текста уловить практически не удавалось, аппарат прошел дополнительные испытания (вместе с переносным шифратором лаборатории Ленинградского управления НКВД) на линии Москва – Сочи. В ходе испытаний (4–14 августа 1937 г.) шифратор зарекомендовал себя в целом положительно. Но выяснилось, что включение «секреток» в линию ВЧ-связи требует высокого качества проводных каналов (хорошая частотная характеристика, отсутствие помех и шумов и др.), что предопределило обязательный учет этих параметров на всех последующих этапах развития сети междугородной правительственной связи.

В сентябре 1937 г., после того как завод «Красная Заря» представил на утверждение второй образец установки ЕС-2,

было принято решение включить ее в постоянную эксплуатацию на линии Москва – Ленинград. Постановлением СНК СССР о развитии правительственной ВЧ-связи К53/ко от 05.01.1938 г. наркомату связи предлагалось к 1 мая 1938 г. обеспечить поставку НКВД 12-ти полукомплектов стоек типа ЕС-2. Так было положено начало серийному производству первого поколения отечественной аппаратуры автоматического засекречивания телефонных переговоров. В 1937 г. для радиотелефонных каналов была разработана и подготовлена к серийному выпуску аппаратура под индексом ЕИС-3 (Егоров-Ильинский-Старицын). В течение последующих 3-х лет завод «Красная Заря» освоил выпуск целой серии аппаратуры простого засекречивания, подобной ЕС-2 (ЕС-2М, МЕС, МЕС-2, МЕС-2А, МЕС-2АЖ, ПЖ-8, ПЖ-8М и др.), которая подключалась непосредственно к аппаратуре ВЧ-связи СМТ-34. К 1940 г. завод выпустил 262 аппарата, в основном с инверсией спектра. Принцип работы новинки был достаточно прост: инверсия с одновременной подачей в канал связи мешающего тона с высоким тембром. Этими установками в 1938 г. было оборудовано 9 междугородных правительственных линий связи, к июлю 1940 г. из имевшихся 103 линий связи 50 были оборудованы аппаратурой засекречивания телефонных переговоров, а на 1 апреля 1941 г. – 66 линий из имевшихся 134. В целом это свидетельствовало о невыполнении приказа НКВД от 1940 г. «Об улучшении правительственной ВЧ-связи» из-за ограниченных производственных возможностей заводов «Красная Заря», №208 и №209, НИИ-10, а также недостаточным их финансированием [Павлов, 2009]. С 1939 г. поступила в серийное производство междугородная автоматика для ВЧ-связи МА-5 (на 5 абонентов и 10 каналов) и малый вариант на 3 абонента МА-3, что обеспечивало автоматическое соединение абонентов без помощи телефонисток. По состоянию на 1941 год в стране функционировало 116 ВЧ-станций и 39 трансляционных пунктов, а количество обслуживаемых абонентов высшего партийного и государственного руководства достигло 720 [Павлов, 2009].

Устройства типа «ЕС» успешно использовались для организации ВЧ-связи практически на всем протяжении Великой Отечественной Войны и позднее. Во второй половине 1938 г. была завершена разработка и проведены испытания аппаратуры «сложного» засекречивания С-1 на магистрали Москва–Ленинград, а в дальнейшем – на магистрали Москва–Хабаровск, Москва–Куйбышев–Ташкент. Препятствиями на пути серийного производства С-1 были сложность и высокая стоимость этой аппаратуры. Степень защиты у неё была низкая и в основном защищала от стандартных схем прослушивания, которые сотрудники НКС имели на своих станциях. Была разработана аппаратура шифрования для телеграфной связи С-380М. Её стойкость тоже была слабая. По этой причине, простые инверторы типа «ЕС» в течение еще почти десяти лет оставались основным гарантом обеспечения безопасности правительственной связи. К первому периоду войны относится разработка аналогичной портативной, исполненной в виде чемодана, засекречивающей аппаратуры типа СИ-15 («Синица») и САУ-16 («Снегирь»), которая применялась для засекречивания любых каналов и использовалась в основном при выездах командующих фронтами и представителей Ставки ВГК в пункты, не имеющие ВЧ-станций [Астрахан, 2001].

В целом в лаборатории отдела радиопередающих устройств комбината имени Коминтерна (Ленинград) в 1933–1936 гг. по срочному заказу отдела правительственной связи ГУГБ НКВД было разработано 4 типа аппаратов. Важнейшими из условий были возможность сопряжения с имеющейся ВЧ-аппаратурой, учет специфики эксплуатации станций правительственной связи и обеспечение узнаваемости расшифрованных голосов абонентов. Разработанные 4 типа «секреток» выполняли различные засекречивающие преобразования: 1) малогабаритная переносная шифрустановка с инверсией спектра частот; 2) установка с инверсией разговорных частот и «воблингом» (качанием частоты радиопередатчика); 3) СУ-1 с динамической инверсией и перестановкой 2-х полос спектра с заданной скоростью; 4) СЭТ-2 – сложная система шифрования с дина-

мической перестановкой 3-х полос спектра по произвольному закону и с произвольной в известных пределах скоростью. Однако ещё в 1940 г. констатировалось, что «разработанная по заказу НКВД заводом «Красная Заря» аппаратура для засекречивания телефонных разговоров обладает слабой стойкостью и не имеет кода» [Астрахан, 2002].

В 1938–1939 гг. в ЦНИИ связи НКПиТ были организованы две лаборатории под руководством В.А. Котельникова по засекречиванию телеграфной и телефонной информации. Владимир Александрович Котельников (1908–2005) великий русский ученый, академик АН СССР, дважды Герой Социалистического Труда, лауреат многочисленных премий. В.А. Котельников опубликовал фундаментальные труды в области радиотехники, теории помехоустойчивой связи, радиолокации, радиоастраномии. Впервые в мире сформулировал и доказал фундаментальную теорему дискретизации, на которой основана вся цифровая обработка сигналов. Под его руководством в 1930 годы были созданы первые отечественные аппараты для шифрования речевого сигнала. Эта работа продолжалась и в годы Великой Отечественной Войны. Параллельно с К. Шенноном В.А. Котельников математически формализовал требования к стойкости шифров. В.А. Котельниковым впервые в СССР были разработаны принципы построения телеграфной засекречивающей аппаратуры, реализованные в аппаратуре «Москва», путем наложения на сообщения знаков шифра.

В.А. Котельников

Предложенная В.А. Котельниковым схема наложения шифра на открытый текст оказалась очень привлекательной, и долгое время использовалась в аппаратуре следующих поколений. Сам шифратор был сложным, громоздким, он был скон-

струирован на электромеханических узлах. В основе конструкции лежал барабан, заполненный шариками. При вращении барабана через систему штырей и щелей шарики случайным образом скатывались по шести вертикальным трубкам на две движущиеся телеграфные ленты, которые были наложены одна на другую через «копирку». В результате на обеих лентах получался одинаковый рисунок – «дорожки» из случайно расположенных пятен. Затем по этим меткам ленты перфорировались. Эти ленты образовывали случайный ключ и рассылались на пункты установки аппаратуры. Считывание шифра с ключа производилось с помощью фотоэлектронных элементов. Эта аппаратура была испытана на линии связи Москва–Комсомольск на Амуре [Быховский, 2003]. На заводе №209 в 1938 г. был размещен заказ на 30 приборов С-308-М, которые гарантировали практически полную невозможность дешифрования телеграфных сообщений [Павлов, 2009]. В начальный период формирования телефонной лаборатории в ней работали Ю.Я. Волошенко, Д.П. Горелов, М.Л. Дайчик, Г. Двойневский, А.Я. Захарова, К.Ф. Калачев, Н.Н. Коробков, Р. Лейтес, В.А. Малахов, В.Н. Мелков, Н.Н. Найденов, А.П. Петерсон, Строганов, А.М. Трахтман, Н.А. Тюрин, В.Б. Штейншлегер и др. [Калачев, 1999].

В 1939 г. В.А. Котельникову было поручено решение важной государственной задачи – создание шифратора для засекречивания речевых сигналов с повышенной стойкостью к дешифрованию. Заказчиком аппаратуры был отдел правительственной ВЧ-связи. Помимо В.А. Котельникова в работах по секретной телефонии принимали А.Л. Минц, К.П. Егоров, В.К. Виторский. С началом Великой Отечественной Войны сотрудники завода «Красная Заря» были эвакуированы в Уфу и входили в состав Государственного союзного производственно-экспериментального института (ГСПЭИ-56), где продолжали результативно работать. Лаборатория В.А. Котельникова была разделена на две части: основная часть вместе с руководителем была эвакуирована в ГСПЭИ-56, а другая часть была передана в НКВД СССР. В специальной лаборатории ЦНИИС была предложена

система, основанная на квазислучайных (известных только получателю) перестановках временных (100 миллисекунд) отрезков и 2-х частотных полос с инверсией речевого сигнала. Управление частотными и временными перестановками на передаче и приеме осуществлялось шифратором, генерировавшим 5 бит гаммы 10 раз / с. Разработка шифратора имела оборонное значение, и для ее завершения лаборатория во время войны была эвакуирована в Уфу, где ее сотрудники объединились с группой специалистов, занимавшихся подобной разработкой на заводе «Красная заря» в Ленинграде. Шифратор был создан к осени 1942 г. [Быховский, 2001], [Быховский, 2006].

Во время Великой Отечественной Войны, разработанная под руководством В.А. Котельникова и испытанная ещё в 1938 г., сложная засекречивающая аппаратура С-1 «Соболь» широко использовалась в действующей армии. Несмотря на все трудности, уже к осени 1942 г. сотрудники лаборатории Котельникова изготовили несколько образцов оборудования для секретной КВ-радиотелефонии под индексом «Соболь-П». Этой аппаратурой была оборудована, в качестве опытной, радиотелефонная связь на линии Москва–Хабаровск [Павлов, 2001]. Это была самая сложная из разрабатываемой в стране аппаратура засекречивания передаваемой информации, не имевшая аналогов в мире. Первые аппараты сразу направили под Сталинград для связи Ставки Верховного Главнокомандования со штабом Закавказского фронта, проводная связь между которыми была разрушена во время боёв. В то время в армии для связи такого уровня пользовались в основном проводными телефонными линиями, а «Соболь-П» позволил устанавливать связь посредством радиоканала. К началу 1943 г. было налажено производство усовершенствованной серии аппаратов «Соболь-П». Сложные механические узлы уникальных шифраторов, разработанных в лаборатории Котельникова, изготовлялись на одном из ленинградских заводов. Для окончательной наладки шифраторов Котельников регулярно летал в блокадный город, не раз подвергался при этом вражеским обстрелам. Готовые аппараты срочно отправляли на фронт. Как вспоминали ветераны Вели-

кой Отечественной Войны, применение шифраторов Котельникова в ходе решающих боев на Курской дуге в значительной степени определило успешный исход битвы. Они обеспечивали систему кодирования речи для закрытой радиосвязи, которая практически не поддавалась вскрытию, это оказалось не по зубам даже лучшим немецким дешифровальщикам вермахта. По сведениям советской разведки, Гитлер заявлял, что за одного криптоаналитика, способного её «взломать», он не пожалел бы три отборные дивизии.

За создание шифраторов Котельников и его коллеги по лаборатории (И.С. Нейман, Д.П. Горелов, А.М. Трахтман, Н.Н. Найденов) получили в марте 1943 г. Сталинские премии I степени. Деньги они передали «на нужды фронта». В частности, на премию, полученную В.А. Котельниковым, был построен танк. В дальнейшем аппаратура «Соболь-П» активно использовалась для связи Ставки Верховного Главнокомандования с фронтами. После окончания Второй мировой войны она получила применение и на дипломатических линиях связи Москвы с Хельсинки, Парижем и Веной при проведении переговоров по заключению мирных договоров, а также при проведении Тегеранской, Ялтинской и Потсдамской конференций глав трёх государств и для связи с Москвой нашей делегации во время принятия капитуляции Германии в мае 1945 г. Работа над усовершенствованием шифровальной аппаратуры продолжалась до последних дней войны и даже после её окончания. За дальнейшие разработки в этой области группе специалистов и В.А.Котельникову в 1946 г. была присуждена вторая Сталинская премия I степени [Синявская, 2009].

Одновременно с созданием аппаратуры засекречивания были начаты работы по её дешифрованию. В 1943 г. НКГБ была создана группа из пяти специалистов под руководством А.П. Петерсона, которая одновременно с работами по созданию аппаратуры шифрования занялась вопросами оценки стойкости аппаратуры засекречивания речевого сигнала. С середины 1944 г. группа А.П. Петерсона начала «сокрушать» одну аппаратуру за другой. В итоге в конце 1945 г. был состав-

лен отчет, в котором постулировалось, что аналоговая аппаратура шифрования мозаичного типа теоретически дешифруема. Для того чтобы получить недешифруемую аппаратуру засекречивания телефонных переговоров, речь необходимо сначала перевести в цифровую форму, и было предложено использовать для этих целей вокодер [vkmtusi]. В лаборатории В.А. Котельникова проводились также исследования возможности создания аппаратуры засекречивания с использованием принципа полосного вокодера с выделением основного тона речи, открытого в 1939 г. американским инженером Г. Дадли. «Я стал думать, как бы передавать речь не всю полностью, а как-то сжать её спектр. Начал рассматривать спектр звуков, чтобы понять, какие частоты определяющие… В это время попалась на глаза ссылка на статью Хомера (на самом деле Гомера – *авт.*) Дадли, опубликованную в октябре 1940 г., где говорилось, что он сделал преобразователь речи – «Вокодер». Бросился смотреть, а оказалось, что там ничего конкретного не написано. Но всё равно, это было очень полезно: идея у него та же, значит, мы на правильном пути. В общем, мы начали делать свой «вокодер». И перед самой войной у нас уже работал его опытный образец. Правда, пока он ещё «говорил» плохо, «дрожащим голосом»… » [Синявская, 2009]. В ходе работы В.А. Котельниковым был также предложен и опробован принцип артикуляционного тестирования систем передачи речи. В 1941 г. Котельников доказал, что можно создать математически недешифруемую систему засекречивания, если каждый знак сообщения будет засекречиваться выбираемым случайно и равновероятно знаком гаммы (совершенно стойкий по К. Шеннону шифр [Шеннон, 1963]). Такая система должна быть цифровой, а преобразование аналогового сигнала в цифровую форму должно основываться на теореме отсчетов (другое – название теорема дискретизации) В.А. Котельникова. Такая аппаратура начала создаваться только после войны. Возможности промышленной базы для выпуска техники засекречивания телефонных переговоров были невелики. Так, в период 1941–1947 гг. опытное производство ГСПЭИ-56 (Уфа), завод №697 НК промсвязи

(Уфа) и завод №209 НК Судпрома (Ленинград) выпустили в общей сложности 2024 шифраторов речи, в основном типа инвертора спектра речи.

Аппаратура для шифрования текстовых сообщений появилась несколько позднее. Хотя еще в конце XIX в. в России были предприняты попытки создания аппаратов для автоматического шифрования телеграфных сообщений. Так в 1879 г. главный механик Петербургского телеграфного округа И. Деревянкин предложил оригинальный прибор по шифрованию телеграмм, который он назвал «Криптограф». Это устройство напоминало известный шифратор эпохи возрождения диск Альберти. Прибор представлял из себя два диска, один из них был подвижным. Применялись и другие примитивные шифровальные приборы, в основном реализующие многоалфавитную замену (линейки, диски, и т.п.). В качестве примеров подобных приборов можно привести механический прибор «Скала», предназначенный для облегчения работы с шифром «лямбда» (подробнее об этом шифре в статье [Бабаш, 2004-2]) и разработанное в 1916 г. подпоручиком Попазовым шифровальное устройство, впоследствии названное «Прибор Вави». Устройство по своей идее было похоже на широко известный шифратор Джефферсона, описание этого устройства можно найти в статье [Бабаш, 2004-1].

В.И. Бекаури

Первая попытка создать текстовый электромеханический шифратор в Советской России была предпринята в 1923 г. специалистами Особого технического бюро (Остехбюро) по военным изобретениям специального назначения, которое было создано в 1921 г. по указанию правительства как филиал московского НИИ-20, занимавшегося разработками в области радиотехники для нужд армии и флота. Под руководством российского

изобретателя В.И. Бекаури Остехбюро стало крупнейшим центром по разработке исключительно разнообразных направлений, имевших важное оборонное значение – минное и торпедное дело, подводное плавание, авиация, связь, парашютная техника, телемеханика и др. В 1925 г. были изготовлены новейшие средства управления кодированными сигналами по радио взрывами мощных фугасов. В 1927 г. в Остехбюро были изготовлены и испытаны образцы усовершенствованных приборов «БЕМИ» (по фамилиям изобретателей Бекаури и Миткевича) для управления взрывами на расстояниях до 700 км шифрованными сигналами от мощных радиовещательных станций.

В московском отделении Остехбюро к 1931 г. среди других уже функционировала лаборатория шифровальной аппаратуры. Именно тогда был разработан и даже изготовлен первый советский действующий макет дискового шифратора. В 1936 г. были успешно проведены войсковые испытания аппаратуры секретной шифрованной связи «Ширма». В дальнейшем была разработана система принципиально нового вида скрытой помехоустойчивой кодовой радиосвязи «Изумруд» для самолетов дальней и бомбардировочной разведывательной авиации, а также для обеспечения связи между штабами ВВС. Однако предвоенный и военный периоды диктовали необходимость разработки таких проектов, как радиоуправление минами, катерами, танками и даже самолетами. Совершенствование приборов «БЕМИ» и методов применения дистанционных минно-взрывных средств в войсках продолжалось в предвоенные и военные годы рядом талантливых инженеров [Басин, 1984], [Монетчиков, 2007].

Донесения о непредсказуемых и необъяснимых взрывах поступали гитлеровскому командованию и с других фронтов. Анализируя эти донесения и данные разведки, немецкие специалисты поняли, что имеют дело с новым инженерным боеприпасом. Однако, узнать, что он собой представляет, им долго не удавалось. В декабре 1941 г. в руки советских войск попал секретный приказ Гитлера, в котором говорилось: «Русские войска, отступая, применяют против немецкой армии «адские

машины», принцип действия которых еще не определен. Наша разведка установила наличие в боевых частях Красной Армии саперов-радистов специальной подготовки. Всем начальникам лагерей военнопленных пересмотреть состав пленных русских в целях выявления специалистов данной номенклатуры. При выявлении военнопленных саперов-радистов специальной подготовки последних немедленно доставить самолетом в Берлин. О чем доложить по команде лично мне» [Басин, 1984].

Радиоуправляемые мины применялись Красной Армией при обороне Москвы, а позже Сталинграда, Курска и других городов. В своих воспоминаниях маршал инженерных войск В.К. Харченко, в годы Великой Отечественной войны начальник штаба инженерной бригады специального назначения, отмечал: «Управляемые по радио советские мины причиняли гитлеровцам немалые потери. Но дело было не только в этом. Приборы Ф-10 вместе с обычными минами замедленного действия создавали в стане врага нервозность, затрудняли использование и восстановление ...важных объектов. Они заставляли противника терять время, столь драгоценное для наших войск суровым летом и осенью 1941 г.» [Монетчиков, 2007]. Мины, управляемые по радио зашифрованными сигналами от радиостанций широкого вещания, использовались до лета 1943 г. Исключительно талантливый и многократно награжденный конструктор В.И. Бекаури по ложному обвинению в шпионаже в пользу Германии был расстрелян в 1938 г., впоследствии в 1956 г. полностью реабилитирован [Дадуков, 2006-1] [pvo]. После падения Берлина на допросе командующего обороной фашистской ставки генерала Г. Вейдлинга на вопрос об установке в Берлине мин, взрываемых по радио, он ответил: «…соответствующей техники не было, а что касается радиофугасов, то ваши инженеры далеко опередили наших…» [Монетчиков, 2007].

В 1930-е годы отдельные образцы приборов для кодирования и засекречивания передач телеграфных аппаратов Шорина были разработаны в НИИС РККА (руководитель конструктор А.И. Цыгикало) – прибор засекречивания ПСТБ для аппарата Бодо, прибор ТК-10 для кодирования связи радиостанции 71ТК,

и аппараты засекречивания телеграфных передач системы КИМ-2 (И.Г. Кляцкин и Б.П. Малиновский) и в 1940–1941 гг. системы конструктора А.А. Дудкина [История СЗИ] [referent].

В СССР теоретическую основу создания шифровальной техники, радикально отличающейся от зарубежных образцов, впервые в 1930 г. предложил талантливый инженер И.П. Волосок, который стал ведущим конструктором многих образцов отечественной шифртехники довоенного и послевоенного периодов. Использованный им принцип наложения случайной последовательности знаков (гаммы) на комбинации знаков открытого текста создавал нечитаемую криптограмму с гарантированной стойкостью против дешифрования противниками. Физическим носителем знаков случайной гаммы являлась перфолента, изготовляемая с помощью оригинального изобретения – специального устройства, называвшегося «Х». В технической лаборатории шифровальной службы (8-й отдел) главного штаба РККА (образована в 1931 г.) под руководством И.П. Волоска в 1932 г. был создан опытный образец советской шифровальной машины с прозрачным авторским наименованием «ШМВ-1», а также образцы механических шифрующих приспособлений к телеграфным аппаратам. Громоздкая и механически ненадежная «ШМВ-1» в серию не пошла. Но уже в начале 1934 г. была начата разработка электромеханической шифровальной машины «В-4». В 1937 г. на ленинградском заводе №209 им. А.А. Кулакова были произведены опытные экземпляры советского шифратора «В-4» (конструктор И.П. Волосок), реализующего шифр гаммирования, а в 1938 г. на заводе началось серийное производство [Дадуков, 2006-2]. В 1939 г. В.М. Шарыгиным была проведена модернизация шифратора «В-4», новая машина получила название М-100 и стала производится параллельно с «В-4», начиная с 1940 г. [Дадуков, 2006-3]. Репрессии 1937 г. отрицательно повлияли на производство шифровальной техники в СССР. Особенно это коснулось ведущего производителя шифровальной техники, завода «Красная Заря» в Ленинграде. Многие перспективные разработки

шифровальной техники оставались в лучшем случае на уровне опытных образцов. Наиболее перспективная аппаратура, «Изумруд» и «В-4», была выпущена очень маленькой серией и предназначалась для шифрования информации, передававшейся по телеграфным линиям связи между штабами военных округов и флотов.

Шифровальная машина М-100 состояла из трех основных узлов – клавиатуры с контактными группами, лентопротяжного механизма с трансмиттером и приспособления, устанавливаемого на клавиатуру пишущей машинки и семи дополнительных блоков. Общий вес комплекта достигал 141 кг. Только одни аккумуляторы для автономного питания электрической части машины весили 32 кг. Тем не менее, данная техника выпускалась серийно и в 1938 г. была успешно испытана в боевых условиях во время гражданской войны в Испании (1936–1939 гг.) на Хасане в 1938 г., в 1939 г. на Халхин-Голе и в 1939–1940 гг. во время финской войны [Клепов, 2009]. По другим данным боевое крещение советские шифрмашины получили лишь в 1939 г. – аппаратура «В-4» использовалась в районе боевых действий у реки Халхин-Гол [Дадуков, 2006-4]. Шифрованная связь в этих военных конфликтах осуществлялась в звене Генеральный штаб – Штаб армии. Руководство эксплуатацией техники осуществлял непосредственно И.П. Волосок. Полученный боевой опыт осуществления скрытого управления войсками показал, что для успешного применения машинного шифрования необходима обособленная работа шифровальных органов РККА. Кроме того, необходимо было обеспечить конспирацию в работе шифровальщиков и их достаточную мобильность при передислокации войск. Для этих целей в 1939 г. в США были закуплены 100 автобусов «Студебеккер». Стало возможным зашифровывать и расшифровывать телеграммы не только во время остановок, но и во время движения колонн. К этому времени лаборатория 8-го отдела Генерального штаба РККА переросла в довольно мощное конструкторское бюро. Сам 8-й отдел возглавлял с 1938 г. П.Н. Белюсов.

Это был талантливейший руководитель шифровальной службы, великолепный администратор, тонкий психолог, прослуживший на своем посту до 1961 г. Под его началом находилась сильная команда конструкторов первых советских шифровальных и кодировочных машин – И.П. Волосок, П.А. Судаков, В.Н. Рытов, П.И. Строителев, Н.И. Гусев, Н.М. Шарыгин, М.С. Козлов.

В том же 1937 г. на заводе №209 под руководством В.Н. Рытова был создан макет малогабаритного дискового шифратора, призванный заменить ручные шифры в оперативном звене управления (армия – корпус – дивизия). В нем нашел применение шифр многоалфавитной замены. Это было довольно компактное устройство, упакованное в один ящик весом 19 кг. В 1939 г. эта шифрмашина под названием К-37 «Кристалл» была запущена в серийное производство и только за 1940 г. было выпущено 100 комплектов К-37. В 1940–1941 гг. она выпускалась в Ленинграде, а в 1942–1945 гг. на заводе №707 в Свердловске, выпуск машины продолжался до 1946 г. [Дадуков, 2006-4]. А всего, к началу Великой Отечественной войны было принято на вооружение шифрорганов СССР свыше 150 комплектов К-37 и 96 комплектов М-100. Эта техника позволила в 5–6 раз повысить скорость обработки шифртелеграмм, при этом сохраняя стойкость передаваемых сообщений [Андреев, 2002]. К июню 1941 г. штат советской шифровальной службы насчитывал 1857 человек.

Во втором квартале 1939 г. на заводе №209 были изготовлены опытные образцы аппаратуры засекречивания телеграфных сообщений «С-308» (для телеграфного аппарата Бодо) и «С-309» (для отечественного телеграфного аппарата СТ-35). В третьем квартале 1939 г. начался серийный выпуск этой аппаратуры на заводе №209, а в 1942–1945 гг. аппаратура производилась на заводе №707 в Свердловске. В 1940 г. конструктором П.А. Судаковым был разработан военный буквопечатающий стартстопный телеграфный аппарат со съемным шифрующим блоком «НТ-20». С января 1941 г. началось се-

рийное производство данной аппаратуры на заводе №209, а в 1942–1945 гг. эти шифрмашины, как и другие, упомянутые ранее шифраторы, производились на заводе №707 в Свердловске. Для регламентации работы данной аппаратуры вскоре после 22 июня 1941 г. был издан Приказ НКО №0095 о засекречивании передач по аппарату «Бодо».

В 1937 г. в черноморском санатории И.П. Волосок познакомился с молодым офицером-шифровальщиком М.С. Козловым и, почувствовав в нем талант конструктора, предложил продолжить службу в лаборатории 8-го отдела Генштаба РККА. Под общим руководством И.П.Волоска новый образец шифрмашины М-101 (рис. 8.1) создавался ведущим конструктором Н.М. Шарыгиным, а некоторые её механизмы изобрел и разработал лично М.С.Козлов. М-101 состояла уже из двух основных узлов, была уменьшена по габаритам более чем в 6 раз и по весу более чем в 2 раза. Машина получила название М-101»Изумруд» и стала производиться параллельно с «В-4», начиная с 1940 г. [Дадуков, 2006-3].

Следует отметить, что советские конструкторы располагали образцами зарубежных электромеханических шифрмашин, в частности такими, как В-211 (рис. 8.2), разработанной знаменитым шведским криптографом Б. Хагелином в 1932 г.

В 1942 г. был издан приказ НКО №0093 о введении на снабжение частей связи приборов «Селектор», автоматически шифрующих телеграммы, передаваемые аппаратом «Бодо», авторам пока не удалось найти описание данного шифратора.

За создание и внедрение шифровальной машины М-101 («Изумруд») в 1943 г. И.П. Волоску, П.А. Судакову и В.Н. Рытову были присуждены государственные премии. Орденами были награждены Н.М. Шарыгин, М.С. Козлов, П.И. Строителев и Н.И. Гусев. Кроме того, И.П. Волоску была присвоена ученая степень «кандидат технических наук» (без защиты диссертации). В этом же году в войска было отправлено свыше 90 комплектов М-101. [Николенко, 1998].

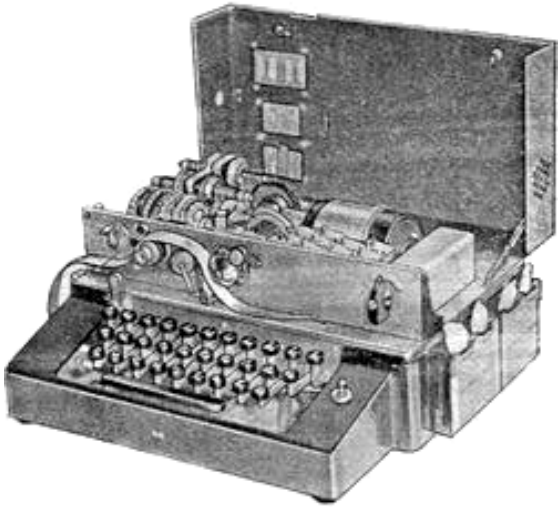


Рис. 8.1. **Шифрмашина М-101**

Рис. 8.2. **Электромеханическая шифрмашина В-211 шведской фирмы «Aktibolaget Cryptoteknik» с русифицированной клавиатурой**

«Усилиями ведущих научных и инженерно-технических кадров страны в Институте №56 НКЭП к концу 1944 г. была практически завершена разработка устройства «Сова» – аппаратуры засекречивания сложной схемы с применением кодирования, которая предназначалась для закрытия ВЧ-каналов, образованных аппаратурой НВЧТ-42. Первые образцы другого типа засекречивающей аппаратуры такого же класса – «Нева» – были изготовлены и установлены на опытной связи Москва–Ленинград летом 1944 г. Аппаратуру «Нева», серийное производство которой было организовано на заводе №209, предполагалось использовать на всей сети правительственной связи, так как она сопрягалась со всеми типами каналообразующей аппаратуры ВЧ-связи. К третьему периоду войны относится и разработка сложного засекречивающего устройства «Волга-С», которому прочили большое будущее на стационарной сети правительственной связи» [Астрахан, 2001].

На машинную шифрсвязь в годы войны легла основная нагрузка при передаче секретных телеграмм. Только в 8-м управлении ГШ РККА за период с 1941 по 1945 годы было обработано свыше 1,6 млн шифртелеграмм и кодограмм. Порой нагрузка на шифрработников 8-го управления доходила до 1500 телеграмм в сутки. В штабах фронтов нормой считалась суточная нагрузка до 400 телеграмм, в штабах армии – до 60. Наряду с шифрами гаммирования применялись шифры многоалфавитной замены. За годы войны управлением шифровальной службы Генштаба (8-е управление ГШ) нижестоящим штабам и войскам разослано порядка 3,2 млн комплектов шифров.

За время Великой Отечественной Войны «Курсы усовершенствования командного состава шифрслужбы» и учебные команды фронтов и военных округов подготовили и отправили на фронт более 5 тыс. специалистов-шифровальщиков. К концу 1944 г. в 130 шифрорганах Красной Армии имелась на вооружении та или иная шифровальная и кодировочная машина, а к исходу войны в эксплуатации уже находилось 396 комплектов техники специальной связи. Специалисты-шифровальщики с честью справились с возложенными на них задачами, обеспечи-

вая машинной шифрсвязью Ставку ВГК, Генеральный штаб, управления Наркомата обороны, Тегеранскую, Ялтинскую и Потсдамскую конференции.

Офицеры-конструкторы 8-го Управления ГШ в годы войны занимались не только созданием новых образцов шифртехники. Внедрение ее в войска, обучение работе – вот, пожалуй, было их основным занятием. Конструктор М.С. Козлов за военные годы был командирован на фронт 32 раза! А рано утром, 9 мая 1945 г., получив срочное предписание госбезопасности и Генштаба РККА, убыл самолетом «Дуглас» в Берлин для участия в работе комиссии по отбору и отправке в СССР наиболее ценного оборудования заводов и фабрик гитлеровской Германии по репарации. Только из Карлхорста и Потсдама для нужд мастерских по ремонту шифровально-кодировочной техники им было вывезено 3 вагона оборудования [Николенко, 1998].

С самого начала войны фашистские дешифровальщики пытались прочесть перехваченные советские криптограммы, зашифрованные машинными шифрами. Но все их попытки были тщетны! Пленные специалисты дешифровальной службы рассказывали, что наши криптограммы, зашифрованные машинными шифрами, были нечитаемы, и с 1942 г. они больше не перехватывались. Было ясно, что уникальная система машинного шифрования русских может быть уязвима только при наличии самой шифртехники и ключей к ней. Приказ Гитлера по вермахту от августа 1942 г. гласил: «кто возьмет в плен русского шифровальщика, либо захватит русскую шифровальную технику, будет награжден Железным крестом, отпуском на родину и обеспечен работой в Берлине, а после окончания войны – поместьем в Крыму». В исполнение гитлеровского приказа в 1942 г. вблизи от оккупированного фашистами Херсона, в Степановке, была организована разведывательно-диверсионная школа. Перед курсантами одной из спецгрупп ставилась задача: во что бы то ни стало добыть советскую шифровальную технику. Подробности деятельности этой группы неизвестны [Андреев, 2002].

К чести советских шифровальщиков следует отметить что, они были преданы своему делу! Есть немало примеров их

героизма в военные и послевоенные годы. Одними из первых войну на криптографическом фронте начали сотрудники советского посольства в Германии. Ранним утром 22 июня 1941 г., после того как стало известно о нападении немцев на СССР, на территории посольства стали разводить костры для уничтожения различной секретной документации, прежде всего шифров. Интересно отметить, что немецкие дипломаты в Москве начали уничтожение секретных документов и шифров еще в середине мая. Все это жгли во дворе посольства. Утром 21 июня в немецкое посольство в Москве поступил приказ из Берлина уничтожить последние шифры.

Настоящий подвиг совершил шифровальщик советского торгпредства в Берлине Николай Логачев. Уже утром первого дня войны эсесовцы проникли в здание торгпредства, Николай успел забаррикадироваться в шифровальной комнате и начал сжигать шифровальные документы, немцы буквально ломились в дверь, но мужественный шифровальщик продолжал работу, от дыма он потерял сознание, но все шифры были уничтожены. Когда немцам все же удалось взломать дверь, то все было кончено, и поживится советскими криптографическими секретами им не удалось. От отчаяния немцы сильно избили Логачева и бросили в тюрьму, впоследствии Н. Логачева вместе с другими советскими дипломатами обменяли на интернированных в СССР сотрудников немецких дипломатических представительств [Сопельняк, 2006].

Вот ещё ряд примеров времен Великой Отечественной Войны. Офицер спецсвязи Л. Травцев вёз секретные документы и шифры под охраной трёх танков и взвода пехоты. Колонна попала в засаду и за несколько минут была практически уничтожена. В автобус с шифрами и документами попал немецкий снаряд – Травцеву перебило обе ноги. Истекая кровью, шифровальщик нашёл в себе силы вскрыть сейфы, облить документы бензином и уничтожить их. Потом он ещё отстреливался, пока не сгорел вместе с подорванной машиной.

Младшего сержанта Е. Стемпковскую фашисты захватили на КП, где она дежурила у передатчика. Отважная радистка от-

стреливалась и успела бросить в нападавших немцев две гранаты, но силы были неравны. Стемпковскую схватили и подвергли пыткам. Фашистам не терпелось скорее доложить своему командованию, что они овладели кодовыми переговорными таблицами русских. Но их мечты были напрасны. Даже после того, как Елене отрубили обе руки, она ничего не сказала. Фашисты убили её. Посмертно Елене Константиновне Стемпковской было присвоено звание Героя Советского Союза [Ганин, 2001].

Люди этой профессии при жизни окружены тайной, а после смерти мало кто знает, что за подвиги они совершили. Традиции высокой ответственности шифровальщиков живы до наших дней. Так, в августе 2000 г. в списке погибших членов экипажа АПРК «Курск», составленном в штабе Северного флота, старший специалист спецсвязи (шифровальщик) гвардии старший мичман Игорь Ерасов назвался из соображений секретности помощником по снабжению. Очень образно описал особенности работы шифровальщиков военно-морского флота В. Пикуль в своем романе «Из тупика»: «Шифровальщик, живущий по соседству с салоном, казалось не подлежал карам уставным, а только небесным: случись «Аскольду» гибель, и он, обняв свинцовые книги кодов, должен с ними тонуть и тонуть, пока не коснётся грунта. И ляжет вместе с книгами мёртвый. Таков закон! Потому-то надо уважать человека, который каждую минуту готов к трудной и добровольной смерти на глубине. На той самой глубине, куда из года в год уносится пепел его шифровок…». Гвардии старший мичман Ерасов встретил смерть именно так. Впервые в шифровальной службе флота приоткрыли для «Красной звезды» завесу секретности и рассказали подробности его гибели. При разборе завалов на АПРК «Курск» в доке следственная группа прокуратуры нашла Ерасова там, где ему и положено было находиться – в третьем отсеке, в шифровальном посту, сидящим за рабочим столом. Он обнимал стоявшую на коленях металлическую шкатулку, в которую складывал для эвакуации кодовые таблицы и другие секретные документы…орден Мужества, которым его наградили посмертно, вручили родителям. Им же флот выделил квартиру [Гундаров].

Г.К. Жуков

Высоко отзывались о работе шифровальщиков в годы войны наши прославленные полководцы – Г.К. Жуков, А.М. Василевский, С.К. Тимошенко, С.М. Штеменко и многие другие. Некоторые цитаты по этому поводу будут приведены далее.

К сожалению, в начальный период войны у вступивших в бои советских войск были значительные проблемы со связью. Войсковая радиосвязь, средства ведения радиовойны не были достаточно развиты. В воспоминаниях крупных советских военачальников часто встречаются примерно такие высказывания: «средствами радиосвязи войска были обеспечены совершенно недостаточно», «проводная связь оказалась уязвимой и часто выходила из строя» и др.

Тяжелая ситуация со связью в войсках в начальный период войны усугублялась действиями противника. Сразу же после нападения на СССР 22 июня 1941 г. немцы развернули на территории нашей страны активную разведывательно-диверсионную деятельность. Целью немецких операций были, в том числе и советские линии связи. Вот как описывает ситуацию, сложившуюся в первые дни войны советский историк Ю.Б. Долгополов: «С самого начала войны диверсионные группы немцев, включаясь в проводные линии связи и используя свои рации, передавали командованию наших частей от имени вышестоящих советских командиров ложные приказы, вносящие дезорганизацию в управление войсками. Эта деятельность приняла столь широкое распространение, что СНК СССР 24.06.1941 г. принял специальное постановление по борьбе с диверсантами в прифронтовой полосе» [Долгополов, 1981]. О том же самом говорит в своих воспоминаниях и Г.К. Жуков: «Чуть позже нам стало известно, что перед рассветом 22 июня во всех западных приграничных округах была нарушена проводная связь… Заброшенные на нашу террито-

рию агентура и диверсионные группы разрушали проводную связь, убивали делегатов связи… Радиосредствами значительная часть войск приграничных округов не была обеспечена» [Жуков, 1971]. Далее Жуков отмечает частые нарушения связи, постоянное запаздывание сведений. Даже Генеральный штаб не имел устойчивой связи с фронтами. В таких условиях руководить войсками было крайне трудно.

Но все же меры по обеспечению связи между руководством страны с фронтом постоянно принимались и совершенствовались, для этого наши связисты прилагали поистине героические усилия. Вот лишь несколько примеров.

Когда в конце 1941 г. Ленинград был блокирован немцами, остро встал вопрос о ВЧ связи с Ленинградским фронтом и городом. НК связи организовал связь по радио. Воспользоваться этой связью в полной мере не могли из-за отсутствия достаточного количества соответствующей шифровальной аппаратуры. Нужна была проводная линия. НК связи и НК обороны приняли решение в экстренном порядке проложить кабель по единственно возможному направлению – по дну Ладожского озера. Прокладка велась уже под обстрелом противника. В результате была организована проводная связь по воздушной линии с Ленинградом через Вологду на Тихвин, далее по кабелю до Всеволожской, затем опять по «воздушке» до Ленинграда. Ставка всю войну имела с Ленинградом устойчивую ВЧ-связь.

К лету 1942 г. немцы оправились после поражения под Москвой, началось наступление на Южном направлении. Был создан Воронежский фронт. В населенном пункте Поворино были развёрнуты работы по монтажу узлов и организации связи. Немцы бомбили Поворино ежедневно. Во время бомбежки связисты и криптографы скрывались в ближайшем овраге, а потом вновь продолжали работы. Вот что вспоминает один из офицеров-связистов П.Н. Воронин: «Однажды, вернувшись из укрытия, увидели догорающие обломки зданий, где мы разместили наши узлы. Погибло и все оборудование. Нашлись «когти» и телефонный аппарат. Влезли на столб с

сохранившимися проводами. А.А. Конюхов и я доложили своим руководителям о случившемся. Но к этому времени обстановка изменилась и ВЧ связь развернули в деревне Отрадное, куда вскоре переместился и штаб фронта. Вскоре мне было приказано срочно выехать в Сталинград» [strf].

В Сталинграде сложилась очень тяжелая обстановка. Все основные линии связи Москвы со Сталинградом шли по правому берегу Волги. После того, как немцы вышли на ее берег выше Сталинграда, в местечке Рынок, и ниже Сталинграда, в районе Красноармейска, город оказался в окружении. 23 августа 1942 г. немцы произвели массированный налет. Весь город горел. Связисты НК связи в тяжелейших условиях вывезли все оборудование междугородной станции на левый берег и смонтировали резервный узел в местечке Капустин Яр, с выходом на Астрахань и Саратов. В Сталинграде действующих линий связи не осталось. Штаб Сталинградского фронта был на правом берегу. Связь с ним можно было организовать только с левого берега. ВЧ станция Сталинграда также была вывезена на левый берег в местечко Красная слобода. Было получено указание тянуть проводную линию через Волгу.

В первую очередь проверили, нельзя ли использовать имеющийся кабельный переход в районе Рынка. Подъехать к кабельной будке было сложно – немцы контролировали все подходы. И все же наши связисты добрались до неё и проверили исправность кабеля. Он работал, но на другом конце отвечали немцы. Использовать этот кабель было нельзя. Оставался один выход – прокладывать новый кабельный переход через Волгу. Речного кабеля не было, решили класть полевой кабель ПТФ-7, не приспособленный для работы под водой (замокал через 1–2 суток). Позвонили в Москву, чтобы срочно прислали речной кабель. Прокладку приходилось вести под непрерывным минометным обстрелом. Большой вред наносили плывущие по реке нефтеналивные баржи. Пробитые снарядами, они плыли по течению, постепенно погружаясь в воду, и перерезали кабели. Каждый день приходилось класть все новые и новые пучки. Коммутатор ВЧ связи был установ-

лен в блиндаже, где размещалось командование фронта. На этот коммутатор связь по проводам передавалась с ВЧ станции, находящейся на левом берегу. Наконец, прибыл речной кабель. Барабан весил больше тонны. Подходящей лодки не нашлось. Сделали специальный плот. Ночью начали прокладку, но немцы засекли проведение работ и минометным огнем разбили плот. Пришлось начинать все сначала. Наконец кабель был проложен. До ледостава он работал надежно. Позднее, в дополнение к нему, по льду проложили и воздушную линию. Столбы вмораживали в лед. В феврале 1943 г. немцы были разгромлены. Связь со Сталинградом начала работать по довоенной схеме [strf].

Постоянно принимались меры по сохранению секретности передаваемой информации. Уже в первые минуты войны один из советских передовых постов передал командованию открытым текстом: «Нас обстреливают. Что нам делать?». Ответ пришел незамедлительно «Вы с ума сошли! Почему ваше сообщение не зашифровано?» [Кан, 2004]. На третий день войны, 24 июня, была издана директива НКГБ СССР о задачах органов безопасности в условиях военного времени и, в частности, об особой сохранности шифров, совершенно исключающей попадание их в руки врага [strf].

Поскольку техники засекречивания радиотелефонов в действующей армии было крайне мало, то «все приказания передавались открытой командой по заранее закодированной карте. Населенные пункты, лощины, бугры – все артерии местности были заранее помечены условными номерами, и немцы ничего не могли понять» [Ваупшасов, 1971]. К сожалению, проблемы со связью, которые возникали в довоенное время, не были разрешены до начала войны, хотя проблема обсуждалась на самом высоком уровне. Однако в дальнейшем в ходе боевых действий безопасности связи стало уделяться гораздо больше внимания и ситуация с организацией связи, обеспечения средствами связи значительно улучшилась.

Хотя, как было сказано ранее отечественные шифрмашины активно и эффективно использовались на фронте, основным

видом шифрования для большинства советских военных были ручные шифры. Наиболее распространенной системой шифрования советских вооруженных сил во время Второй мировой войны были коды с перешифровкой [Кан, 2004].

Впервые в СССР стойкая система шифрования с одноразовой гаммой была разработана в начале 1920-х гг. Активное применение одноразовой гаммы в дипломатической переписке началось с 1927 г. [Гольев, 2008]. Несколько позже одноразовая гамма стала применятся для перешифровки кодов в Красной Армии и советских спецслужбах.

Во время Великой Отечественной Войны советские шифровальные службы обеспечили секретность наших сообщений, не позволили противнику получить сведения о наших замыслах и действиях, «… советская шифровально-кодировочная аппаратура в военный период сыграла особую роль, поскольку именно ее использовали на важнейших направлений скрытой связи. Именно она обеспечивала возможность оперативного закрытия важнейшей стратегической и оперативно-стратегической информации от противника» [Дадуков, 2006-5]. Приведем еще одну цитату о роли советской шифртехники во Второй мировой войне: «Созданная в предвоенные годы отечественная шифровальная техника в процессе Великой Отечественной Войны держала свой первый по – настоящему серьезный экзамен на зрелость. Огромные ресурсы были вложены в эту войну, длившуюся четыре долгих года, и вместе со страной криптографическая военная служба прошла столь же непростой путь от поражений в начале войны до решающей победоносной фазы, повернувшей врага вспять. Советская криптография, сумевшая скрыть от врага наши стратегические планы, но раскрывшая многие намерения врага, внесла в Победу свой весомый вклад» [Дадуков, 2006-6]. Надо отметить, что ни одна советская шифрмашина не была взломана противником, хорошей стойкостью отличалась и значительная часть наших ручных шифров. А теперь приведем оценки работы советских шифровальщиков прославленных полководцев Великой Отечественной. Г.К. Жуков: «Хорошая работа

шифровальщиков помогла выиграть не одно сражение» [Жуков, 1971], А.М. Василевский: «Ни одно донесение о готовящихся военно-стратегических операциях нашей армии не стало достоянием фашистских разведок» [Василевский, 1978]. Маршал Василевский отмечал: «Будучи начальником Генерального штаба, я ни одной минуты не мог обойтись без ВЧ-связи, которая, Благодаря высокой сознательности и мастерству воинов-связистов, наилучшим образом обеспечивала оперативное руководство действующими фронтами и армиями» [Василевский, 1978]. А командующий 1-м Украинским фронтом маршал И.С. Конев так оценивал роль правительственной связи: «Надо вообще сказать, что эта связь ВЧ, как говорится, нам была Богом послана. Она так выручала нас, была настолько устойчива в самых сложных условиях, что надо воздать должное нашей технике и нашим связистам, специально обеспечивавшим эту связь ВЧ и в любой обстановке буквально по пятам сопровождавших при передвижении всех, кому положено пользоваться этой связью». Еще одну оценку значения правительственной связи дал маршал И.Х. Баграмян: «Без ВЧ-связи не начиналось и не проводилось ни одно значительное военное действие. ВЧ-связью обеспечивались не только штабы, но и командование непосредственно на передовых линиях, на дозорных пунктах, плацдармах. В Отечественной войне ВЧ-связь сыграла исключительную роль как средство управления войсками и способствовала выполнению боевых операций» [Баграмян, 1950].

Оценили надежность наших шифров и представители противника, так начальник штаба при ставке верховного главнокомандования немецких вооруженных сил генерал-полковник А. Йодль в своих показаниях на допросе 17 июня 1945 г. сообщил: «Основную массу разведданных о ходе войны – 90 процентов – составляли материалы радиоразведки и опросы военнопленных. Радиоразведка – как активный перехват, так и дешифрование – играла особую роль в самом начале войны, но и до последнего времени не теряла своего значения. Правда, нам никогда не удавалось перехватить и расшифровать радиограммы вашей (советской – *авт.*) ставки, штабов фронтов и армий.

Радиоразведка, как и все прочие виды разведок, ограничивалась только тактической зоной» [Йодль, 2001], а вот что говорил на одном из совещаний А. Гитлер: «Эти проклятые русские шифровальные машины, мы никак не можем их расколоть!» [Дадуков, 2006-6].

8.3. Дешифровальная служба

Огромный вклад в победу внесли советские радиоразведчики и криптоаналитики в ходе Великой Отечественной Войны. Накануне войны наши дешифровальщики предупредили руководство страны о нападении Германии. Сотрудники органов государственной безопасности и пограничники неоднократно докладывали руководству страны информацию, содержавшуюся в дешифрованной переписке ответственных деятелей Италии, Турции, Японии, о сроках нападения Германии на СССР [Сыромятников, 2001]. Например, весьма ценные сведения были получены из дешифрованной дипломатической переписки Японии. В начале июня 1941 г. нашими спецслужбами были дешифрованы телеграммы японского представителя в Кенигсберге японскому послу в Москве о военных приготовлениях немцев в Восточной Пруссии. В первой из них сообщалось: «В течении последней недели из Мемельского порта (ныне город Клайпеда на территории Литвы, в описываемое время принадлежал Германии – *авт.*) была направлена в Финляндию часть расположенных в Мемельской области войск… в этом районе происходит их концентрация… пассажирский поезд, который вышел из Берлина утром 29 мая и прибыл сюда в тот же день вечером, на пути разминулся с 38 порожними воинскими составами. Военные перевозки по линии Познань – Варшава проходят более оживленно, чем в этом районе… 30 мая мною замечено, что между всеми пунктами восточнее Кенигсберга проведен телефон… Все это наводит на мысль о начале войны» [Сыромятников, 2001]. 10 июня 1941 г. из данного источника была получена

следующая информация: «Выехав утром 9-го числа из Берлина в Кенигсберг, мы по пути перегнали шедшие в восточном направлении 17 воинских составов, 12 составов с мотомехчастями, 3-с танками, 1-с полевой артиллерией и 1-с санитарными частями» [Сыромятников, 2001].

Ценнейшая информация была получена из дешифрованных сообщений представителей союзников Германии в столице Финляндии Хельсинки. Из переписки посольства Японии: «Учитывая обстановку, существующую здесь (завершение всеобщей мобилизации) я сжег нижеследующие документы…» (идет их перечень) [Сыромятников, 2001]. А вот что сообщает итальянский посол 19 июня 1941 г.: «Объявленная тайно всеобщая мобилизация здесь уже завершена. Страна находится на военном положении. Продолжается прибытие крупных соединений вооруженных сил Германии, включая авиационные части. Считается, что Германия немедленно примет решение в отношении СССР» [Сыромятников, 2001].

Важная информация поступала из столицы Румынии Бухареста, так за два дня до нападения немцев была дешифрована телеграмма, отправленная в Токио послом Японии: «Обстановка вошла в решающую фазу развития. Германия полностью завершила подготовку от Северной Финляндии и до южной части Черного моря, закончила формирование и вооружение по штатам военного времени 154 дивизии, предназначенные для нападения на СССР, и уверена в молниеносной победе. Румыния также ведет подготовку к тому, чтобы выступить на стороне Германии» [Сыромятников, 2001]. Практически одновременно японский посол в Бухаресте, обладавший большими связями сообщил о скором начале войны послу Страны Восходящего Солнца в Москве: «Утром 20 июня германский посланник сказал мне доверительно… Германия полностью завершила подготовку к войне от Северной Финляндии и до южной части Черного моря и уверена в молниеносной победе» [Сыромятников, 2001]. Весьма интересные сведения имелись и в шифрпереписке нейтральных (на тот момент) государств, в качестве примера приведем телеграмму

от 3 июня 1941 г. из Бухареста в Госдепартамент США: «Фельдмаршал фон Лист, специалист по ведению «молниеносной» войны, находится, как говорят, в районе расположения германских войск в Молдавии» [Сыромятников, 2001].

Вот еще одно сообщение, полученное советскими специалистами в мае 1941 г.: «Генералы германской армии производят рекогносцировку вблизи границы: генерал Рейхенау – в районе местечка Ульгувек 11 мая, 13 мая генерал с группой офицеров в районе Белжец… 23 мая в районе Радымно» [Сыромятников, 2001].

К сожалению, эту информацию, как и сообщения на эту тему из других источников советское руководство должным образом не оценило. Приведем без комментариев лишь высказывание маршала А. Василевского: «В чем причины столь крупного просчета этого опытного и дальновидного государственного деятеля (Сталина – *авт.*) Прежде всего в том, что наши разведорганы, как справедливо отмечает в своих воспоминаниях Г.К. Жуков, не смогли в полной мере объективно оценивать поступавшую информацию о военных приготовлениях фашистской Германии и честно, по-партийному, докладывать ее И.В. Сталину. Я не буду касаться всех аспектов такого положения, они в основном известны. Остановлюсь лишь на том, что в этом, видимо, сыграла свою роль и некоторая обособленность разведуправления от аппарата Генштаба. Начальник разведуправления, являясь одновременно и заместителем наркома обороны, предпочитал выходить с докладом о разведданных непосредственно на Сталина, минуя начальника Генштаба. Если бы Г.К. Жуков был в курсе всей важнейшей развединформации... он, наверное, смог бы делать более точные выводы из нее и более авторитетно предоставлять эти выводы И.В. Сталину и тем самым в какой-то мере повлиять на убеждение И.В. Сталина, что мы в состоянии оттянуть сроки начала войны, что Германия не решится воевать на два фронта – на Западе и на Востоке» [Василевский, 1978].

Большой вклад советские дешифровальщики внесли в победу под Москвой, «… уже в первые дни войны Б.А. Арон-

ским (с помощью своих помощников и переводчиков) были дешифрованы кодированные донесения послов ряда союзных Германии стран в Японии. По поручению Императора Японии послы докладывали своим правительствам о том, что Япония уверена в их скорой победе над Россией, но пока сосредоточивает свои силы на юге Тихого океана против США (а ведь эта война тогда еще даже не началась!). Аналогичные сведения были получены С.С. Толстым путем дешифрования переписки линий связи высших эшелонов власти Японии» [Кузьмин, 1998-1]. В качестве примера приведем сообщение, отправленное 27 ноября 1941 г. из Токио в посольство в Берлине, дешифрованное советскими специалистами: «Необходимо встретиться с Гитлером и тайно разъяснить ему нашу позицию в отношении Соединенных Штатов. Объясните Гитлеру, что основные усилия Японии будут сконцентрированы на юге (против США и Англии – Б.А. и А.П.) и что мы предполагаем воздержаться от серьезных действий на севере (против СССР – Б.А. и А.П.)» [Анин, 1996]. Эта информация была подтверждена и другими источниками, в частности, донесениями нашего знаменитого разведчика Р. Зорге. Таким образом, руководство СССР убедилось, что Япония в ближайшее время не нападет на нашу страну и пошло на переброску войск с Дальнего Востока и из Сибири. Именно эти соединения сыграли решающую роль в ходе победоносного наступления. В предвоенные годы Сергей Семенович Толстой возглавлял японский отдел дешифровальной службы НКВД. Одним из самых крупных успехов накануне войны было дешифрование группой специалистов во главе с Толстым японских шифрмашин, известных под названиями, данными им американцами «оранжевая», «красная» и «пурпурная» [Кузьмин, 1998-1].

В довоенные годы Ставка Верховного Главнокомандующего приняла решение о создании радиодивизионов особого назначения (ОСНАЗ). Они входили в состав Главного разведывательного управления (ГРУ) Генштаба Красной Армии и во время войны вели перехват открытых и шифрованных сообщений немцев и их союзников в прифронтовой полосе, за-

нимались пеленгацией вражеских передатчиков, создавали радиопомехи, участвовали в операциях по дезинформации противника. В каждом батальоне было от 18 до 20 приемников перехвата и 4 пеленгатора. Подготовка персонала для этих подразделений началась в 1937 г. в Ленинграде. Этим занимались на инженерном радиотехническом факультете Военной электротехнической академии связи имени С.М. Буденного. В июле 1941 г. первые выпускники этого потока были эвакуированы в Подмосковье, где был создан специальный учебный центр. Вот что вспоминает один из бывших руководителей советской радиоэлектронной разведки генерал-лейтенант П.С. Шмырев: «В учебном центре изучали организацию радиосвязи в немецко-фашистской армии, в пределах того, что знали сами преподаватели. Тренировались в приеме на слух, изучали общевойсковые дисциплины» [Бурнусов, 2009]. К сожалению, с основной части операций этих подразделений до сих пор не снята завеса секретности. Сведений об этих операциях очень мало, но некоторые факты авторам удалось найти. Так на Ленинградском фронте действовали 472, 345 и 623 отдельные радиодивизионы (орд) ОСНАЗ. 623 орд ОСНАЗ с 1942 г. вел радиоразведку на Карельском перешейке. К концу 1942 г. советскими специалистами была полностью выявлена сосредоточенная здесь группировка противника. Удалось определить количество соединений Германии и Финляндии и места их дислокации, аэродромы базирования финских ВВС и частей люфтваффе в Финляндии, Норвегии, а также расположенных в полосе действия войск Ленинградского фронта. Специалисты дивизиона своевременно сообщали в разведотдел штаба Ленинградского фронта о налетах вражеской авиации [Бурнусов, 2009]. Успешно продолжал работу 623 орд ОСНАЗ и в последующие годы войны. Приведем цитату из боевого отзыва разведотдела 7-й армии от 6 июля 1944 г.: «Группа радиоразведчиков 623-го отдельного радиодивизиона на Свирском направлении за время работы и особенно в период начала наступательных операций дала много ценного материала о противнике. Личный состав группы с большой ответственностью отнесся к выполнению поставленных группе задач…» [Бурнусов, 2009]. А вот что сказано в боевом

отзыве штаба 21-й армии Ленинградского фронта за период с июня по сентябрь 1944 г.: «623-й отдельный радиодивизион в период всей операции на Карельском перешейке обеспечивал ценными данными штаб армии и в значительной степени помог вскрыть группировку финнов в ходе наступления» [Бурнусов, 2009]. Специалисты дивизиона продолжали активно работать, руководству фронта поступали сведения о группировке финских войск, проводящихся перегруппировках и местонахождении штабов противника. Продолжали радиоразведчики информировать командование о предстоящих вылетах авиации противника. «По результатам хорошей работы дивизиона приказом командующего армии из числа личного состава дивизиона награждены правительственными наградами шесть человек» [Бурнусов, 2009].

Одним из них был Петр Спиридонович Шмырев. Весь труднейший период блокады он находился в Ленинграде и на позициях войск, оборонявших город на Неве, принимая активное участие в организации радиоразведки сетей связи противника на всех этапах битвы за Ленинград. Вот как его заслуги были оценены в наградном листе от 16 апреля 1944 г.: «При непосредственном участии П.С. Шмырева созданы ряд схем и конструкций, которые в значительной степени улучшили условия выполнения заданий командования фронта. Шмырев возглавил рационализаторскую работу в дивизионе, в результате чего многие образцы табельной аппаратуры модернизированы и в эксплуатации показали хорошие результаты. Много и успешно работает над аппаратурой, обеспечивающей непрерывность связи и управления в синхронной пеленгации. При непосредственном участии Шмырева восстановлен ряд образцов трофейной спецаппаратуры и создан аппарат собственной конструкции, на котором добыто большое количество ценных данных о противнике в период наступательных операций… За хорошие показатели в работе неоднократно имел благодарности от командования дивизиона и начальника РО штаба Ленинградского фронта. Достоин награждения орденом Красной Звезды» [Бурнусов, 2009].

В целях более эффективной организации радиоперехвата советское командование провело мероприятия по укрупнению частей радиоразведки, отдельные дивизионы были сведены в бригады. Так в сентябре 1944 г. инженер-капитан Шмырев был назначен в 97-й радиодивизион 1-й отдельной радиобригады ОСНАЗ Ставки Верховного главнокомандующего. До конца войны дивизион вел радиоразведку соединений сухопутных и военно-воздушных сил противника на южном направлении советско-германского фронта. Дивизион работал на территории Румынии, Чехословакии, Венгрии, Югославии, действуя в составе войск 2 Украинского фронта. «За этот период дивизионом была вскрыта дислокация более 100 аэродромов противника, на которых базировались свыше 40 частей ВВС Германии. Было зафиксировано более 30 тыс. самолето-вылетов боевой и транспортной авиации противника. Вскрыта дислокация 30 крупных войсковых штабов сухопутных войск. Успешной боевой работе способствовала четкая организация технического обеспечения, руководство которым осуществлял заместитель командира по технической части Петр Шмырев. Он был награжден орденом Красной Звезды, медалями «За боевые заслуги», «За оборону Ленинграда», «За взятие Будапешта», «За освобождение Белграда», «За победу над Германией в Великой Отечественной Войне 1941–1945 гг.»» [Бурнусов, 2009].

Теперь рассмотрим результаты деятельности дешифровально-разведывательной службы (ДРС) Главного морского штаба в годы Великой Отечественной войны. В образованном 30 декабря 1937 г. Наркомате ВМФ в Управлении разведки было создано 7-е отделение (в дальнейшем 11-й отдел), в задачу которого входила организация и руководство дешифровальной работой. Подготовка флотских криптоаналитиков осуществлялась на криптографических курсах, организованных при Академии Генштаба РККА. В мае 1939 г. и феврале 1941 г. на флот было направлено свыше 40 специалистов, которые стали ядром ДРС во время Великой Отечественной войны. Весьма незначительная по численному составу, не превышающему 150 человек ДРС ВМФ СССР показала очень

хорошую результативность и эффективность. Эта служба непрерывно выдавала достоверные разведывательные данные самого разнообразного содержания, в том числе и стратегического значения. Объектами разведки стали не только собственно морские силы Германии и ее союзников, но также и приморские группировки сухопутных войск, и в первую очередь авиации – главной ударной силы немцев в войне против СССР. Всего морскими дешифровальщиками было вскрыто более 300 кодов и шифров Германии, ее союзников и нейтральных государств и прочитано несколько сот тысяч радиограмм. Следует отметить, что управление немецкой авиацией и легкими силами немецкого флота практически полностью контролировалось нашими криптоаналитиками. Очень помогала «болтливость» союзников Германии, «оповещающих свое командование о стратегических планах, тщательно скрываемых самими немцами. А также феноменом ведомственности, когда сохраняется «своя» тайна, а «чужими» секретами пренебрегают. Так, из переписки авиации подчас становилось известно о предстоящих операциях сухопутных войск, для обеспечения которых предпринимались те или иные акции ВВС. Успешному раскрытию любых шифросистем сопутствовал не только каждодневный упорный труд, но и аналитическое осмысливание происходящих изменений и их динамики, что позволяло в ряде случаев добиваться успеха там, где это, с точки зрения теории, казалось невозможным» [Куличенко, 2004].

Рассматривая работу военно-морских дешифровальщиков каждого из флотов, видно, что например, специалистами ДРС Краснознаменного Балтийского флота (КБФ) только за период 1941–1943 гг. «было раскрыто 256 шифров и кодов Германии (направление возглавлял капитан-лейтенант Семенов) и Финляндии, благодаря чему прочитано 87362 криптограммы, а это около 100 сообщений в день. Чтение переписки береговых постов немецкой, финской и шведской служб наблюдения позволяло получать ценнейшие сведения о фарватерах, свободных для плавания, о минной, гидрографической и метеообстановке на Балтийском море, об интенсив-

ности движения судов и системе их защиты, что представляло первостепенный интерес для командования флота при планировании боевой деятельности подводных лодок и морской авиации» [Куличенко, 2004]. Так, 18 марта 1943 г. балтийские радиоразведчики получили сведения, что на аэродром Котлы прибыла группа немецких бомбардировщиков, это были Ju-88 из группы I/KG1 «Гинденбург». Штаб ВВС КБФ разработал операцию по уничтожению вражеских самолетов, 20–21 марта на Котлы произведено два налета советских штурмовиков. В результате по советским данным уничтожено 10 бомбардировщиков и 5 повреждено. 23 марта остатки группы были отведены на аэродром Дно, а 7 апреля отправлены на отдых и переформирование в Восточную Пруссию. Отметим, что криптоаналитики КБФ работали достаточно эффективно, при этом необходимо учесть, что находились они в блокадном Ленинграде. Шло накопление опыта, появилась возможность глубокого анализа шифров и кодов наших противников, исследование которых ранее не велось из-за недостатка сил и средств [Куличенко, 2004]. Благодаря воспоминаниям В.А. Круглова [Круглов, 1983], служившего в 1942–1945 гг. в 1 морском радиоотряде особого назначения КБФ можно подробнее рассказать о деятельности этого подразделения в годы войны. Вот что вспоминает ветеран: «Я служил в 1-м морском радиоотряде особого назначения, подчиненном Краснознаменному Балтфлоту. Отряд вел большую и ответственную работу, связанную с радиоперехватами, поиском вражеских каналов связи, их центров, объектов особой секретности и т. п. Своими средствами мы должны были искать и находить врага всюду: на суше, в воздухе и на море. В нашу обязанность входило прослушивание эфира на огромном театре действий, на всех доступных нам радиоволнах. Нашему разведрадиопункту пришлось побывать в составе нескольких фронтов: Ленинградского, 2-го и 3-го Прибалтийских. С 1944 г. мы входили в состав 2-й ударной армии и принимали активное участие в обеспечении командования важными радиосведениями, способствовавшими планированию боевых операций». Весьма ценные сведения специалисты 1 отряда ОСНАЗ КБФ получи-

ли при освобождении Прибалтики. «Нам, радистам-осназовцам, было известно, что наступление Ленинградского и Волховского фронтов перепутало все карты немецкой группы армий «Север». Уже с 14 января 1944 г. в эфире звучали (пока еще шифрованные) ее радиосигналы бедствия. По данным нашего радиоперехвата, командующий группой армий «Север» фельдмаршал фон Кюхлер поспешил 22 января на доклад к Гитлеру, который, однако, не дал ему разрешения отойти на лужские рубежи и к озеру Ильмень. Кюхлер был отстранен от командования, вместо него вступил в должность генерал-полковник В. Модель. А Модель, как сообщали радиоразведчики врага, без разрешения фюрера все-таки отвел свои войска к реке Луга. Таким образом, наступление 2-й ударной армии на правом крыле Ленинградского фронта отбросило левое крыло группы армий «Север» к Луге, что позволило нашей 42-й армии выйти к восточному берегу Чудского озера, а 67-й армии Ленфронта вместе с 54-й Волховского фронта освободить от врага окрестности Пскова. Форсировать с ходу реку Нарва – мощный оборонительный рубеж, именовавшийся в документах «Пантерой», – войска 2-й ударной армии не смогли. О сильных укреплениях этого рубежа сообщали радисты немецких объектов, а наши перехватчики передавали эти сведения в Центр. Поэтому был найден другой район переправы через реку – вблизи населенного пункта Усть-Жердянка. И в феврале воины 30-го гвардейского корпуса перешли Нарву, взломав укрепления противника в районе Долгой Нивы» [Круглов, 1983].

Интересную информацию удалось получить из радиоперехвата и дешифрования сообщений иностранных военных формирований, действовавших на стороне Германии. Стало известно, что в боевых действиях участвуют норвежцы (241-я пехотная дивизия, танковая дивизия «Норланд»), голландцы (танковая бригада «Нидерланды»), бельгийцы (моторизованная бригада «Валония»). Все они считались «добровольцами», но исполняли волю фашистов [Круглов, 1983]. Пропаганда немцев сообщала о многократном численном превосходстве немецких войск в Прибалтике, о наличии мощного вооруже-

ния, высоком моральном духе солдат, готовых отразить любой удар советских войск. Но, дешифруя немецкие перехваченные радиограммы, советские специалисты знали истинную картину, серьезно отличавшуюся от сообщений геббельсовской пропаганды [Круглов, 1983]. Снова обратимся к воспоминаниям В.А. Круглова: «С 22 сентября 1944 г., с момента освобождения Таллина войсками Ленфронта, наш радиоотряд вел перехват в районе всего побережья Балтийского моря. Радиоцентр находился под Таллином. Здесь же по заданию командования КБФ формировались подразделения перехвата и поиска, называемые «радиопунктами», «точками», которые направлялись на разные фронты. В марте 1945 г. сформированный в Эстонии радиопункт принимал участие в освобождении польской земли, обеспечивал связью командование 2-го Белорусского фронта и 1-й армии Войска Польского. В сложных условиях, идя буквально по пятам врага, радисты особого назначения неутомимо выполняли свою работу в боях при освобождении городов Данциг (Гданьск), Кольберг (Колобжек), Свинемюнде (Свинеусце), а также на территории Германии после форсирования реки Одер. В эти ответственные дни на основной линии перехвата мы несли круглосуточную вахту и, прослушивая позывные сотен различных радиостанций, помогали в обнаружении особой радиоточки, находившейся, как позже выяснилось, в ставке Гитлера, в Берлинской рейхсканцелярии. Теперь уже можно рассказать о том, как с помощью наших радистов особого назначения и польских связистов была осуществлена дерзкая операция, завершившаяся обнаружением и уничтожением фашистского линкора «Гнейссенау» (видимо имеется ввиду линкор «Гнейзенау» – *авт.*), пытавшегося уйти из Гданьском бухты с остатками разгромленных войск из группы армий «Север»» [Круглов, 1983]. Одним из существенных успехов радиоразведчиков КБФ стало обнаружение и уничтожение полигонов для запуска крылатых ракет ФАУ-1 и баллистических ФАУ-2 в Пенемюнде и Близене. «Полигоны для ФАУ создавались в обстановке строгой секретности. Фашисты надеялись, что успеют опробовать

это оружие. В апреле 1945 г., за месяц до окончания войны, Гитлер пытался запугать своих противников этим новым оружием, при помощи которого он хотел уничтожить сначала Англию, а затем отрезать советские войска от Берлина и повернуть вспять колесо войны. Оперативные действия радиоразведки, в том числе и наших разведчиков-радистов в содружестве с польскими группами Сопротивления, помогли вовремя обнаружить полигоны, и они были взорваны. Быстрое продвижение советских войск на всех фронтах, в особенности стремительное освобождение Польши и выход наших и польских войск на Одер, сыграло весьма существенную роль в последующем взятии Берлина. В этих блистательных победах есть частица труда и наших чекистов эфира, сделавших многое во имя великой Победы» [Круглов, 1983].

А вот что происходило на Черноморском театре военных действий. До начала войны Германия не имела сил флота и морских баз на Черном море. Поэтому основные усилия были направлены на Румынию и Турцию – тут и были достигнуты наиболее существенные результаты. «Главной задачей, поставленной перед ДРС Краснознаменного Черноморского флота (КЧФ), являлось добывание разведданных в интересах обеспечения обороны приморских баз и проведения противоблокадных действий, что имело исключительно важное значение для общего положения фланга армии и наших морских коммуникаций» [Куличенко, 2004]. 22 июня 1941 г. произошла смена большинства шифрсистем и ключей почти на всех контролируемых до этого каналах связи противника. Но героическая работа советских дешифровальщиков и их профессиональное мастерство дали свои результаты, уже 25 июня советские специалисты вскрыли новые шифры противника. Наиболее ценным источником информации явилась шифрпереписка румынского Генерального штаба со своей миссией связи при командующем группировкой немецких вооруженных сил на юге СССР фельдмаршале Манштейне. «В результате чтения переписки командование ЧФ имело исчерпывающую информацию не только о текущей боевой

обстановке, но и о некоторых стратегических замыслах врага. Вот несколько примеров полученной информации от криптографов ЧФ:

– боевые приказы о штурме Одессы, Севастополя, Новороссийска;

– планировавшееся направление главного удара в районе Курска в предстоящей летней кампании 1943 г.;

– подготовка покушения на глав правительств союзных держав во время предстоящей Тегеранской конференции;

– условия, при которых Турция вступит в войну с Советским Союзом;

– план увода (или уничтожения) румынского флота, разработанный немцами в связи с наступлением советских войск» [Куличенко, 2004].

Полученная дешифровальщиками КЧФ информация была высоко оценена высшим руководством нашей страны. Так летом 1942 г. Верховный главнокомандующий И.В. Сталин очень высоко оценил работу ДРС КЧФ, заявив: «Если бы не было разведки Черноморского флота, я не знал бы обстановки на Юге» [Куличенко, 2004]. При этом стоит отметить, что ДРС КЧФ не имела на вооружении даже элементарного оборудования для механизации трудоемких процессов криптоаналитической работы. Советские специалисты работали в прифронтовой полосе при постоянном боевом воздействии противника, в сложных бытовых условиях. Вот что вспоминает один из криптоаналитиков КЧФ Зайцев: «Устроились в недостроенном туннеле для аварийного спасения, пробитом между штольнями, отгородившись от внешнего мира брезентом; брезентовая же занавесь отделяла нас от Уманского (радист-перехватчик. – В.К.), первоклассного специалиста, не пропустившего ни одного донесения в Генштаб командующего румынским горно-стрелковым корпусом, вместе с немцами штурмовавшего город (Севастополь, июнь 1942 г.). ДРС ВМФ непрерывно выдавала достоверные разведывательные данные самого разнообразного содержания, в том числе и стратегического значения» [Куличенко, 2004].

Советская радиоразведка активно работала в Заполярье. Радиоперехват вели специальные береговые радиостанции, морские суда, в том числе и гражданские, полярные станции. Боевые задачи, поставленные перед дешифровально-разведывательной службой Северного флота (СФ), определялись целями, преследуемыми силами флота, кроме активной борьбы на морских коммуникациях противника приходилось осуществлять защиту наших внешних морских путей с Англией и США. Самый малочисленное (по сравнению с другими флотами) подразделение криптографов-североморцев (за всю войну через службу прошли всего 15 человек) в целом справилось со всеми задачами. Всего за годы войны вскрыто 9 кодов и 575 их вариантов, прочитано свыше 55000 криптограмм, исходящих от самолетов и авиабаз, что позволило контролировать закрытую переписку ВВС Германии. За годы войны было аналитическими методами раскрыто 26 шифров, 13 кодов, используемых силами береговой обороны, аварийно-спасательной, маячной и радионавигационной службами, и прочитано около 3000 криптограмм. При этом у криптологов нашего Северного флота, похоже, не было никаких подручных электромеханических и компьютерных средств, имевшихся в изобилии у их коллег по антигитлеровской коалиции. Только мозговые усилия... И огромное желание внести посильный вклад в разгром третьего рейха [Куличенко, 2004].

Особое внимание уделялось радиообмену немецких подводных лодок. Наши специалисты неоднократно фиксировали сеансы связи немецких подлодок и радиостанций, находящихся на территории СССР (радиостанции на немецких базах использовались не только для радиоперехвата, но и для управления действиями немецких субмарин). Обнаруживали следы работы немцев в советском Заполярье уже после окончания войны. Например, во время осмотра брошенного немецкого наблюдательного пункта на острове Вардропер (юго-восточная часть Карского моря) были найдены радиодетали и кусок антенны [Куличенко, 2004].

Для координаций действий немецких подлодок из, так называемых «волчьих стай», в 1943 г. у города Кальбе в Герма-

нии была построена первая в мире сверхдлинноволновая радиостанция «Голиаф». Радиоволны очень низкого «звукового» диапазона 3-30 кГц проходят сквозь Землю и могут проникать в морскую воду на глубины до 20 м. Подводная лодка, находящаяся гораздо глубже, может использовать буй с антенной на длинном буксируемом кабеле. Буй может находиться на глубине нескольких метров и не обнаруживается сонарами. Мощность передатчика была исключительно высокой – 1800 кВт, что в диапазоне 15-60 кГц обеспечивало связь с подводными лодками на расстоянии до 4000 км. Эффективная шифрованная связь (с использованием знаменитых шифраторов «Энигма») на таких расстояниях требовала передающих антенн исключительно больших размеров из-за огромной длины волны (только опоры для антенны представляли собой стальные трубы высотой 210 м). Эта станция позволяла связаться с подлодкой практически в любой точке мирового океана. По причине крайне высокой технической сложности таких антенн только СССР и США имеют передатчики крайне низких частот для связи с погруженными лодками. ВМС Великобритании предпринимали попытки построить свой передатчик в Шотландии, но проект был свернут.

В начале 1945 г. станцию «Голиаф» захватили американцы, но при разделе Германии на зоны влияния она отошла к Советскому Союзу. В 1946 г. станция была разобрана, а все оставшиеся на старом месте строения разрушены; 3 года трофей хранился на складах связи под Ленинградом, пока в 1949 г. не было принято решение о восстановлении станции в пойме реки Кудьмы в поселке Дружный Нижегородской области. Место установки было выбрано по двум причинам: из-за схожести здешних почв с немецкими, где станция стояла изначально (качество работы зависит от состояния почвы) и достаточной удалённости от границ. Все системы радиостанции были восстановлены за 3 года и 27 декабря 1952 г. она вышла в эфир. В начале 1960-х «Голиаф» был включён в систему наблюдения за космическими аппаратами. С 2001 г. бездействовала в связи с ремонтом. 30 сентября 2003 г. вновь встала на боевое

дежурство. Входит в сеть службы точного времени Бета [Информационная программа].

Важную информацию поставляла радиоразведка СФ поставляла летчикам, в частности передавались сведения о немецких самолетах подбитых нашими истребителями и упавших на территории противника. Вот один пример, 26 августа 1941 г. по результатам радиоперехвата переговоров немецких летчиков с наземной радиостанцией группе советских летчиков, в которую входил легендарный пилот, дважды Герой Советского Союза Б.Ф. Сафонов, было засчитано три сбитых немецких бомбардировщика Ju-88 [Марданов-1]. 30 мая 1942 г. советская радиоразведка перехватила немецкую радиограмму из района Петсамо (Финляндия), с приказом прекратить атаки на конвой PQ-16 и всем самолетам вернуться на базы. Конвой получил возможность спокойно продолжить путь. Это стало возможным благодаря успешной атаки советских истребителей, во главе с Борисом Сафоновым (который по радиосообщениям сбил три Ju-88), к сожалению, цена успеха была очень высока, в ходе вылета легендарный советский ас погиб [Марданов-2].

Полученная информация тщательно анализировалась разведкой Северного флота. В результате этих мероприятий удалось установить районы действия немецких подводных лодок. Маршруты конвоев стали прокладывать в обход опасных участков. При невозможности обогнуть опасный участок туда направлялись дополнительные противолодочные силы, и усиливалась охрана транспортных судов. Эти меры позволили существенно снизить потери наших судов от действий немецких подводников, а в некоторых случаях и уничтожить врага. В августе 1943 г. в предполагаемом районе действия немецких субмарин патрулировала советская подводная лодка С-101. Советские подводники обнаружили идущую в надводном положении немецкую лодку U-639 и потопили ее залпом трех торпед. На месте гибели U-639 среди плавающих обломков советские моряки обнаружили почти неповрежденную сигнальную книгу.

Успешная разработка непрерывно совершенствующихся документов скрытого управления противника оказалась воз-

можной благодаря самоотверженной аналитической работе дешифровальщиков, в первую очередь владеющих немецким языком, – капитан-лейтенанта Данилова и старшего лейтенанта Новохатского, которые мастерски использовали любую «зацепку», чтобы преодолевать все новые и новые ухищрения врага. Вклад небольшого, но дружного и целеустремленного, самоотверженно работавшего коллектива криптографов в общий ратный труд моряков-североморцев оказался весомым [sfinxclub].

Свой вклад в победу над Японией внесли и специалисты ДРС Тихоокеанского флота (ТОФ). Она начала свою работу в середине 1934 г. в Хабаровске. Криптоаналитики дальневосточных подразделений ДРС ВМФ добывали информацию, «необходимую для подготовки ударов, предопределивших сокрушительный разгром японских вооруженных сил на театре военных действий» [Куличенко, 2004].

Дивизионы ОСНАЗ внесли заметный вклад в победу под Курском. Накануне Курской битвы буквально за сутки до начала сражения наши криптоаналитики вскрыли шифрованный приказ Гитлера о наступлении. Перехватив радиограмму, связисты опознали почерк радиста ставки главнокомандующего противника, а по характеру передачи сделали вывод, что она содержит очень важный приказ. Дешифровальщики знали, что речь может идти о крупном наступлении и предположили, что в конце документа находится подпись Адольфа Гитлера. С помощью атаки «открытый-шифрованный текст» криптограмма была раскрыта. Она подтвердила информацию из других источников, в том числе и сообщения от нашего знаменитого разведчика Н. Кузнецова, назвавшего дату наступления немецких войск под Курском. Приказ Гитлера войскам гласил: «Этому наступлению придается решающее значение. Оно должно завершиться быстрым и решающим успехом...» [Жельников, 1996]. Для проведения операции, на флангах Курского выступа были сосредоточены 50 дивизий, 10000 орудий, 2700 танков и свыше 2000 самолетов. В дешифрованном приказе указывалось, что наступление начнется утром. Не верить этой информации было нельзя. Поэтому в 2 ч 20 мин советские войска начали ар-

тиллерийскую контрподготовку, которая причинила немцам, сосредоточенным на исходных рубежах, значительные потери. В ходе грандиозного сражения враг был разгромлен потеряв большое количество живой силы и техники. Так, например, из-за больших потерь ВВС, понесенных под Курском. Германия вынуждена была впредь почти полностью отказаться от действий своей авиации по объектам нашего глубокого тыла. При этом источник информации очень сильно скрывался. Успех криптографов стал одним из значительных факторов, приведших к победе под Курском. Однако о роли криптографов в победе под Курском до сих пор говорили лишь в очень туманных выражениях. Так, маршал А.М. Василевский в своей статье «Историческое сражение», написанной для газеты «Правда» от 04.07.1968 г., отметил роль неких «важнейших разведывательных данных» [Жельников, 1996]. А вот еще одна оценка Василевского роли разведки перед Курской битвой: «В этот ответственный момент советское командование предъявляло особые требования к органам разведки. И нужно сказать, она была на высоте и неплохо помогала нам. В первые два года войны мы, руководители Генштаба, не раз выслушивали справедливые упреки Верховного Главнокомандующего в адрес Разведывательного управления. В 1943 г. таких замечаний почти не было. Как ни стремился враг держать в тайне планы своего наступления, как ни старался отвлечь внимание советской разведки от районов сосредоточения своих ударных группировок, нашей разведке удалось определить не только общий замысел врага на летний период 1943 г., направление ударов, состав ударных группировок и резервов, но и установить время начала решительного наступления» [Василевский, 1978]. Другой участник подготовки битвы под Курском, маршал Г.К. Жуков, в своих мемуарах привел блестящий пример того, как можно делиться воспоминаниями, ничего по сути дела не рассказывая: «Стало известно, что сведения, полученные в тот день от захваченного пленного солдата 168-й пехотной дивизии, о переходе противника в наступление на рассвете 5 июля, подтверждаются...» [Жуков, 1971].

Интерес для советских радиоразведчиков и криптоаналитиков во время войны представляли и шифрованные сообщения союзников. Так наши специалисты достигли существенных успехов в дешифровании английской переписки. Так перебежавший к англичанам в августе 1945 г. заместитель резидента ИНО НКГБ в Турции К. Волков сообщил, что все английские сообщения на линии связи Лондон-Москва в течении 2,5 лет дешифровывались в СССР [Анин, 1996].

Подведем итоги. В ходе войны советские дешифровальные службы предоставили политическому и военному руководству СССР большое количество важнейшей информации. Эта информация поступала во время всех важнейших сражений (в том числе битвы за Москву, Сталинградской битвы, сражения на Курской дуге и др.) и способствовала нашим победам. Советские криптоаналитики вскрывали ручные и машинные шифры иностранных государств. В годы войны удалось дешифровать ряд немецких шифраторов (но не «Энигму»). Приведем оценку их работы данную бывшим Генеральным директором ФАПСИ генералом А.В. Старовойтовым: «Нам была доступна информация, циркулирующая в структурах Вермахта (почти вся!). Я полагаю, нашим маршалам была оказана существенная помощь в достижении перелома в ходе войны и, наконец, окончательной победы. Наши полевые центры дешифрования работали весьма успешно. Войну в эфире мы выиграли» [Кузьмин, 1998-1]. А вот как оценивает деятельность советских специалистов в годы войны П.С. Шмырев: «… Я часто вспоминаю Великую Отечественную Войну. Помню себя и своих товарищей – радиоразведчиков 1941 г., когда мы мало знали и еще меньше умели. И вспоминаю их же и себя в 1943–1944 гг., когда радиооператоры знали по почерку чуть ли не всех немецких радистов, определяя по ним номера дивизий, корпусов, армий. Любая задача нашим радиоразведчикам была по плечу».

Список рекомендуемой литературы

1. Андреев А. Именно у нас в городе тайное становилось явным // Гривна. – 2002. – № 48(412). – с. 28.
2. Анин Б.А. Радиоэлектронный шпионаж. – М.: ЗАО Изд-во Центрполиграф, 2000. – 493 с. ISBN 5-227-00659-8.
3. Астрахан В.И., Гусев В.В., Павлов В.В., Чернявский Б.Г. Становление и развитие правительственной связи в России. – Орел: ВИПС, 1996.
4. Баграмян И. Так начиналась война. – М., 1950.
5. Басин Я.З. И творцы, и мастеровые. – Минск: Вышэйшая школа, 1984.
6. Бурнусов И. Мэтр радиоэлектронной разведки // Независимое военное обозрение. – 2009. – №35. – с. 15.
7. Василевский А. Дело всей жизни. – М., 1978.
8. Ваупшасов С.А. На тревожных перекрестках. – М.: Издательство политической литературы, 1971.
9. Востоков К. Предупредить нападение // Независимое военное обозрение. – 2001. – №25. – с. 7.
10. Востоков К. Разведка слушает эфир // Независимое военное обозрение. – 2001. – №46. – с. 7.
11. Ганин В. 80 лет назад создана шифровальная служба. // Северный курьер. – 2001.– №87(23903). – www.dizzaster.ru.
12. Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П. Криптография: страницы истории тайных операций. – М.: Гелиос АРВ, 2008.
13. Гундаров В. «Под грифом особой важности». – Режим доступа: www. redstar.ru (сайт газеты «Красная Звезда»).
14. Дадуков Н.С., Репин Г.А., Скачков М.М., Филин Ю.П. Советская шифровальная техника. Ленинградский период: 1935–1941. Ч. 1. Истоки. // Защита информации. INSIDE. – 2006. – №1. – с. 91–96.
15. Дадуков Н.С., Репин Г.А., Скачков М.М., Филин Ю.П. Советская шифровальная техника. Ленинградский период: 1935–1941. Ч. 2. Пролог. // Защита информации. INSIDE. – 2006. – №2. – с. 83–87.

16. Дадуков Н.С., Репин Г.А., Скачков М.М., Филин Ю.П. Советская шифровальная техника. Ленинградский период: 1935–1941. Ч. 3. Комбинат техники особой секретности. // Защита информации. INSIDE. – 2006. – №3. – с. 93-96.
17. Дадуков Н.С., Репин Г.А., Скачков М.М., Филин Ю.П. Советская шифровальная техника. Ленинградский период: 1935–1941. Ч. 4. Расширение номенклатуры шифровальной техники. // Защита информации. INSIDE. – 2006. – №4. – с. 92–96.
18. Дадуков Н.С., Репин Г.А., Скачков М.М., Филин Ю.П. Советская шифровальная техника. Ленинградский период: 1935–1941. Ч. 5. Накануне. // Защита информации. INSIDE. – 2006. – №5. – с. 75-79.
19. Дадуков Н.С., Репин Г.А., Скачков М.М., Филин Ю.П. Советская шифровальная техника. Ленинградский период: 1935–1941. Ч. 6. Первый экзамен выдержан! // Защита информации. INSIDE. – 2006. – №6. – с. 85–89.
20. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1996.
21. Жуков Г.К. Воспоминания и размышления. – М., 1971.
22. История средств защиты информации. – Режим доступа: http://www.referent.ru:2003/nvk/forum/archive/61/61100
23. Йодль А. «Война с Россией – это такая война, где знаешь как начать, но не знаешь чем она кончится» // Сигары Шееле для «Барона Дризена». – М.: Издательский дом «Гелеос», 2001. – с. 89–106.
24. Калачев К.Ф.. В круге третьем. – М., 1999.
25. Кан Д. Война кодов и шифров. – М.: Рипол Классик, 2004.
26. Клепов А. Информационное оружие Сталина. – Режим доступа: http://www.proza.ru/go/www.proza.ru/2009/06/17/949
27. Круглов В.А. Чекисты эфира // Вторая ударная в битве за Ленинград. – Л.: Лениздат, 1983. Использован текст, размещенный на сайте «Ленинград Блокада Подвиг».
28. Кузьмин Л.А. Не забывать своих героев // Защита информации. Конфидент. – 1998. – №1. – с. 83–85.

29. Кузьмин Л.А. ГУСС – этап в развитии советской криптографии // Защита информации. Конфидент. – 1998. – №4. – с. 89–94.
30. Куличенко В. Русские против «Энигмы» // Независимое военное обозрение. – 2004. – №40. – с. 7.
31. Лекарев С., Порк В. Радиоэлектронный щит и меч // Независимое военное обозрение. – 2002. – №2. – с. 7.
32. Марданов А. Может хватит бездумных нападок?! // История Авиация. – №31. – с. 16.
33. Марданов А. Может хватит бездумных нападок?! // История Авиация. – №33. – с. 21.
34. Мерзляков В. КРО ОГПУ: люди и судьбы двадцатых // В сб. Тайные операции российских спецслужб с IX по XXI век. – М.: Гелиос, 2000. – с. 215–252.
35. Монетчиков С. Без грифа «секретно»: техника особой секретности. // Братишка. – 2007. – Режим доступа: www.bratishka.ru.
36. Николенко А. Умные машины // Воздушно-десантные войска. Спецназ. – 1998. – №4-6(9-11).
37. Павлов В.Г. «Сезам откройся!» Тайные разведывательные операции: Из воспоминаний ветерана внешней разведки. – М., 1999.
38. Павлов В.В. «Из истории создания и развития системы правительственной электросвязи советского государства» (1930–1941гг.). // Труды Общества изучения истории отечественных спецслужб, Т. 1. – 2009.
39. Синявская С. «Три дивизии за шифр». // Электронное издание «S&TRF – Наука и технология РФ», 08.05.2009. – Режим доступа: www.strf.ru.
40. Соболева Т.А. История шифровального дела в России. – М.: ОЛМА-ПРЕСС-Образование, 2002.
41. Сопельняк Б. Заложники Третьего рейха // Московский Комсомолец». – 2006. – 19 июня. – с. 11.
42. Сыромятников Б. Неоценимый вклад. Военные контрразведчики в битве под Москвой // Независимое военное обозрение. – 2006. – № 44. – с. 7.

43. Очерки истории российской внешней разведки в 6 томах, под ред. Е.М. Примакова и С.Н. Лебедева. – М., «Международные отношения», 1999.
44. Шеннон К. Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963.
45. Kahn D. The codebreakers. – N-Y: Macmillan Publ. Co., 1967.
46. http://en.wikipedia.org

Глава 9.

Дешифрование умерших языков

9.1. Общие замечания о дешифровании умерших языков[1]

Криптография и археология. Многие народы, населявшие Землю, бесследно исчезли, о других остались лишь археологические памятники со следами неведомой письменности или упоминания трудов греческих или римских историков. И лишь иногда удается оживить эти памятники, заставить говорить их на современных языках. ***Геродот*** в своей «***Истории***» сообщает, что египтяне пишут справа налево и что они употребляют двоякого рода письмо: одно называют священным ***(иератическим)***, другое – общенародным ***(демотическим).*** Но уже в IV в. египетские иероглифы воспринимаются как рисуночное письмо, в котором отдельные знаки обозначают самостоятельные понятия. Более того, высказываются и мнения, что иероглифы являются орнаментом и простыми украшениями. Только в ***эпоху Возрождения*** появился интерес к загадочным иероглифам. Чтобы воскресить египетскую письменность, пришлось потрудиться многим ученным. Упомянем некоторых из них. Первый, кто пытался оживить египетские иероглифы, был иезуит ***Анастасий Кирхер***. Он же показал, что ***коптский язык*** – исчезающий язык египетских христиан – был древнеегипетским народным языком. Датский ученый ***Карстен Нибур,*** занимаясь в Каире копированием всех доступных ему иероглифических надписей, обнаружил, что количество различных иероглифов невелико. Поэтому

[1] В данной главе использованы материалы, переданные авторам Г.П. Шанкиным и материалы курсовой работы студента Кулай Александра Юрьевича (при научном руководстве Бабаша А.В.).

египетскую письменность нельзя рассматривать как целиком идиографическую, т.е. такую, в которой для каждого слова имеется отдельный знак. В 1799 г. при отступлении наполеоновских войск из Египта совершенно случайно вблизи г. Розетта был найден камень, испещренный письменными знаками. Уже с первого взгляда можно было установить, что эта надпись состоит из трех частей: верхняя составлена из иероглифов, самая нижняя – из греческих букв, а к средней сначала и не знали, как подступиться. ***Розетский камень*** привлек внимание европейских ученых. И только в 1821 г. ***Жан Франсуа Шампольон*** завершил многолетнюю работу над расшифрованием египетской письменности. В результате он мог передавать демотический текст, знак за знаком, иератическим письмом и это последнее – иероглифами, на что до него никто не был способен. Свой вклад в расшифровку египетских иероглифов внесли также английский ученый ***Томас Юнг***, немецкий ученый ***Лепсиус*** и многие другие.

Клинопись была забыта даже более основательно, чем египетские иероглифы. ***Геродот*** упоминает о персидских буквах, а ***Страбон*** – об «***ассирийской письменности***», но не они, не древние евреи, видимо не знали о клине как основном элементе этой письменности. Только в XIX в. европейским ученым удалось заставить заговорить древнеперсидскую клинопись. Среди них в первую очередь следует назвать ***Георга Фридриха Гротенфенда***.

Поразительным открытием было дешифровка ***хеттской*** письменности. Дело в том, что о хеттах молчали все доступные европейцам исторические источники. И только в одной книге – Библии – об этом народе говорится в разных местах. Швейцарский востоковед ***Людвиг Буркхард*** во время одного из своих путешествий вблизи сирийского города Хама нашел камень, покрытый знаками, отличными от египетских. Прошло несколько десятилетий, прежде чем стало ясно, что это письменность исчезнувшего народа – хеттов. Но только в 1917 г. Чешский ученый ***Бедржих Грозный*** опубликовал труд «Язык хеттов, его строй и принадлежность к индогерманской группе языков».

Загадочной до сих пор остается ***Индская цивилизация*** (IV-II тысячелетия до н.э.). Она открыта в начале XX в. По-видимому, индская цивилизация была культурой бронзового в.. Ее города были застроены 2-3-этажными домами с водопроводом и канализацией, земледелие также достигло определенных успехов: выращивали пшеницу, хлопок и другие культуры; домашнее животноводство было представлено коровами, буйволами, свиньями, овцами… На керамике и металлических предметах сохранились надписи. Но до сих пор неизвестен ни язык этой письменности, ни какие-нибудь связи с народами, ныне населяющими ***полуостров Индостан.***

До сих пор остаются непонятными письмена древних жителей островов ***Пасхи.***

Общие замечания о дешифровании умерших языков. Сделаем предварительные замечания о языке и письменности. Проблемы возникновения, эволюции языков изучает специальных раздел языкознания – *этимология.* Эволюция письменности (письменная речь) включает в себя следующие этапы.

Прообразом «письменного письма» является так называемое «предметное письмо». В этом письме смысл передаваемого сообщения заключается в физическом наборе передаваемых предметов (камешки, цветы, ремешки и др.), которые пересылались получателю этого набора. Получатель должен был понять смысл присланных ему предметов (в последовательности их расположения).

К этому «письму» прибегали древние персы, китайцы, перуанские индейцы и др. Один из способов передачи сообщения заключался, например, в использовании нитки, на которой завязывались разноцветные узелки. Смысл сообщения должен был понят по размерам, цвету узелков и расстояниям между ними. Классическим примером в этом смысле является протописьмо **«кипу»**, которое использовалось перуанцами Латинской Америки. Этот метод использовался и в криптографии (**диск Энея**). Другой пример – так называемые древние руны, которые использовали древние германцы и славяне. Сообщение в этих рунах передавалось в виде различных сочетаний де-

ревянных палочек с нанесенными на них отметками («зарубками»). Позднее эти сообщения стали передаваться не сочетанием палочек, а их графическим изображением. Например, знак *Л* означал палочку, на которой нанесено три зарубки. Эти послания могли фиксироваться на деревьях, камнях и др.

Интересно, что и в наши дни сохранилось это древнее «протописьмо». У одного из живущих в наше время африканских племен («**Иебу**») для передачи сообщений используются жгуты из прутьев и ремешков с подвешенными на них предметами.

Аналогичное «письмо» сохранилось у племени северносибирских **юкагиров**. К началу XX в. их осталось всего около 400 человек. Сообщения передаются юкагирами в виде комбинации шнуров, палочек, перьев и орнамента, в целом напоминающей женское украшение. Один из исследователей попросил прочитать текст, запечатленный на украшении женщины племени юкагиров. Поначалу он принял это «сооружение» за обычное женское украшение. Женщина дословно прочитала текст, заключенный в этом украшении: «Уходишь. Ты любишь русскую, которая преграждает путь ко мне. Пойдут дети, и ты будешь радоваться им. Я же буду вечно грустить и думать лишь о тебе, ждать, когда придет другой русский мужчина, который меня полюбит». Это уже не письмо, а целая поэма.

Индейцы Северной Америки до сих пор используют так называемое **«ленточное письмо»** (пояса «вампум»). На ленту из кожи нанизываются разноцветные раковины – вампум. Таким образом даже заключались договоры с европейцами-колонизаторами.

Из предметного письма родилось так называемое *пиктографическое* (рисуночное) письмо. Знаки-рисунки обозначали бытовые сцены (охота, сражение, пир, религиозный обряд и др.). Связь рисунка со звучанием речи отсутствует; на любом языке рисунки истолковываются, а не «читаются».

Развитием пиктографического письма явилось *идеографическое письмо*. Слово «идеография» в переводе означает

письмо с помощью идеограммм. Идеограмма – знак, обозначающий не звук какого-либо языка, а целое понятие. Так, например, цифра 2 обозначает не три фонемы: д – в – а, а понятие определенного числа. Сюда же относятся химические и математические формулы и др. В значительной мере идеографической является древняя египетская письменность, письменность Майя, шумерская и аккадская письменность, современное китайское письмо. Однако в этих письмах наряду с идеограммами и *логограммами* (знаками, обозначающими не абстрактное понятие, а реальные слова, передающие это понятие) используются и фонетические знаки (*фонема* – минимальная единица звукового строя языка).

К идеографии относится и *иероглифическое письмо*. В нем фигурные знаки обозначают целые понятия, слова, слоги, буквы, а также фонетические единицы речи. В переводе слово **«иероглиф»** означает «священные письмена». Как отмечалось ранее, стилизованные рисунки в идеографическом письме выражают не только понятия, но и (главным образом) слова: две ноги означает ходить, человек с длинной бородой – старость и др. Связь знака со звучанием по-прежнему отсутствует, а сами знаки допускают множество толкований. Набор знаков обычно носил авторско-индвидуализированный характер.

Возникло и так называемое *идеографически (логографически)* – звуковое письмо: в нем стилизованные знаки означали не только слова, но и отдельные слоги. Поэтому это письмо иногда называют словесно-слоговым. Появились так называемые *знаки – детерминативы* (толкователи). Эти знаки не несли отдельной смысловой нагрузки, а поясняли слова, которые могли быть поняты неоднозначно. Например, слово «лев» могло означать как зверя, так и имя человек. В первом случае поясняющий детерминатив имел вид зверя, во втором – человек.

Разновидностью указанного письма явилось так называемое *ребусное письмо*. В нем последовательность знаков-рисунков изображала не только слова-понятия, но и последовательность звуков в слове. Этот ребус можно было понять только тогда, когда было известно прямое значение и «звучание» рисунков. Это

вызывало значительные затруднения. Попытки чтения этого письма напоминают решение современного рисуночного ребуса. Так, слово «стоять» можно было изобразить так: 100 ъ (ъ – буква старославянской азбуки, называемая «ять»).

Дальнейшее развитие письма пошло по пути создания универсальных знаков, т.е. «словаря» текстов. На создание таких знаков существенно влиял способ из фиксации, и, в частности, материал, на котором они записывались. Так, в Месопотамии знаки наносились на сырые глиняные дощечки, которые затем обжигались на огне. Поэтому эти знаки либо рисовались на сырой глине, либо выдавливались так называемой *клинописью.* На египетских папирусах уже можно было рисовать достаточно сложные округлые знаки. Письмо на бумаге допускало изображения любой формы.

Шли тысячелетия. Развитие письменности пошло по пути фонетизации знаков: эти знаки должны были не только обозначать слова и слоги, но и их звучание в устной речи. Началась привязка речи к письму. Знак стал обозначать не только и не столько обозначаемый предмет, но и соответствующее слово (звук). При этом появилась необходимость появления обозначений букв – фонем (элементарных звучащих частей речи). Например, волнистая линия уже не только изображала понятие «волна», но и букву (звук) «в». Для передачи слова стало необходимым использовать несколько знаков.

На этом пути возникли оригинальные особенности. Так, в некоторых письменностях стали исключаться гласные звуки. Предполагалось, что читатель восстановит их «по смыслу». Здесь могли возникать и элементы недопонимания, двусмысленные толкования. Так, например, в древнесемитском письме изображение руки обозначало букву «*d*», квадрата – букву «*p*», полукруга – букву «*t*». Эти три знака, идущие подряд, означали *dpt*. После возможного дополнения гласными получалось слово *depot*. Однако это слово имело два значения: «корабль» и «аппетит», В этом случае использовались знаки детерминативы («челн» и «высунутый язык»). Вместе с тем, дополнение другими гласными могло привести к прочтению и совершенно другого слова.

Знаки, изображающие не буквы, а целые слова и понятия (их называют идеограммами), стало необходимо определенным образом выделять в письме. Такие знаки используются и сейчас (например, транспортно-дорожные знаки).

Заметим, что на «заре истории» египетские и месопотамские письмена уже в значительной мере были фонетизированы. Пропуск гласных породил расширение обозначений согласных (в зависимости от контекста). Например, в Египте для обозначения согласных использовалось по два знака, при этом изменялось их звучание. Кроме того, употреблялись знаки для обозначения целых слогов. Использовались и сложные написания согласных (как, например, русский звук «ш» в современном немецком языке записывается как «*sch*»).

Окончательное становление фонетического буквенного письма, в котором знак обозначает звук, является исторической заслугой древних греков, которые опирались при этом на примитивный финикийский алфавит. Современные европейские алфавиты (латинский, русский) – потомки греческого алфавита.

Проблемы дешифрования умерших языков следующие.

При исследовании древних языков могут возникать различные ситуации. Во-первых (**вариант А**), язык известен, но письменность неизвестна. Например, русская речь (которая известна) записана непонятными знаками. Задача – понять то, что написано и «озвучить» письмо.

Здесь обычно применяются классические криптографические методы дешифрования, аналогичные дешифрованию шифров простой замены и кодов: частотный анализ появления букв, биграмм, слов, подбор и проверка вероятных слов и др. Частоты букв и биграмм определяются по звуковым характеристикам речи, аналогичным образом выделяются вероятные слова.

Во-вторых (**вариант Б**), известна письменность, но язык неизвестен. Письмо можно прочитать, но невозможно понять и озвучить. Например, человек, не знающий итальянского языка, может (зная латинский алфавит) прочитать письмо на итальянском языке без понимания смысла текста. Задача – оз-

вучить и понять его. 'Эту задачу часто называют задачей *интерпретацией текста*.

Здесь также возможны особенности. Например, известна письменность не исследуемого письма, а некотором смысле родственная ему (например, имеется письмо с текстом на русском языке, известном исследователю, но записанное по-болгарски).

В-третьих (**вариант В**): и письмо, и письменность неизвестны. Это самый сложный вариант. Его дешифрование обычно ведется путем поиска перехода к первому или второму варианту ситуаций (вариантам А или Б).

Большую помощь в изучении древних письмен оказывает дополнительная информация, которой располагает исследователь (как и при дешифровании в профессиональной криптографии). Эта дополнительная информация может включать в себя следующие составляющие.

1. Наличие так называемой «билингвы» – двуязычной записи одного и того же текста. В случае удачи один из языков известен. Нередко появлялись не «чистые» билингвы, а так называемые «квазибилингвы»: в них тексты повторяются не дословно, а лишь по смыслу.

2. Наличие в исследуемых текстах так называемых *глоссов* – заметок на полях, выполненных на известном языке и толкующих слова неизвестного языка.

3. Обнаружение родства неизвестного языка с известным. Такая находка является удачей, хотя и порождает различные толкования в языково-теоретическом смысле.

4. Знание исторической обстановки, имен и титулов царей, военачальников, богов и др.

5. Знание места и времени написания письма.

6. Догадки о тематике письма (по месту их обнаружения): хозяйственные записи (склад), эпитафия (кладбище), хвала правителю (официальное место), жреческие прорицания (храм) и др. Правильная догадка позволяет найти наиболее вероятные слова, фразы и др.

7. Наличие в письме знаков-детерминативов, *картушей* (выделяющих, как правило, в овальную рамку, имена царей,

военачальников и др.). Исследование документа на неизвестном языке включает в себя ряд этапов, некоторые из которых имеют определенное сходство с этапами решения дешифровальной криптографической задачи:

- составление каталога знаков, идентификация отличающихся написаний одного и того же знака (в этом случае внешне почти одинаковые знаки могут оказаться различными);
- частотный анализ знаков и их сочетаний; исследование начальных, средних, конечных букв, слов;
- разбиение текста на слова и предложения (если текст написан слитно);
- поиск наиболее вероятных слов (слово «царь», имя правителя и др.);
- поиск билингвы. В случае успеха задача существенно упрощается; методика ее решения становится во многом похожа на решение криптографической задачи дешифрования по открытому и шифрованному текстам; квазибилингва задачу усложняет;
- поиск родственного к исследуемому известного языка. Выдвижение и проверка гипотез. Здесь могут возникнуть и сомнительные ситуации.

Например, одинаков записанные в разных языках буквы предполагаются одинаково звучащими. Но здесь возможны и ошибки. Так, буквы В, С, Н, Р, Х пишутся одинаково на русском и английском языках, но звучат по разному, другой стороны, одинаковые звуки могут записываться по разному: звук [*b*] – по-русски это буква Б, а в латинском алфавите – В; звук [*n*] – Н и N; звук [*g*] – Г и G и др.

Таким образом, к подобного рода предположениям следует относиться весьма осторожно. Это замечание относится и к одинаковым корням слов. Например, корень, звучащий как [*da*], в латинском языке образует слово «давать», а в хеттском – «брать».

Исторические примеры дешифрования. ***Библейские находки (дешифрование по варианту А).*** В середине XX в. француз **Э. Дорм** исследовал надписи, найденные при рас-

копках в сирийском городе Библ (от которого родилось слово Библия), Письмо было похоже на иероглифическое, но как таковое не читалось. Достаточно быстро удалось установить, что используемый язык является уже известным финикийским. Этот вывод можно было сделать по месту обнаружения текста и по времени, к которому относилось его написание. Оказалось, что было использовано так называемое слоговое письмо, в котором каждый знак обозначал слог. После этой догадки дальнейшее дешифрование уже не вызывало существенных затруднений, частоты слов устной речи отождествлялись с частотами знаков-слогов.

Готский и тохарский языки (дешифрование по варианту Б). 1. Восстановление готского языка. Готский язык – самый старый германский язык. К X в. умер, сохранились лишь рукописи. Современный немецкий язык лишь отдаленно напоминает готский.

2. Восстановление тохарского языка. Во второй половине XIX в. на юго-западе Китая были найдены свитки рукописей. По ним был восстановлен тохарский язык, относящийся к индоевропейской группе. В результате был пролит свет на историю переселения народов в Центральной Азии.

Египетские иероглифы (дешифрование по варианту В). Эти иероглифы появились более 3 тыс. до н.э. Письмо имеет вид последовательного изображения птиц, змей, перьев, рук, завитков и др. Древние греки приняли их за изложение тайн магии и каббалистических учений. Но они не установили истинного смысла письменных текстов.

Содержание указанных иероглифических текстов – это религиозные гимны, «божественные» слова царских посланий и др. Напомним, что слово «иероглифы» в переводе означает «священные высеченные знаки».

В более поздние времена тексты содержали жреческие предсказания, магические символы и др. При этом начали применяться криптографические преобразования текстов (для сокрытия религиозных тайн).

Иероглифическое письмо быстро изменялось, упрощалось, и в конце концов древняя иероглифика оказалась забы-

той. Остались лишь письменные тексты на пирамидах. Также изменился и язык.

Заметим, что древняя египетская символика встречается и в более поздние времена. Так, например, на государственной печати США, созданной в конце XIX в., присутствует символ «глаз». В египетской символике глаз соответствовал понятию «божья справедливость».

Великий композитор, масон А.В.Моцарт (XVIII в.) по заказу своих братьев-масонов создал полную масонской символики оперу «Волшебная флейта». Действие оперы происходит в Египте, в храме Исиды и Осириса. В ней присутствуют элементы мифического истолкования иероглифов.

В конце XVIII в. Наполеон при походе на Египет привел с собой ученых различных научных направлений. Среди них оказался ученый-египтолог **П. Бушар**. Он обратил внимание на интересный камень – плиту из базальта, на котором была выбита двуязычная надпись. Впоследствии оказалось, что этот камень-билингва (и даже – трилингва): один и тот же текст был написан иероглифами, дематическим (упрощенным иероглифическим) письмом, и по-гречески. По городу, где он был найден, билингва получила название «Розеттский камень». 'Этот камень оказал решающее влияние на дешифрование древних иероглифов. В криптографических терминах к шифрованному тексту добавился соответствующий открытый текст, написанный на известном языке.

Прочитать древние иероглифы на египетских пирамидах попытались еще в средние в.. Так, в IV–V вв. н.э. римлянин **Гораполлон** предложил аллегорическое истолкование иероглифических текстов, но ошибся и ввел в заблуждение последующих исследователей. Аллегорически-пиктографический смысл посланий древности допускал различные толкования.

Известный криптограф средневековья итальянец **Альберти** также пытался расшифровать древнеегипетские тексты, но потерпел неудачу.

В XVI в. итальянец Дж. Фоссе, личный секретарь папы Льва X, написал около 60 книг, посвященных египетской ие-

роглифике. В каждой книге исследовался один или несколько иероглифов. Он, по следам Гораполлона, попытался аллегорически толковать иероглифы. Так иероглиф «слон» (рисунок) он отождествлял со словом «чистота» (так как слоны, соблюдая гигиену, купаются в реках); «лев и кабан» – «сила духа и тела»; «лев и петух» – «благоговение и кротость» и др. Но эти толкования в основном оказались ошибочными.

Интерес к проблеме нарастал. В XVII в. вышла книга **Г. фон Гогенбурга** (Германия) «Thesaus Hieroglyphicorum» – большое собрание древних иероглифических надписей, в последствии широко использованная исследователями.

В XVII в. иезуит, ученый-вулканолог, человек, интересовавшийся криптографией и считавший себя криптографом **А. Кирхер** (Германия) объявил о дешифровании иероглифов. Но это оказалось ошибкой. Вместе с тем Кирхер использовал заслуживающий внимания прием возможного сведения **варианта В** к **варианту А**. Так, он предположил, что в основе древнеегипетского языка лежит древний коптский язык – «язык фараонов». Этот язык сохранился до наших дней, но в сильно видоизмененном виде. Он используется в Египте в современной коптской церкви – церкви египетских христиан. Правда, алфавит этого языка – греческий.

Кирхер внес большой вклад в изучение древнего коптского языка. 'Это дало ему возможность раскрыть некоторые иероглифы. Например, по-коптски «вода» звучит как «пш»; поэтому иероглиф означает понятие «вода'[5], и одновременно соответствует звуку «т». Но в целом Кирхер глубоко заблуждался в своих исканиях и породил массу нелепостей вокруг дешифрования иероглифики.

Впервые всерьез (в научном смысле) приступил к исследованиям «Розеттского камня» парижский профессор **С. де Саси**. Он отверг тайную символику в иероглифических надписях и применил в своих исследованиях метод, который современный криптограф назвал бы «методом протяжки вероятного слова». Он обоснованно предположил, что за словами, обрамленными картушами, скрываются слова – имена (Птоломей, Александр,

Клеопатра и др., которые он нашел в греческом тексте). Де Саси верно прочитал указанные слова, но дальше этого не продвинулся. Заметим, что в это время еще не было доказано, что камень – это «чистая» билингва, а не «квазибилингва».

В XIX в. другие ученые достигли некоторых успехов в прочтении и толковании отдельных фрагментов (английский ученый Т. Юнг и др.). Но задача до конца так и не была решена.

Наконец, в XIX в. проблемой заинтересовался молодой французский ученый **Жан-Франсуа Шампольон.**

Сначала он пошел по пути Горапполона (символическое, аллегорическое толкование иероглифов). Но вскоре он убедился в том, что этот путь ведет в тупик.

Затем Шампольон плодотворно использовал идею Кирхера о древнекоптском языке как языке, родственном иероглифическому. Это приблизило **вариант В** к **варианту А**.

Шампольон глубоко ознакомился с историей древнего Египта, изучил древние языки, выдвигал различные гипотезы и, к сожалению, часто заблуждался. Он тщательно проанализировал тексты на «Розеттском камне». Оказалось, что в иероглифическом тексте присутствует около 1500 иероглифов, из них около 170 различных. В греческом – около 200 слов. Шампольон предположил, что некоторые иероглифы передают звуки (фонемы), из которых состоят слова. Впоследствии это подтвердилось. Затем оказалось, что иероглифы передают и отдельные буквы, и биграммы, и слова (на известном к тому времени коптском языке). Он принял идею, аналогичную идее де Саси, и также использовал метод «протяжки вероятного слова». Шампольон прибегал и к толкованию некоторых иероглифов, и это оказалось справедливым. Так, например, иероглиф «глаз» и означал слово «глаз»; иероглиф «лук» – слово «лук», «хлеб» – «хлеб», «человек с палкой» – «бить», «лилия» – «юг» (так как этот цветок растет на Юге) и др. В тексте оказались и омонимы (омофоны) – слова, одинаково звучащие, но означающие различные предметы; имелись и знаки – пустышки (которые получились в результате нагромождения знаков друг на друга).

В надписях имелись картуши, выделяющие написанные побуквенно имена Птоломея и Клеопатры (Ptolmees, KJeopatra). С помощью раскрытия иероглифических букв этих имен были прочитаны другие имена: Alexander, Caesar и др. Тайна древнеегипетских иероглифов в основном была раскрыта. Последующие исследователи довели дело Шампольона до конца.

В жизни Шампольона имел место один неприятный эпизод. Дело в том, что пытаясь опередить Шампольона его соотечественник Ленуар выпустил книгу «Новое объяснение», в которой утверждал, что ему удалось впервые дешифровать египетские иероглифы. Однако Шампольон доказал, что это не дешифрование, а «чистейший вздор, голая выдумка, авантюристическое смешение фантазии и ложной учености».

Чрезмерное напряжение подорвало здоровье Шампольона. Он умер в возрасте 41 г. (в 1832 г.).

Как это часто встречается, к исследованию серьезной и «модной» проблемы приступили различного рода дилетанты, авантюристы и др. В иероглифах видели еврейское учение «каббала» с ее символикой, другие тайные учения, астрологические тексты и др. Профаны на основе идей Горапполона и собственной фантазии «надешифровали» огромное количество несуразиц.. К их числу относится и российский граф Пален, который утверждал, что с помощью каббалы он дешифровал иероглифы за одну ночь. Все эти спекуляции побудили Вольтера бро-сижь следующую фразу в адрес дешифровальщиков: «для них гласные недочет, а согласные не имеют значения».

Однако среди тайноискателей оказывались и талантливые люди. Так, англичанин **Т. Юнг** еще до Шампольона индуктивно-правильно расшифровал 76 групп иероглифических символов. Однако остальные 150 групп были им расшифрованы неверно.

История сохранила имя Шампольона как первого ученого, квалифицированно дешифровавшего древние египетские иероглифы.

Ассиро-вавилонская клинопись. В середине XIX в. француз **П.Э. Ботта**, врач, дипломат, археолог, ученый-лингвист,

обнаружил в Месопотамии (современный Ирак) большое количество глиняных табличек с клинописным текстом. Тем самым он стал первооткрывателем древнейшей цивилизации, существовавшей около 5 тыс. назад. Он выпустил книгу, в которой привел рисунки табличек.

К этому времени уже имелся некоторый опыт прочтения клинописи. Так, еще в XVII в. была обнаружена древнеаравийская (так называемая переспольская) клинопись. Клинопись Ботга была аналогична переспольской.

В начале XIX в. немец **Г.Ф. Гротефенд**, педагог, филолог, еще до находки Ботта нашел метод дешифрования аравийской клинописи. На некоторых ранее обнаруженных табличках были найдены трилингвы, но все три – на неизвестных языках. Поначалу эти письмена приняли за орнамент, а не тексты.

Гротефенд доказал, что хотя клинописные знаки и направлены в разные стороны, основных направлений письма может быть только два: либо сверху вниз, либо слева направо, так как угол, образуемый двумя клиньями, всегда обращен налево. Далее он доказал, что тексты нужно читать слева направо, (что европейцам показалось вполне естественным).

Первые тексты, которыми занялся Гротефенд, были надгробными надписями. Он изучил новоперсидские надписи на надгробных плитах и выявил довольно часто повторяющиеся обороты типа русского «спи спокойно». В качестве исходной версии он принял гипотезу о том, что в одной из записей надмогильной трилингвы использован древнеперсидский язык, и что в этих надписях могли быть использованы такие же «стандарты». В качестве одного из этих стандартов «по-персидски» он принял текст: «А» великий царь, царь царей, царь «В», сын «С» великого царя, царя царей ... . Он выделил наиболее часто встречающиеся группы клиньев и отождествил их со словом «царь». При этом он обоснованно предположил, что запись на древнеперсидском языке (главном в месте обнаружения трилингвы) должна занимать центральное место в этой трилингве.

Тщательно изучив исторические документы, Гротефенд пришел к выводу том, что за условными символами «А» и «В»

должны скрываться имена Дария и Ксеркса, написанные побуквенно. Отождествив эти предположения с текстом клинописи, он получил первые двенадцать букв древнеперсидского клинописного алфавита. Затем аналогичным путем он опознал еще несколько букв. Окончательно же работу по дешифрованию клинописи завершил француз **Э. Бюрнуф** и норвежец К. Лассен в 1836 г.

Но с дешифрованием клинописи произошло то же самое, что и со многими другими открытиями и изобретениями: оно было осуществлено дважды! Несколько позднее и совершенно независимо от Гротефенда, Бюрнуфа и Лассена это сделал англичанин **Г.К. Раулинсон**, майор английской армии, состоявший на персидской службе. В 1859 г. он был назначен английским послом в Тегеране.

По сути дела Раулинсон использовал ту же методику, что Гротефенд. Ему удалось продвинуться дальше Гротефенда, в чем он убедился, ознакомившись с публикациями Гротефенда в 1836 г.

В целях получения новых исторических материалов Раулинсон скопировал надпись, нанесенную на скале, нависшей над пропастью. Для этого ему пришлось спуститься и висеть на веревке над этой пропастью. Он не только скопировал надпись, но и дал ее полный перевод. Но полностью задача еще не была решена (другие тексты не читались). С помощью новых исследователей удалось расшифровать около шестидесяти знаков древнеперсидской клинописи, и лишь спустя много лет работа была полностью завершена. Помимо прочтения текстов их нужно было еще и понять. Здесь помогло определенное сходство древнеперсидского и новоперсидского языков.

Как было отмечено ранее, трилингва содержала надписи на трех ясно различных языках.

Дешифрование второго текста связано с именем датчанина **Вестергаарда**. Третью надпись дешифровали Раулинсон и немец **Опперт**. Были сделаны следующие выводы.

Первая (древнеперсидская) надпись – это алфавитное письмо, знаки которого являются одновременно и звуками.

Каждая группа клинописных знаков могла означать и букву. В третьей надписи каждый отдельный знак означал букву, а иногда и целое слово (некоторый аналог идеографического письма). Более того, встречались одни и те же знаки, означающие различные слоги и даже различные слова, а некоторые различные сочетания знаков давали одну и ту же букву. Исследователи пришли в замешательство. Результаты предшествующих дешифрований начали вызывать серьезные сомнения.

Приведем лишь один пример многозначности чтения надписи. Буква «Р» изображается шестью различными знаками в зависимости от того, в какой слог она входит: «ра», «ри», «ру», «ар», «ир», «ур» (напомним, что гласные обычно опускались). Если к этим слогам добавляется еще и согласный звук, путем складывания каждых двух звуков образуются особые знаки для звуков «рам», «мар» и др. Многозначность основывается на том, что несколько знаков, объединенных в группу, теряют свое первоначальное значение и означают совершенно иное понятие или имя. Так, например, группа знаков, составляющее имя Навуходоносор (правильнее – Набукудурриусур), прочитанных в слоговом прочтении дает Ан-па-ша-ду-шеш.

И здесь помогла удача. Были обнаружены таблички-словари, созданные, очевидно, для учебных целей (VII в.) и содержащие расшифровку значений клинописных знаков в их отношении к буквенному письму.

Затем начали находить и другие древние учебники по основам клинописи и словари, причем некоторые их них были составлены на известном шумерийском языке (этот язык еще сохранился в религии и юриспруденции).

Выводы «старых» дешифровальщиков были подтверждены, и тем самым проблема прочтения персепольской клинописи была полностью решена. Сегодня имеется немало ученых, свободно читающих клинописные тексты.

Результаты работы по дешифрованию персепольской клинописи позволили дешифровать находки Ботта. Обнаружилась древняя шумерская цивилизация. Суть этой находки заключалась в следующем.

Дешифровальщики клинописи «вычислили» существование еще одного, более древнего (чем аравийский) народа с его удивительно развитой цивилизацией. Эти вычисления напоминают те, с помощью которых астрономы находят новые небесные тела, невидимые в их время. Изучая взаимосвязи между языком и письменностью, они пришли к выводу о том, что обнаруженная клинопись – не изобретение вавилонян и ассирийцев. Их клинопись является лишь развитием и видоизменением изобретения другого, более древнего народа, не относящегося к семитским народам (к которым принадлежали вавилоняне и ассирийцы). По предложению француза **Ж. Оперта** этот народ назвали *шумерами*. Шумеры в древние времена заселяли двуречье между Тигром и Ефратом (на территории современного Ирака). Эта местность называлась Месопотамией.

Начались новые раскопки (француз **Э. де Сазек** и др.). Были найдены материальные следы древнейшей и очень развитой цивилизации, и среди них – древние письменные клинописные памятники.

Шумеры – самая древняя из известных в настоящее время цивилизаций, существовавшая еще до древнеегипетской. История происхождения шумеров неизвестна. Она уходит корнями за III тысячелетие до нашей эры. На основе шумерской цивилизации возникла вавилонская культура. В письменных памятниках шумеров впервые упоминается библейский всемирный потоп. Этот «шумерский потоп» был, очевидно, исторически связан с мощным разливом Тигра и Ефрата, который был принят жителями за всемирный потоп.

Клинопись шумеров удалось прочитать с помощью уже накопленного опыта чтения клинописи. Выяснилось, что шумерская цивилизация оказала мощное влияние на последующие цивилизации. В частности, удалось установить, что шумерам принадлежат следующие очаги нарождавшейся цивилизации:

- древнейшие юридические нормы, понятия вины, мести, справедливости и др.;
- сведения об искусстве древнего врачевания. Роль колдунов, магов, волшебников во врачевании, религиозные предпи-

сания больным. Особо подчеркивалась ответственность врача: «Если врач сделает человеку тяжелый надрез бронзовым ножом и причинит смерть этому человеку, или, снимая бронзовым ножом бельмо у челов., повредит глаз, ему следует отрубить руку»;

- астрономические наблюдения, изучение влияния космоса на жизнь Земли; разработка первой карты звездного неба, создание календарей. Время обращения Луны вокруг Земли шумеры вычисляли с ошибкой всего в 0,4 с.;
- первые математические успехи. Шумеры использовали позиционную шестидесятеричную систему исчисления, аналогом которой является и наша десятиричная система (являющаяся ее наследницей). Они создали первые счетные таблицы – «ЭВМ древности». В математике шумеры разбирались гораздо глубже, чем последующие цивилизации. Так, древние греки называли числа, превышавшие 10.000, просто «тьмой», понятие чисел порядка 10^6 появилось на Западе лишь в XIX в. (во времена Декарта, Ньютона, Лейбница). Шумеры свободно оперировали числами порядка 10^{15};
- удивительные успехи в архитектуре и градостроительстве. Шумеры впервые стали применять арочные конструкции. В Европе они появились лишь после походов Александра Македонского;
- создание религиозных мифов, позднее вошедших в основные религии мира (в том числе и в христианскую) и др.

Один из крупнейших археологов XX в. **Л. Вуллей** так подвел итоги месопотамских находок: «Если судить о заслугах людей только по достигнутым ими результатам, то шумерам должно здесь по праву принадлежать почетное, а может быть и выдающееся место... Их цивилизация как факел в ночи осветила еще погруженный в варварство мир» .

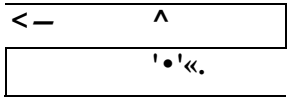
Хеттская клинопись. Хетты – древний народ, занимавший во втором тысячелетии до нашей эры обширную территорию в районе современной Южной Турции, Южного Ирака и Северной Серии. На культуру хеттов значительное влияние оказали шумеры. Первоначально хетты использовали иероглифическое письмо, но затем перешли на клинопись.

Цивилизация хеттов была забыта. Ее заново «изобрели» англичанин **А.Г. Сэйс** и ирландский миссионер **У. Райт** в конце XIX в. Корни своего изобретения они нашли в Библии (Ветхий завет), в которой имелись упоминания о некоторой народности, проживавшей в указанном регионе.

В результате поисков вначале был обнаружен так называемый Хаматский камень с хеттскими иероглифами. Поначалу надписи были приняты за своеобразный орнамент, но вскоре выяснилось, что это древнейшие письмена.

Один из первых вопросов, возникающих при исследовании странных записей, это вопрос о направлении чтения: слева – направо, справа – налево и др. Известно, что арабы пишут справа – налево, китайцы – сверху – вниз, египтяне используют и то, и другое. У египтян (как указывалось ранее) существовали специальные знаки, указывающие на направление письма: поворот головы совы, наклон тростника, указывающая рука.

Л.Г. Сайс в результате исследований пришел к интересному выводу. Оказалось, что хетты писали по следующему маршруту:



Такое правило письма получило в последующем название «правила бустрофедона» («как пашет вол»). При этом Сейс правильно истолковал знаки-указатели направления письма.

Язык и письменность были неизвестны. Но здесь исследователям повезло: была обнаружена билингва – печать с клинописными и иероглифическими текстами. Однако обе письменности и язык были неизвестны. Правда, некоторые иероглифы легко истолковывались: царь, земля и др. (они напоминали пиктографию). Основная заслуга в дешифровании хеттской клинописи принадлежит чешскому исследователю начала XX в. Б. Грозному. Один из первых дешифрованных им текстов – это песня-стихотворение:

Ткани Несы! Ткани Несы
Принеси, приди!
Матери моей одежды
Принеси, приди!
Предка моего одежды
Принеси, приди!

Неса – древний хеттский город. Хетты называли свой язык «несийским».

Как выяснилось в результате исследований, хеттский язык близок к индоевропейской группе языков, к индоевропейскому проязыку – санскриту. Этот факт позднее установил Грозный.

Когда Грозный приступил к исследованиям, ни язык, ни письменность хеттов были неизвестны. Имелись лишь предварительные результаты изучения тайны хеттов, в частности, соображения относительно возможного языка. Априорные сведения и документы, находящиеся в руках Грозного, заключались в следующем:

- он имел представление о культуре хеттов. Эти сведения были накоплены ранее в результате проведения раскопок, прочтению египетской иероглифики, ассиро-вавилонской клинописи, содержанию некоторых хеттских «дипломатических» документов, написанных на аккадском языке. Аккадский язык, к этому времени уже известный, являлся аналогом общепринятого в XVIII–XIX вв. в Европе французского языка (языка «международного общения») в древние времена в Восточном Среднеземноморье;
- он имел сведения о взаимных связях древних цивилизаций, в том числе о языково-письменных «внешнеполитических» документах в данном регионе и их содержании;
- он располагал большим количеством хеттских клинописных текстов, найденных при раскопках;
- отметим, что Грозный являлся полиглотом; в частности, он основательно изучил древние языки.

Кроме того, он имел некоторый опыт дешифровальной работы, полученный им при прохождении службы в австро-

венгерской армии во время Первой мировой войны в должности штабного дешифровальщика.

Довольно быстро Грозный установил, что хеттская клинопись является аналогом иероглифической ассиро-вавилонской. Эта клинописно-иероглифическая письменность была изучена аналогично египетской. Исследуя клинопись, Грозный писал «... в нашем деле имеет значение не только доскональное знакомство с научным материалом, но и известные комбинарные способности, игра воображения, интуиция, ясновидение». Основной способ исследований, использованный Грозным, заключался в выдвижении и проверке гипотез. В начале исследований Грозному предстояло решить следующие задачи:

- установить происхождение письменных источников и места их нахождения, Грозный имел в своих руках копии около 20000 табличек и их фрагментов. Определение мест обнаружения находок могло бы дать общее представление о содержании текстов: если табличка найдена в храме, то текст носит скорее всего религиозный характер; если на складе – то это хозяйственные записи и др.
- классифицировать таблички по местам их обнаружения. Опознать и склеить куски табличек. С этой целью он много времени проводил в музее, где хранились таблички;
- в целях облегчения различения знаков текста переписать слова (перекодировать) с табличек древности латинскими буквами и их сочетаниями.

При этом появились странные закономерности. Хеттское слово (на латыни) «harmi» звучит так же, как на древнеиндийском слово «есть»; «daai» – как славянское «дай» или латинское «dare» «давать») и др. Но вскоре Грозный понял, что это лишь случайные совпадения, неизбежные при кодировке.

Грозный начал с классификации слов по их окончаниям для восстановления грамматических форм неизвестного языка. Это был огромный труд. Грозный сравнивал слова с написанием глагольных форм на греческом и древнеиндийском языках. Ему удалось восстановить несколько глаголов и понять их значение (по сходству с указанными языками).

Затем он выделил клинописные идеограммы (слова, понятия, имена) по сходству соответствующих знаков с известной аккадской клинописью. Однако читались они, по-видимому, по разному. Так, число 45 имеет одно и то же значение в различных по языку письменных текстах, но читается по разному. Грозный хотел восстановить и речевое звучание хеттского языка.

На этом пути Грозный установил первое слово – слово «хлеб». Он предположил, что за ним следует слово «едите»; за следующим словом «вода» – «пьете» и т.д. Эти слова – глаголы были записаны побуквенно. Свое предположение Грозный перепроверил по различным текстам, что подтвердило его догадку. Первая правильно переведенная фраза была такой: «Сейчас хлеб будете есть, воду потом будете пить». Развивая свой успех. Грозный пришел к полному прочтению письменности.

Хеттский язык, до этого ошибочно считавшийся семитским, оказался языком индоевропейской группы, но с использованием клинописного алфавита.

В результате дешифрования Грозным хеттской письменности был получен очень важный исторический материал, проливавший свет на становление человеческой цивилизации.

Однако хеттские иероглифы еще не были дешфрованы, но по клинописи и историческим данным язык уже был известен. Кроме того, к этому времени накопилось уже более 100 билингв с клинописью и иероглифами. Казалось бы, что проблема скоро будет решена. Но выяснилось, что языки клинописи и иероглифов являются различными, хотя и родственными (как родственны, например, латинский и итальянский языки). Таким образом, хетты использовали два языка: один – при клинописи, другой – при письме иероглифами.

В первичном дешифровании иероглифов были получены частичные успехи. Так, швейцарский профессор **Э. Форрер** расшифровал ряд знаков и слов и получил некоторые результаты по синтаксической структуре иероглифического письма. Американец **И. Гельб** установил, что помимо идеограмм у хеттов было только 60 фонетических знаков. Таким

образом, это письмо является частично слоговым, но с необычным строем: согласный в слоге обычно следует за гласным звуком (в современных европейских языках обычно гласный звук следует за согласным).

Окрыленный успехом чтения клинописи Грозный попытался создать общую теорию дешифрования древних текстов (нечто подобное попытке Эйнштейна по созданию общей теории поля). Но как и Эйнштейн, Грозный успеха не добился. К этому времени у пожилого Грозного начались негативные старческие изменения мозга. Он полностью уверовался в свою гениальность и смело взялся за хеттские иероглифы. Он изучил обнаруженные печати с протоиндийскими иероглифами (III в. до н.э.). Эти иероглифы уже были дешифрованы. Грозный нашел сходство между хеттскими и протоиндийскими иероглифами и «прочитал» хеттские иероглифические тексты. Однако это прочтение оказалось грубо ошибочным, что доказали другие исследователи. Аналогичным образом Грозный грубо ошибочно «дешифровал» так называемое критское линейное письмо «Б». Его дешифрование специалисты назвали «убогой галиматьей из хеттских и вавилонских слов». Грозный в старости существенно подорвал свой авторитет ученого-исследователя древних текстов.

Прочитать некоторые иероглифы удалось немцу **Х.Т. Боссерту**. Он обнаружил большую билингву с древней иероглификой и уже прочитанным к тому времени финикийским письмом (вариант – «билингва»). После этого задача была решена достаточно просто.

Дешифрование хеттской письменности позволило получить важные сведения о древней культуре. Так, например, выяснилось, что хетты переняли у древних вавилонян их познания в математике. Эти познания были удивительными. За XV веков до Архимеда, Пифагора, Эвклида в древнем Вавилоне уже были известны формулы для вычисления площади треугольника, прямоугольника, объемов пирамиды, конуса и др. Древние математики уже умели возводить числа в степень, решать квадратные и кубические уравнения и др.

Представляет интерес юридичекий кодекс хеттов, трактовка ими взаимоотношений между преступлением и мерой наказания за него.

Например. Если женщина изнасилована в доме, то ее ждет смертная казнь (поскольку она могла позвать на помощь и не сделала этого). Если же она изнасилована в горах, то с нее снимается вина. Насильник в обоих случаях подлежит смертной казни.

Прочтение клинописи еще вызывало сомнения. В связи с возникшими сомнениями был проведен необычный эксперимент. Четырем наиболее известным «клинописцам» был выслан недавно обнаруженный клинописный текст с просьбой дешифровать его. Все дешифрования оказались идентичными, однако сами ученые были оскорблены таким «испытанием» их способностей. Но эксперимент окончательно подтвердил истинность чтения клинописных текстов.

Фестский диск. В дешифровании умерших языков имели место не только победы, но и поражения. К недешифрованным до настоящего времени документам относится так называемый фестский диск (диск из Феста).

Француз **Л. Пернье** в 1908 г. во время раскопок на о. Крит (в городе Фест) обнаружил интересный документ. Он представляет собой плоский диск из обожженной глины размером с ладонь (около 16 см в диаметре). Происхождение диска относят примерно к XVII веку до н.э.

По обеим плоским поверхностям диска проходит глубокая спиральная борозда, делающая по 4 витка на каждой стороне диска. В результате диск разбивается на спиралевидные полосы. Эти полосы разделены на отдельные участки (поля) поперечными радиальными черточками. Эти поля заполнены разнообразными знаками-рисунками: кипарис, кустарник, ветвь, колос, лилия, гусеница, пчела, дельфин, сокол, голова льва, коровья нога, бегущий человек, женщина с обнаженной грудью, голова в уборе из перьев и др. Некоторые рисунки в явном виде не интерпретируются.

Сразу же был отмечен важный момент: знаки не нарисованы, а оттиснуты с помощью «штемпелей». Таким образом, это был «напечатанный» текст. Следовательно, при написании текстов был использован ограниченный набор знаков.

Количество знаков на обеих сторонах диска равно 242. Из них различных – 45. Знаки появляются с разной частотой: от одного до 20 раз.

Однако ограниченное общее количество рисунков-знаков (242) давало основание предположить, что количество знаков алфавита текста может быть значительно больше. В целях изучения такой возможности был проанализирован темп нарастания (появления) новых знаков с увеличением длины текста. Оказалось, что новые знаки появляются в экспоненциально-убывающем объеме. Транспонирование экспоценты на бесконечную длину гипотетического текста привело к выводу о том, что полный алфавит содержит около 60 знаков.

Одна из первых проблем возникающих при исследовании диска, это проблема направления чтения. Как читать письмена: от центра диска к краям или наоборот. Эта проблема сегодня окончательно так и не решена.

Многочисленные специалисты приступали к попыткам дешифрования. При этом выдвигались различные гипотезы, среди которых можно выделить следующие:

- исследуемое письмо относится к идеографическому. Эту гипотезу большая часть ученых отвергла, так как в идеографическом письме должно было быть значительно больше различных знаков;
- письмо является слоговым (знак изображает слог). Эту гипотезу большинство ученых приняло, так как в известных слоговых письменах насчитывается 50–60 знаков. Для буквенного письма знаков многовато (в них обычно 25–35 знаков). Словесное письмо насчитывает несколько сотен знаков, поэтому едва ли исследуемое письмо является таковым;
- разбиение на поля соответствует разбиению текста на слова. Эту гипотезу поддерживает большинство ученых. В этом случае обнаруживаются полные и частичные повторения слов.

Появляется возможность выделения корней слов, префиксов и суффиксов;

- фестское письмо по сути своей похоже на хеттское иероглифическое письмо. Оно, в частности, содержит аналогичный знак раздела между словами. Эту идею активно пропагандировал Грозный, однако большинство ученых ее не приняло. Похожие знаки раздела используются и в других письменах;
- некоторые знаки письма являются знаками-детерминативами. Например, рисунок «голова с убором из перьев» может означать некоторую официальную руководящую личность, которая могла носить такой головной убор. За этим знаком должно следовать имя этого человек. Эту точку зрения большинство ученых поддержало и др.

Дешифровальщики диска столкнулись со следующими проблемами:

- диск является единственным памятником представленной им системы письменности; аналогов этого письма нет;
- очень трудно догадаться о возможном содержании текста;
- отсутствуют глоссы, картуши; не известны исторические имена, которые могли бы быть отражены на диске;
- отсутствуют билингвы и квазибилингвы и др.

Целый ряд исследователей объявил о своих успехах в дешифровании, но все они оказались ошибочными. Основные ошибки заключались в следующем:

- толкование некоторыми специалистами фестского письма как пиктографической письменности. Несмотря на то, что уже было доказано обратное, они «надешифровали» («истолковали») большое количество вариантов открытого текста:
- произвольная привязка изображений к их необоснованным эквивалентам в уже дешифрованных языках (древнегреческом, семитском и др.). Попытки чтения знаков на этих языках;
- идеографическое толкование текста (по хеттскому и египетскому языкам);
- отождествление первого звука, изображающего предмет при его прочтении, со звуковым звучанием первого слова (*акрофонический* способ чтения);

- сомнительное отождествление знаков-изображений с известными иероглифическими знаками;
- ошибочный подбор возможного «открыв «st'ra»; сомнительные попытки создания искусственной билингв, хотя бы квазибилингвы и др.;

Тайна фестского диска не раскрыта. Исследователи связывают перспективу раскрытия этой тайны с возможным появлением новых исторических документов древности.

Следует однако отметить любопытный факт. В конце XX в. наш соотечественник **Г. Гриневич** выступил с сенсационным заявлением. Ему, оказывается, путем применения тончайших методов криптографии удалось дешифровать фестский диск!

Сразу же отметим, что заявление Г.Гриневича и результаты его исследований были немедленно опровергнуты мировым научным сообществом. Он был обвинен в некомпетентности, а его выводы названы «псевдонаучным бредом». Тем не менее приведем некоторые из них.

Г.С. Гриневич пришел к выводу о том, что старинная славянская письменность намного старше шумерской письменности и появилась еще в начале V-го тысячелетия до н.э.

Как же появились славяне на о. Крит в Средиземном море в это время? Очень просто. Они бежали на юг в силу «несносных» условий жизни на севере. Об этом и повествует диск, текст которого нужно читать следующим образом:

ГОРЕСТИ ПРОШЛЫЕ НЕ СОЧТЕШЬ,
ОДНАКО ГОРЕСТИ НЫНЕШНИЕ ГОРШЕ.
НА НОВОМ МЕСТЕ ВЫ ПОЧУВСТВУЕТЕ ИХ.
ВАМ ПОСЛАЛ БОГ ЕЩЕ МЕСТО В МИРЕ БОЖЬЕМ.
РАСПРИ ПРОШЛЫЕ НЕ СЧИТАЙТЕ.
ЧТО ВАМ ПОСЛАЛ БОГ, ОБСТУПИТЕ ТЕСНЫМИ РЯДАМИ.
ЗАЩИЩАЙТЕ ЕГО ДНЕМ И НОЧЬЮ.
НЕ МЕСТО – ВОЛЮ.
ЗА МОЩЬ ЕГО РАДЕЙТЕ.
ЖИВЫ ЕЩЕ ЧАДА ЕЕ, ВЕДАЯ, ЧЬИ ОНИ
В ЭТОМ МИРЕ БОЖЬЕМ.

На другой стороне диска написано:
БУДЕМ ОПЯТЬ ЖИТЬ, БУДЕТ СЛУЖЕНИЕ БОГУ,
БУДЕТ ВСЕ В ПРОШЛОМ – ЗАБУДЕМ, КТО МЫ ЕСТЬ.
ГДЕ ВЫ ПОБУДЕТЕ, ЧАДА БУДУТ, НИВЫ БУДУТ,
ХОРОШАЯ ЖИЗНЬ – ЗАБУДЕМ, КТО МЫ ЕСТЬ.
ЧАДА ЕСТЬ – УЗЫ ЕСТЬ – ЗАБУДЕМ, КТО ЕСТЬ.
ЧТО СЧИТАТЬ, ГОСПОДИ! РЫСИЮНИЯ ЧАРУЕТ ОЧИ.
НИКУДА ОТ НЕЕ НЕ ДЕНЕШЬСЯ,
НЕ ИЗЛЕЧИШЬСЯ ОТ НЕЕ.
НЕ ЕДИНОЖДЫ БУДЕТ, УСЛЫШИМ МЫ:
ВЫ ЧЬИ БУДЕТЕ, РЫСИЧИ, ЧТО ДЛЯ ВАС ПОЧЕСТИ;
В КУДРЯХ ШЛЕМЫ; РАЗГОВОРЫ О ВАС.
НЕ ЕСТЬ ЕЩЕ, БУДЕМ ЕЩЕ МЫ, В ЭТОМ МИРЕ БОЖЬЕМ.

Болгарский ученый **Иванов** аналогичным образом «перевел» надпись на диске с предполагаемого древнелидийского языка:

Сторона А.

Когда Яра отправился в поход на Лилимува, когда отправился и не успел, Ярамува его устранил, прогнал своего любимца, и он сам уничтожил Лилимува. Тархумува решил относительно Яра, чтобы он ушел на отдых. Тархумува был в плохих отношениях с этим Лилимувой. Тархумува решил относительно Яра, чтобы он отдыхал (ушел на отдых) во дворце. Он (Тархумува) напал на границу области Сандапия. Апипумува убежал. Упарамува встречает меня, разгневанный из-за своих интересов, однако Рунда применил насилие и отразил его. Сармасу удалился к Ярамува.

Сторона Б.

Сарма обдумывает и свободно готовит свой план: он натравливает. Илион (Троя) его подстрекает, однако я берегусь. Сарма, разгневанный на Эфес, принял решение в свою пользу. Илион его подстрекает. Сармасу освободился, пришел и применил насилие. Илион его поощряет. Для унижения Ярину он отправился в Ялисос, наложил тяжелую дань, однако проявил снисхождение, взял ему глаза и удалился в Газену. Однако Яра гневается из-за унижения. Яра собрал урожай,

обеспечил мне счастливое пребывание и клянется, что не будет создавать неприятностей, так как это не в его интересах.

Это послание он трактовал как секретный текст, написанный специально изобретенным шифром и является шпионским отчетом.

Существуют и иные, не менее фантастические предположения.

Дешифрование фестского диска далеко от завершения.

Письменность майя. Во II–X вв. н.э. на территории современной Мексики (Юкатан) существовала могучая цивилизация, о которой европейцы узнали лишь в середине XVI в.

Среди испанских конквистадоров оказался монах-францисканец **Диего де Ланда**. Его основная цель заключалась в обращении в христианство язычников-туземцев. Однако у последних оказалась высокоразвитая цивилизация. Они хранили рукописные тексты со своими языческими религиозными гимнами, описанием истории народа, его обычаев, обрядов, астрологические календари и др. Поэтому де Ланда в первую очередь занялся уничтожением этих «крамольных» текстов, что ему в достаточной мере удалось. Погибли бесценные памятники древней цивилизации. Сожженные тексты были зафиксированы на длинных полосах бумаги (из папируса, луба и фикуса, сложенные «гармошкой» и были нанесены волосяной кисточкой).

Однако де Ланда совершил и благородный поступок. Сознавая, что губит весьма ценные исторические, написанные кисточкой тексты на папирусах, он скопировал ряд текстов и написал книгу – «Сообщение о делах в Юкатане». Эта книга через несколько веков была обнаружена в испанских архивах и является ценным источником по истории и письменности древнего народа.

В книге Ланда был обнаружен алфавит майя, содержащий 27 знаков. Там же содержался календарь майя и их математические рассуждения. В результате астрономические и математические тексты майя были легко дешифрованы. Оказа-

лось, что майя использовали двадцатиричную арифметику (по числу пальцев на руках и ногах) и использовали особые знаки для обозначения чисел и операций над ними. К этому времени были обнаружены три уникальных рукописи майя в виде записей на архитектурных сооружениях («пирамидах»).

Казалось бы, что алфавит де Ланда решает все проблемы прочтения рукописей майя. Но дело оказалось гораздо сложнее. Во-первых, выяснилось, что алфавит оказался далеко не полным и, к сожалению, весьма искаженным. Во-вторых, письменность майя оказалась не буквенно-алфавитной, а иероглифической. В ней присутствовали знаки, означающие целые слова и понятия; их «побуквенное» чтение невозможно.

Дальнейшие исследования позволили выдвинуть следующие гипотезы:

- письмо содержит фонетические (произносимые) слова и звуки;
- в письме имеются знаки-детерминативы;
- в письме есть слова, читаемые по буквам;
- в письме есть знаки, означающие корни и слоги слов и др.

Некоторые знаки-идеограммы правильно прочитал француз **Л. де Рони**. Его дело продолжил американец **С. Томас**. Но, к сожалению, они дали большое количество ошибочных толкований знаков, что завело последующих исследователей в тупик. Один из источников ошибок – сильные искажения знаков, допущенные переписчиками письменности.

Исследователи вновь вернулись к пиктографичскому («иконографическому») истолкованию знаков письменности майя. Их пытались истолковывать как иконописную письменность, в которой группы знаков изображают нечто конкретно-религиозное, мистическое действие, а не являются записью какого-то буквально понимаемого текста.

Эту идею поддержал американец **Э. Томпсон**, в середине XX в. считавшегося непререкаемым авторитетом в науке о древних майя и их письма. Однако оказалось, что расшифровка новых знаков не помогает толкованию других, вновь появляющихся в письме. Предшествующие исследователи

частично лишь «угадали» некоторые знаки; их «пролонгация» на новые знаки порождала недоумения.

В конечном счете выяснилось, что толкование письма майя как алфавитного, так и пиктографического не подтвердилось. Исследователи пришли в тупик.

В письме майя оказалось около 300 различных знаков-иероглифов, устойчиво повторяющихся в различных сочетаниях. В пиктографической письменности нарастание новых знаков носит устойчивый характер и составляет около 75 новых знаков на каждые 100 знаков последующего текста. Анализ письменности майя такой закономерности не выявил.

Отпала и версия звукового (фонетического) письма. Во всех известных звуковых алфавитах в среднем встречается 30–40 знаков-букв; максимальное их количество никогда не превосходит 80 знаков.

Отпал и вариант слогового письма. В нем обычно 40–50 знаков, но никогда не более 150.

Морфемное письмо также было отвергнуто. В этом письме знаки передают корень слова или грамматические частицы. В таком письме обычно содержится не менее 1000 знаков.

Вариант слово-фразового письма также был отвергнут. В таком письме должно быть не менее 3000 знаков.

В середине XX в. к изучению письменности майя приступил наш соотечественник **Ю. Кнорозов**. В своих исследованиях он применил современные ЭВМ и известные ему криптографические методы анализа текстов. Были тщательно проанализированы не только частоты появления знаков, но и частоты биграмм, триграмм и др.

В результате проведенных исследований Ю.Кнорозов пришел к выводу о том, что письменность майя является смешанной: часть знаков передает морфемы, другая часть – звуки и слоги. Такая письменность уже встречалась ранее: в древнем Египте, Месопотамии и до сегодняшнего дня на Дальнем Востоке. Числовые показатели письма в целом укладываются в «заданные» рамки.

Математические, арифметические знаки письменности были сравнительно легко понятны. Поражала доведенная до

совершенства логичность принятой системы счета (двадцатиричной). В это время в Европе еще считали на пальцах, а майя уже ввели понятие нуля и бесконечно больших чисел. Астрономические достижения майя также поражали. Они очень точно вычислили продолжительность лунного месяца – 29,53086 дня (по сегодняшним вычислениям – 29,53096); солнечный год по майя длился 365,242 дня, что совпадает с современными вычислениями с точностью до 0,0001 дня!

Удивительно, что столь развитая по современным понятиям цивилизация в техническом смысле оказалась первобытной. Майя не знали ни плуга, ни колеса и др. В конечном счете это привело к вырождению цивилизации майя.

Итак, Кнорозов остановился на гипотезе о том, что письменность майя носит иероглифический характер. Начался второй этап исследований.

Существенную помощь в решении задачи могло бы оказать звуковое звучание речи майя («звучание текста»). Но эта речь, как и письменность, были в значительной мере утрачены. Были исторические примеры дешифрования текстов без из смыслового озвучивания (см. язык шумеров и др.). Но знание устной речи могло бы существенно помочь решению задачи.

К середине XX в. сохранились потомки древних майя. Это племя майя-киче. Но их язык существенно отличается от языка древних майя, а письменность и вообще не похожа на древнюю. Кнорозов взялся за изучение общей эволюции языков и письменностей в целях выдвижения гипотез об эволюции языка майя. В этой эволюции прослеживаются определенные закономерности, которые могут помочь созданию «мостиков» из прошлого в настоящее. Большую помощь здесь может оказать изучение устно сохранившихся древних мифов, легенд, басен и др. Другими словами, по этим памятникам культуры можно попытаться пройти «вниз» по историческим слоям, попытаться понять смысл и содержание древних текстов. Ю. Кнорозов обратил в этом смысле внимание на написанную еще в XVI в. книгу «Чилам-Балам», содержавшую басни, прорицания, предания древних майя. Эта книга была обнаружена в XIX в.

Выяснилось, что после завоевания Латинской Америки европейцами книги майя начали записываться латиницей. Ю. Кнорозову удалась попытка «озвучить» язык майя по латинизированной книге «Чилам-Балам». При этом он использовал современный язык книги. Выяснилось, что на европейские языки речь майя трудно переводима. В частности, глаголы майя указывают не только на субъект, но и на объект действия.

Однако Кнорозов показал, что рукописи майя можно в определенном смысле перевести и понять на современных языках, и дал соответствующие примеры (связанные с изображениями «индюк», «собака» и др.). Кнорозов не смог до конца прочитать рукописи майя. Однако проделанная им работа позволила ученому совету, в котором он защищал кандидатскую диссертацию, присудить ему ученую степень доктора исторических наук.

К сожалению, многие авторитетные ученые Запада не признали достижений нашего соотечественника. На Ю. Кнорозова «обрушился» общемировой авторитет в области дешифрования умерших языков – американец **Э. Томпсон**. Один из его аргументов заключается в следующем: «Поскольку в России никогда не было никаких дешифровок, их поэтому там и быть не может». Аргумент оригинален, но не более того.

Тем не менее значительное количество ученых-исследователей древних языков считают работы Ю. Кнорозова недостаточно обоснованными. По общепринятому мнению, дешифрование рукописей майя требует дальнейших усилий. Основная надежда здесь возлагается на появление новых исторических документов.

Письменность о. Пасхи. О древней народности, населявшей о.Пасхи в Тихом океане, европейцы узнали лишь в XVIII в. Остров открыл голландец **Я. Ротвеген** в 1722 г. Это небольшой по площади остров (118 км^2), культура которого относится к полинезийской. Остров, найденный в пасхальное воскресенье, был назван островом Пасхи.

Отважные мореплаватели обнаружили на острове огромные каменные изваяния языческих богов, поразившие их

воображение своими размерами. Но что важнее, были обнаружены письменные тексты аборигенов.

В самом начале были обнаружены 12 деревянных дощечек с вырезанными на них рисунками-надписями. Количество находок быстро возрастало. Однако сама письменность оказалась оригинальной, не имеющей исторических аналогов. Никаких билингв не было и в помине.

Оставалась надежда на возможность восстановления «древнего» языка аборигенов о. Пасхи по языку современных обитателей этого острова. Сразу же оказалось, что и язык, и письменность населения острова в корне отличаются от «древних». Этот язык был назван языком «ронго-ронго» и он исчез где-то в середине XIV в.

Следует отметить, что в середине XIX в. культура местных жителей была начисто обезглавлена. Пираты (в основном португальские каперсы) захватывали и продавали в рабство значительную часть мужского населения (в том числе – вождей, жрецов, сказителей, т.е. носителей культуры). Вернувшиеся из рабства завезли на остров страшную болезнь – чуму. Цивилизация разрушилась.

Новые находки странных дощечек мало прибавили к успеху исследователей. Аборигены уже не могли ни читать, ни говорить по древнему. На вопросы о том, что же содержат таблички, они начинали петь, но одна и та же дощечка получала различные варианты песнопения. «Поющие» дощечки были отвергнуты большинством ученых, но тем не менее нашлись и сторонники этой гипотезы. Вот пример их рассуждений.

Строфа, прочитанная на дощечке, в одном из вариантов прочтения («песнопения») в современном звуковом исполнении дает фразу:

«ТАУРА АТУЛ ТАПА ПУРЕ ТОКО РАНГИ ТЕА» (жрец божества читает молитвы изображению бога РАИАТЕА). Другая фраза имеет вид:

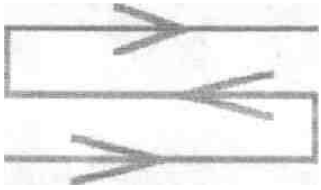
«КАИ РОНГО-РОНГО ТОКОРУА МАРАМА» («исполнять с табличек песнопение для близнецов Солнца и Луны»).

Допустимы и совершенно другие толкования текстов на дощечках. Однако значность толкования не доказана, по-

скольку сходство их «пропения» с оригиналом (к тому же истолкованным по обобщенно-истолкованным песням современных аборигенов) вызывает большие сомнения.

Наш соотечественник Ю. Кнорозов заинтересовался письмом ронго-ронго. Он достаточно убедительно показал, что все попытки свести дешифрование этого письма к вариантам А и Б несостоятельны. И язык, и письменность аборигенов о. Пасхи изменились коренным образом.

К исследованиям ронго-ронго в середине XX в. подключился известный норвежский путешественник, ученый-историк **Тур Хейердал**. Ему удалось обнаружить на о. Пасхи рукописные тетради (на бумаге). Удалось установить, что они написаны «обратным способом письма» по следующему пути написания:



Однако ни новые находки, ни новые гипотезы не привели к прочтению умершего языка. К настоящему времени отпали наиболее популярные гипотезы. К ним относится и гипотеза об использовании примитивного словесно-слогового иероглифического письма. Это письмо родственно *морфемному*. Напомним, что морфемы – это части слова (корень, префикс, окончание и др.). Они отличаются от слогов. Так, например, слово ПОЛЕТЕЛИ содержит 5 морфем: префикс ПО, корень ЛЕТ, суффиксы Е и Л, окончание И. Слогов в этом слове 4: ПО-ЛЕ-ТЕ-ЛИ. Исследования продолжаются.

Критские письмена. В конце XIX в. на о. Крит (Средиземное море) были найдены глиняные таблички с неизвестными надписями. Аналогичные таблички были обнаружены и на материковой части Греции. Один из первых исследователей текстов – **А. Эванс** (Англия) – обнаружил наличие двух

различных письменностей на найденных табличках. Они относились ко второму тысячелетию до н.э. Эти письменности получили обозначения «А» и «Б» с добавлением: «линейные письма А и Б». Эванс высказал предположение о том, что тексты написаны на древнегреческом языке. Однако эта догадка не привела к легкому дешифрованию письмен.

Усилиями последующих ученых было установлено, что письмо Б действительно написано на греческом языке, но при использовании другого, символического алфавита. Основная заслуга в этом поиске принадлежит англичанину **Вентрису**. По сути дела он отождествил разгадку письмен «Б» с решением проблемы дешифрования шифра простой замены при наличии найденных им греческих эквивалентов «открытого текста».

Представляет интерес высказывания Вентриса о проблеме дешифрования умерших языков: «Дешифровка – дедуктивная наука, использующая контролируемый эксперимент. Она формирует гипотезы, которые проверяются и часто отбрасываются. Однако то, что остается после проверки, обрастает новыми фактами, и вот наконец, исследователь начинает ощущать твердую почву под ногами: его гипотеза согласуется с фактами, осмысленные куски текста высвобождаются из вековой тьмы. Ключ к шифру найден».

Таким образом Вентрис формулирует главный критерий истинности дешифрования: осмысленное прочтение «шифрованного» текста и доказательство единственности соответствующего «открытого» текста.

Решение Вентриса было перепроверено с помощью новых находок и полностью подтвердилось.

С дешифрованием линейного письма А дело обстояло сложнее, Выяснилось, что дешифрование письма Б мало помогает дешифрованию письма А. Язык этого письма (А) оставался неизвестным. Различные гипотезы отвергались. В этих исследованиях применялись вероятностно-статистические методы, по аналогии совпадающие с криптографическими методами первичного анализа шифрованных текстов. На этом пути не оправдались поиски родственных (по статистическим

особенностям текста) языков. Но некоторые аналоги оказались оправданными, однако этого не хватало для продолжения дешифрования. Находки остались лишь частными догадками.

Тайна линейного **письма А** не раскрыта до сих пор.

Экзотика. Таинственность умерших языков прождала и порождает фантастические предположения об их происхождении. Заметное место в этих предположениях занимает космический характер непонятных текстов. В качестве примера приведем эпизод, описанный известным писателем и журналистом **Ю. Семеновым** в книге «На «козле» за волком» (М., 1974). В одной из своих многочисленных зарубежных командировок Ю.Семенов оказался в Историческом музее Японии. Экспозиции музея произвели на него большое впечатление. Наскальная живопись, фантастические цветовые эффекты, космические шлемы на головах будд и др. подвели автора к оригинальным выводам. Один из этих выводов связан с предполагаемым космическим происхождением таинственных текстов. При этом он ссылается на результаты исследований, проведенных белорусским ученым **В. Зайцевым**.

Позволим себе привести пространную выдержку из книги Ю. Семенова.

«На границе между Китаем и Тибетом находится горный пещерный район Байян-Кара-Ула. Вот уже четверть в. в этом районе археологи находят странные каменные диски, исписанные непонятными „ эрами и иероглифами. Несколько тысяч лет тому назад с помощью неизвестных орудий труда жители пещер высекали из камня эти диски, которых найдено уже 716 штук.

Все диски, подобно граммофонным пластинкам, в центре имеют отверстие, от которого спирально отходит двойной желобок, доходящий до периметра диска. Об этих желобках немецкий журнал пишет:

«Очевидно, это не звуковые бороздки, а письмена, самые странные, которые когда-либо были найдены в Китае, да и во всем мире».

Археологи-дешифровальщики двадцать лет ломали голову над раскрытием тайны дисков. По мнению Семенова разгадка оказалась настолько поразительной, что Пекинская академия наук не разрешала ведущему профессору-исследователю публиковать свои работы. Вывод этого профессора заключался в следующем: «Бороздчатые письмена, повествующие о космических кораблях, которые, по свидетельству надписей на дисках, существовали 12000 лет тому назад».

В высокогорных пещерах Байян-Кара-Ула живут племена **дропа** и **хам**. Люди этих племен очень малорослы и тщедушны. Рост их примерно 1 м 30 см. До сих пор ученые не могли отнести их к какой-либо конкретной этнической группе. Сведения об этих племенах весьма скупы.

Расшифровав иероглифы на дисках, китайский археолог и его коллеги нашли в тексте упоминание о народах дропа и хам: «...Дропа спустились с облаков на своих воздушных глиссерах. Десять раз до восхода солнца мужчины, женщины и дети прятались в пещерах. Наконец они поняли знаки и увидели, что на этот раз дропа прибыли с мирными намерениями...».

По мнению китайских археологов, иероглифы Байян-Кара-Ула таинственны до такой степени, что толкование их и использование с научной целью возможны только с большой осторожностью.

Для получения дополнительных данных о дисках с них соскоблили частицы камня и отправили для анализа в Москву. Здесь было сделано удивительное открытие. Диски содержали большое количество кобальта и еще какого-то металла. Другие исследования выявили необычный ритм вибрации, словно диски были заряжены и когда-то включены в цепь, служа проводником электричества.

До сих пор диски Байян-Кара-Ула представляют неразрешенную загадку, связанную с какими-то событиями глубокой древности.

Древние китайские легенды повествуют о маленьких человечках, худых, желтолицых, которые якобы приходили с облаков. Эти человечки были безобразны: они имели огром-

ные головы и чрезвычайно худые и щуплые тела. Их безобразие вызывало в земных племенах чувство отвращения и было причиной того, что все избегали их, а какие-то «люди на быстрых лошадях» их избивали.

Таковы легенды. Но действительность подтверждает эти легенды:

Археологи и спелеологи находят в пещерах Байян-Кара-Ула остатки могил и скелетов давностью 12000 лет. Эти останки принадлежат людям с огромными черепами и слаборазвитыми скелетами. Первые китайские археологи, открывшие захоронения, в своих отчетах писали об «исчезнувшем виде обезьян? Но ведь до сих пор никто не находил ни обезьяньих могил, ни дисков с письменами, созданными доисторическими обезьянами.

...Японские археологи во время раскопок, произведенных в различное время в префектурах Аомори и Иватэ, обнаружили статуэтки, изображающие каких-то людей или человекоподобных в странных костюмах типа скафандров и шлемах, закрывающих всю голову. На шлемах ясно видно что-то вроде щелевых очков, дыхательных фильтров, антенн и слуховых аппаратов. Скафандры снабжены даже «приборами ночного видения». Эти статуэтки получили название «догу»...

В одной японской сказке из сборника «Ниппон Мукаси Банаси» рассказывается, что человек вернулся из космического путешествия молодым, но не застал дома даже своих потомков. («Почему так скоро? Ведь я у тебя тут только два часа был? Ангел ответил: «Не два часа, но тридцать два г.»).

Пророк был сражен этими словами. Он понял, что возвращение на Землю будет означать для него либо смерть, либо глубокую старость, – ведь он не заметил, что на небе постарел на целых тридцать два года. И он взмолился: «Зачем мне возвращаться в плоть мою дряхлую?» – и скорбел пророк. Но ангел его утешил: «Не скорби, ты не будешь старым».

А мы только в начале XX в. из открытия А. Энштейна узнали о возможных причудах времени, связанных с движением тела на околосветовых скоростях.

...Справедливы эти гипотезы или нет, они всегда определяли направление научных поисков. Гипотеза – это сегодняшний день завтрашней науки. Правда, не каждая из них может стать теорией. Мир знает и такие, которые не были доказаны в течении нескольких столетний. Даже опровергнутая гипотеза полезна, ибо для того, чтобы отрицать, нужно накопить много положительных знаний. «Лучше держаться такой гипотезы, которая со временем окажется неверной, чем никакой , – так говорил Дмитрий Менделеев.

Такова суть рассказа Ю. Семенова. Следует отметить, что имеют место многочисленные попытки связать криптографию с возможностью обмена сообщениями с внеземными цивилизациями (если они существуют). Можно согласиться с тем, что общение на разных языках, принятых в различных цивилизациях, по необходимости будет использовать и криптографические методы.

Однако перед официальной государственной криптографией стоят сейчас проблемы вполне земные – защита собственной конфиденциальной информации и раскрытие систем защиты потенциальных противников. В этом сегодня и заключается смысл деятельности государственных криптографических организаций.

В заключение подраздела приведем фантастические предположения о некоторых возможностях применения криптографии. Речь идет о дешифровании сообщений из **космоса**. Предполагается, что эти сообщения направляют нам внеземные цивилизации.

Мнения ученых о возможности существования разумной внеземной жизни разделились.

Часть ученых склоняется к тому, что внеземные цивилизации не существуют. Земля – уникальное космическое образование. Возникновение жизни на Земле было связано с таким редким стечением различных обстоятельств, что они едва ли могли бы повториться еще где-либо. Религия активно поддерживает эту позицию, поскольку саму Землю и жизнь на ней создал Бог. Едва ли он был озадачен проблемой создания других миров.

Другая группа ученых, допуская возможность существования иных разумных миров, категорически отрицает возможность установления контактов с ними. Одна из причин заключается в том, что такие миры весьма удалены от нас, так что даже свет проходит соответствующее расстояние за многие миллионы лет. Поэтому не имеет смысла тратить силы и средства на попытки установления контактов. Известный писатель-фантаст Г. Уэлс, отмечая бессмысленность поиска внеземной жизни, отмечал: «Ни одно животное не станет смотреть вверх. Только это нелепое создание – человек – тратит время попусту, глазея на небо». Естественно, здесь имеет место своеобразный юмор.

Наконец, ученые-оптимисты (энтузиасты) считают, что внеземные цивилизации существуют и с ними можно установить реальный контакт. Именно они и рассматривают такой вопрос, как возможность применения криптографических методов в процессе установления этих контактов. Предположения этих ученых и рассматриваются далее.

Еще древнеримский поэт, философ и просветитель Тит Лукреций Кар (I в. до н.э.), разъясняя свою позицию по поводу образования космических тел, писал:

«Если ты это как следует понял
Природа свободной сразу тебе предстает
Лишенной хозяев надменных»

Однако существование богов Лукреций не отрицал, но богами для него была сама природа. Он заметил: «Крайне невероятно, что эта земля и небо – единственные, которые были созданы». Эта точка зрения нашла определенную поддержку от древних ученых до ученых нашей современности.

Известный астроном К.Гюйгенс, открывший кольца Сатурна несколько веков назад, писал: «А почему у каждой из этих звезд или солнц не может быть как у нашего солнца такой же свиты планет со своими лунами?». Отметим, что в наше время обнаружены 19 планет в ближайших к нам звездных системах. Эти планеты аналогичны планетам нашей солнечной

системы. Английский епископ Д. Уилкинс, опубликовавший первую английскую книгу по криптографии (еще в XVII в.) на английском языке, написал трактат на тему: «Открытие мира на Луне, или трактат, имеющий тенденцию доказать, что не исключена возможность существования еще одного мира на планете».

В эпоху Возрождения английский поэт Мильтон писал о том, что существуют иные миры, отличные от мира Адама и Евы.

В конце XIX в. итальянец Дж. Скиапарелли открыл ныне широко известные «каналы» на Марсе. Возникло предположение, что эти каналы созданы разумными существами. Как отмечалось ранее, в XIX в. были обнаружены планетарные системы (звезды и сопутствующие им планеты), аналогичные нашей. Был сделан вывод о том, что в этих системах присутствует по крайней мере одна «Земля». Итак, если внеземные цивилизации (инопланетяне) существуют, то контакт с ними может иметь двоякий характер:

- личный контакт (представители цивилизаций находятся рядом друг с другом);
- внеличностный контакт (в этом случае возникает проблема передачи информации по какому-либо каналу дальней связи).

Общая проблема в обоих случаях заключается в том, что ни язык, ни его «письменная» (физическая) реализация неизвестны. Это напоминает ситуацию варианта «В» при дешифровании умерших языков. Задача – свести эту ситуацию к вариантам А и Б.

При личном контакте возможна передача информации лишь путем прямого воздействия на органы чувств. При этом учитывается тот факт, что инопланетяне могут иметь «набор из других чувств». Но первые предположения опираются на гипотезу о том, что у «них» тот же набор, что и у «нас». В рамках такого предположения рассматриваются следующие возможности.

Земной человек обладает пятью органами чувств:

1) обоняние (ощущение запаха). Исследователи сразу же отвергли этот канал связи. Различать тонкие запахи посильно

лишь парфюмерам. Передать содержательную информацию путем тонкого сочетания запахов весьма проблематично;

2) вкус (ощущение сладкого, соленого, острого и др.). Отвергнут по тем же причинам;

3) осязание (физическое, «тепловое» восприятие информации). Этот способ возможен, но маловероятен. Есть примеры, когда глухонемой человек воспринимает речь говорящего путем наложения пальцев на его горло и внутреннего анализа исходящих физических колебаний. Есть примеры сознательного кодирования информации в форме, доступной осязательному восприятию адресатом. Например, четыре нажатия пальца означают «стол», три нажатия – трехножная табуретка и др. Известная «азбука» Брейля, предназначенная для слепых людей и передающая конфигурацию букв по чувственному восприятию специально разработанной рельефной методике их фиксации (на носителе), позволяет слепым читать пальцами специально подготовленные для них тексты. Однако и этот вариант отвергнут;

4) остаются лишь зрение и слух. 'Этот подход наиболее реален. Показать предмет (например, «стул»), назвать его, а затем и показать его функциональное назначение (сесть на стул) действительно является наиболее совершенным (по земным меркам) объяснением для инопланетян значения и звучания понятия «стул». При этом можно и обучать «их» правилам земной арифметики: показать стул, нажать на «руку» адресата четыре раза (четыре ножки); показав табуретку с тремя ножками, нажать три раза и др.

Заметим, что в данном случае речь идет только о сознательной передаче информации инопланетян. А как понимать передаваемую ими инфрмацию? Ведь «они» могут пользоваться совершенно другой «математикой-арифметикой»? Например, использовать другую систему исчисления. В этом случае передача числа «четыре» в двоичном коде, например, может иметь вид паузы (при «нажатии» младшего разряда и одного активного нажатия в разряде следующем). Вообще «они» могут пользоваться системой счета, в которой число

обозначается, например, визуально воспринимаемым предметом («точка» = 1, «прямая» = 2, «треугольник» – 3 и др.).

Таким образом, в плане передачи информации инопланетянам, возникает проблема не криптографии (тайнописи), а «клерографии» («всем понятное письмо»). Здесь мы имеем дело, по словам Д. Кана, с «антикриптографией».

Наиболее вероятным считается внеличный контакт. С этой целью изучаются сигналы, поступающие из космоса. Используются мощные телескопы, радиотелескопы, радиотехнические методы выделения сигналов на фоне «шума» и др. Заметим, что в этих работах принимал участие известный ученый-криптограф **У. Фридман** (США). Неоднократно объявлялось о находке «разумных сигналов», но в конечном счете это оказывалось ошибкой. С Земли отправлялись радиосветовые сигналы, ракеты-контейнеты с символическими записями, радиоаппаратурой и др.

Но надежд на установление контактов пока очень мало. Нашумевшие в наше время сообщения о якобы имевших место контактах людей с разумными существами, прилетевшими к нам на неопознанных летающих объектах (НЛО), не находят обоснованного научного подтверждения. То же самое касается и телепатической связи, якобы используемой пришельцами.

Тем не менее энтузиасты не оставляют своих надежд. Один из важных вопросов для них – как распознавать язык посланий из космоса. Русский ученый-лингвист Н.Д. Андреев (АН СССР) предложил метод, который по его мнению, позволит людям расшифровать любой язык. Этот метод он назвал «статистико-комбинаторным анализом». В нем используются статистические особенности текстов, по существу аналогичные методам криптографического исследования открытых текстов (частоты букв, биграмм, длины слов и расстояния между ними и др.). Он подтвердил работоспособность своего метода некоторыми примерами на текстах различных языков. Однако возникают сомнения, которые можно, в частности, выразить в одном вопросе: если метод действительно универсален, то почему же до сих пор сохраняется тайна умерших на Земле языков?

Для общения с инопланетянами предлагается разработать некоторый универсальный, понятный всем мыслящим существам язык. В основу разработки этого языка кладется опыт создания «земного универсального языка» – **эсперанто**. Разработки универсальных языков начались еще в начале XVII в., когда латинский язык еще продолжал держать статус международного языка, но уже начал утрачивать свои позиции. В XVII в. Р. Декарт (математик и философ) поставил задачу разработки универсального «философского языка». В этом языке предполагалось выделить основные понятия, которые можно было бы объединять по правилам строгой логики в предложения, а затем и в содержательные тексты. О таком языке мечтал и другой великий математик – Лейбниц. Он пытался выделить так называемые «монады» – элементарные содержательные элементы («молекулы») текста, с помощью которых можно строить любые осмысленные тексты. Однако исследования в этом направлении окончились неудачей, поскольку, в частности, по необходимости они опирались на свойства определенных языков и соответствующих письменностей.

Предлагались и другие, оригинальные методы создания универсальных искусственных языков. Например, одно из предложений опиралось на идею передачи информации с помощью музыки. По предположению, «музыкальные фразы» по своему гармоническому строю доступны для понимания чувствами, эмоциями человек независимо от языка, на котором говорит слушающий музыкальное произведение. Действительно, произведения классиков мировой музыкальной культуры оказывают идентичное эмоциональное воздействие на слушателей любой национальности (вызывая чувство тревоги, страха, радости, сомнения и др.). С помощью музыкальных нот можно передавать содержательную» мелодию. Так, сочетание нот «доми-соль» (весьма гармоничное по восприятию и идущее снизувверх) означает слово «бог»; обратное сочетание («соль-ми-до») содержит идею «опускания вниз», т.е. вполне может служить обозначением «сатаны». Автор этой идеи, француз Ж.Ф. Сюдр, заметил, что такой язык можно не только «петь», но и выражать в красках (если семь нот заменить семью цветами).

В конце XIX в. итальянский математик Дж. Пеано (это имя известно любому современному математику) предпринял попытку свести язык к некоторым формулам, используемым в математике и логике. Предложения (идеи) являются отображением множества входящих в него слов в множество осмысленных предложений (идей). Правило понимания возможного высказывания, содержащегося в предложении и скрывающегося за данным набором слов, определяются строгими законами логики. Для обозначения логического понимания терминов Пеано предложил специальные, искусственные знаки, которые используются и в наши дни. Последователи Пеано пытались, но безуспешно, перенести его методологические предпосылки для решения проблемы общения с инопланетянами. В формальной математике идеи Пеано положили начало новому математическому направлению исследований – математическая логика.

Проводились исследования и иных способов передачи информации. Оказалось, что «язык животных» достаточно содержателен. Так, например, известный «танец пчелы» способен передать информацию от пчелы-разведчицы к пчелам улья не только о факте самой находки нектаросодержащего места, но направление и расстояние до него; пчела при этом использует различные внешние характеристики «танца»: скорость вращения вокруг оси, амплитуды «выбросов» в разные стороны и др.

Исследовались «языки» кур, собак, дельфинов и др. Действительно, эти животные способны воспринимать значение некоторых слов-команд, поданных человеком, но этого совершенно недостаточно для установления взаимного, полноценного информационного контакта.

Д. Кан, оптимистично настроенный на возможность контактов с высокоразвитыми внеземными цивилизациями, пишет: «... человек прочтет любое сообщение, которое может прийти от звезд. Может статься, что однажды Земля обогатится глубочайшими познаниями сверкающих цивилизаций...»

В заключение отметим, что профессиональный криптограф решает «чисто земные» задачи. Он защищает информацию и преодолевает защитные меры противника, имеющего

«чисто земное» происхождение. Тем не менее, исследователи «умерших», «космических» языков находят оригинальные методы, которые представляют определенный интерес для криптографии. Знакомство с этими метода и может оказаться небесполезным для специалиста-криптографа.

Дешифрование умерших языков нередко по необходимости использует методы криптографии. Однако следует отметить одно существенное отличие проблем, стоящих перед официальными, профессиональными криптографами и учеными-дешифровальщиками умерших языков.

Официальный (государственный) криптограф имеет дело с противником, который сознательно разрабатывает методы защиты (шифрования) информации. По словам А. Эйнштейна, природа сложна, но не злонамеренна. Поэтому дешифровальщик умерших языков имеет дело не с сознательным сокрытием тайн, а лишь с утерянными, но в свое время общеизвестными способами материальной (письменной) записи информации. В этом смысле он может в своих исследованиях опираться на поиски новых исторических источников информации, которые могут помочь ему в решении стоящих проблем (аналогичные язык и письменность, преемственность письменности и др.).

Отметим, что шифр и ключ в их строгом научном понимании в «дешифрованных» письменностях отсутствуют.

Сознательное сокрытие тайны (шифрование) обладает существенными особенностями. Защищающий информацию обязан учитывать возможности «противника», который использует все доступные ему средства для раскрытия интересующей его тайны. Поэтому при создании способов защиты необходимо учитывать силы и средства, которые противник может направить на дешифрование. Однако противник скрывает свои силы, средства, методы дешифрования, и поэтому защищающийся может лишь оценивать способности противника. В этой оценке могут появляться «прорехи», и тогда все усилия по защите могут свестись «на нет». Здесь идет уже интеллектуальная воина, воина, в которой побеждает наиболее подготовленная сторона. Перед дешифровальщиками умерших языков такие проблемы не стоят.

Отметим еще один важный момент. Перед современным официальным (государственном) дешифровальщиком стоит серьезная проблема: нужно не только дешифровать сообщение, но и сделать это «вовремя». Если текущая секретная информация дешифрована поздно, то ее ценность может свестись к нулю. Информация «текущего времени» достаточно быстро «устаревает». Историческая информация не предъявляет таких требований по «скорости дешифрования». Здесь можно работать спокойно и неспешно.

Отметим и еще один момент. При сознательном сокрытии тайны можно использовать и такой прием. Если есть серьезные опасения о надежности защиты, то защищающаяся сторона может «подсунуть» дезинформацию противнику, прикрывая ее своим «надежным шифром», т.е. дезинформировать противника. В исследовании умерших языков этот прием исключен. Некого и незачем дезинформировать через столетия. Проблема борьбы с дезинформирующим противником перед де-шифровальщиками умерших языков не возникает.

Тем не менее, ознакомление ученых-дешифровальщиков умерших языков с основами криптографических методов дешифрования безусловно целесообразно. Одновременно современному специалисту-криптографу небесполезно ознакомиться с приемами дешифрования умерших языков. Это знакомство может навести на новые, оригинальные методы дешифрования секретной переписки.

9.2. Дешифрование языка майя[1]

Аббат Шарль Этьен Брассер де Бурбур – известный французский американист – в 1863 г. нашел в библиотеке Мадридской академии истории манускрипт «Сообщение о делах в Ютакане, извлеченное из сообщения, которое написал брат Диего де Ланда ордена св. Франциска». Помимо истории покорения испанцами народа Юкатана в этом манускрипте повест-

[1] Приведенные ниже материалы полностью основаны на работе: Кузьмищев В. Тайна жрецов майя, Молодая гвардия, 1968.

вовалось о страшных событиях 12 июля 1562 г., когда многие индейцы майя были обвинены в ереси и попали на эшафот, были уничтожены священные реликвии майя, преданные аутодафе. Эта рукопись открывала след, который вел к древним майя. Идя по нему можно было проникнуть в глубь истории этого великого народа. По иронии судьбы этот след эту «тропинку» отдавал в руки человечества тот, кто уничтожил важнейшие документы для изучения народа майя – их рукописи.

Попытки дешифрования. Обнаруженный Брассером де Бурбуром манускрипт был копией составленного Ландой «Сообщение о делах в Юкатане», переписанной с должным старанием тремя неизвестными писцами в 1616 г. Она хорошо сохранилась, сравнительно легко читалась, и, хотя переписчики допустили (очевидно, сознательно) ряд сокращений, к счастью, они сохранили наиболее ценные части оригинала, в том числе очень важный для решения рассматриваемой проблемы список 27 алфавитных знаков, которыми, по словам Ланды, пользовались писцы древних майя. В своем сообщении Ланда дал огромную и ценнейшую информацию об индейцах майя. Она помогла и продолжает помогать сегодня раскрывать многие тайны их великой цивилизации.

Правда, есть немало оснований полагать, что подлинным автором, или по крайней мере соавтором, является Гаспар Антонио Чи – главный «консультант» по древним майя не только самого Ланды, но и многих других испанцев, которые неоднократно упоминают его имя в своих сообщениях того периода. Однако нет (или не сохранилось) ни письменных, ни устных свидетельств, которые подтверждали бы с должной достоверностью такое предположение, и поэтому Ланда имеет полное право единолично претендовать на авторство сообщения – основного, наиболее полного и при этом весьма точного документа о древних майя.

Не вызывает сомнений, что Ланда действительно был выдающимся знатоком индейцев майя и их удивительной цивилизации. Но это еще больше отягощает его вину за бесчеловечное обращение с индейцами и уничтожение бесценных

сокровищ их древней культуры. Подобному «деянию» католического монаха нет никаких оправданий!

В «Сообщении о делах в Юкатане» Ланда записал легенды о прошлом майя. Многие из них, очищенные от двойной мистической приправы – майя и католической, легли в основу хронологии и истории майя. Он рассказал о быте, обычаях и религии этого народа, о том, чем питались майя, как одевались и что строили, чему радовались и отчего печалились; как женились, воспитывали детей и хоронили умерших; он описал их ремесла, торговлю, земледелие и даже правосудие. Его подробные, хотя и тенденциозные – ведь он был католическим монахом, – записи довольно полно раскрывают духовный мир майя – мрачный и откровенно жестокий во всем, что касалось их религии, даже если сделать скидку на тенденциозность францисканского монаха.

Ланда помог понять и изучить на основе собранного в сообщении материала систему летосчисления и календаря майя, их счет, который кстати сказать, был двадцатеричным. В результате календарные знаки, как в рукописях, так и на других памятниках культуры майя сравнительно легко поддались расшифровке (перед исследователями ведь был не такой уж сложный календарно-цифровой код, которому соответствовали даты и числа, а не древний язык) и стали достоянием не только ученых.

Наконец, Ланда дал довольно подробное, хотя и путаное, описание письменности майя и записал «алфавит», ставший впоследствии знаменитым. Конечно, Ланда не предполагал, что три столетия спустя вокруг «алфавита» возникнут ожесточенные споры и зародится полемика длинною в целый век; что его «алфавит» будет порождать надежды и с одинаковой легкостью убивать их; вызывать страстные дискуссии, доходящие порой до откровенной ругани в среде ученых мужей, и заставит сесть за дешифровку письменности майя как маститых ученых, так и совсем еще юных студентов и даже школьников…

Иными словами, Диего де Ланда и его «Сообщение о делах в Юкатане» сегодня, как и 100 лет назад, стоят в центре всех исследований, которые связаны с историей и культурой древних народов Америки. Именно поэтому найденный

Брассером де Бурбуром в испанских архивах манускрипт столь сильно взволновал ученых. Но больше всего их обрадовал так называемый «алфавит Ланды».

Однако разве Ланда не уничтожил все рукописи майя и тем самым не «обезвредил» составленный им самим «алфавит»?

К счастью от костров испанской инквизиции чудом все же уцелели три ставшие уникальными рукописи майя. Кроме того, на древних архитектурных сооружениях этого великого народа-строителя были обнаружены многочисленные знаки, высеченные на камнях либо вылепленные на гипсовых барельефах, весьма схожие с теми, что заполняли рукописи. Во время раскопок, которые к моменту открытия Брассера де Бурбура весьма робко, но все же велись на развалинах древних столиц, крупных центров и больших и малых городищ майя, археологи нашли высокие продолговатые камни – стеллы, сплошь разукрашенные теми же таинственными знаками. Надписи попадались и на пластинах, статуэтках и других мелких украшениях. Словом к концу XIX в. накопилось немало текстов майя.

Казалось, что теперь перед учеными стояла предельно ясная задача: пользуясь «алфавитом Ланды», который к тому же дает в своем сообщении три примера написания с его помощью слов, прочесть древние рукописи и другие тексты. Но первые же попытки решить столь простую на первый взгляд задачу потерпели провал.

Первым приступил к чтению знаков письма майя сам Брассер де Бурбур. И он действительно «прочел», но только не знаки, а то, что ему хотелось. «Ожившие вулканы… содрогание земли… извержение лавы…» (в «переводе» Брассера де Бурбура, который был страстным сторонником существования и гибели от катастрофы мифической Атлантиды) впоследствии оказались… лишь списком дней из календарей майя!

Подобных «переводов» появилось немало; они делались как с помощью «алфавита Ланды», так, впрочем, и без него. Рекорд фантазерства принадлежит французу Ле Плонжону: он умудрился объявить «космогонической поэмой», повествующей (конечно, на языке майя) о гибели Атлантиды, названия букв греческого алфавита – альфа, бета, гамма и т.д.!

Правда, серьезные ученые сразу же отвергали подобные дилетантские «открытия» незадачливых дешифровальщиков.

Уже в 1881 г. знаток древневосточных письмен Леон де Рони предпринял серьезное изучение письма майя. Сделав предложение, что письмо майя является иероглифическим, т.е. аналогичным древним иероглифическим письменам Китая, Египта, Вавилона, он стал искать в нем три типа знаков, являющихся «китами», на которых держится любое иероглифическое письмо: *идеографические*, передающие корни слов; *фонетические*, передающие один слог или один звук; *ключевые*, или *детерминативы*, знаки, которые употребляются для пояснения смысла слова, хотя сами не читаются. Например, слово «лев» может служить для обозначения животного и собственного имени; благодаря знаку-детерминативу читатель определит, о чем именно идет речь.

Используя знаки «алфавита Ланды» и остроумно комбинируя их с материалами рукописей, де Рони удалось обнаружить знаки-идеограммы для названий цветов, найти иероглифы, обозначающие четыре стороны света. Более того: он показал, что в письме майя были фонетические (т.е. алфавитные или слоговые) знаки, и привел пример слова, записанного такими знаками: куц (индюк).

Работы Леона де Рони продолжил американский ученый Сайрус Томас, однако вместо ключа к дальнейшей дешифровке письма майя их усилиями невольно был создан крепкий замок, который замкнул двери перед несколькими поколениями исследователей, пытавшихся проникнуть в тайну письма. Дело в том, что и де Рони и особенно Сайрус Томас допустили массу ошибочных и произвольных толкований знаков.

Это было связано в первую очередь с тем, что, как ни старались переписчики рукописи Ланды, они все же сильно исказили знаки «алфавита», и отождествить их с древними иероглифами было чрезвычайно трудно. Именно поэтому оба ученых допустили серьезные палеографические ошибки.

Случилось так, что эти досадные сами по себе ошибки сыграли роковую роль в исследовании письменности майя. Они послужили для доказательства правоты тех исследователей, ко-

торые отрицали существование у майя иероглифического письма, передающего звуковую речь. Ошибочное определение рисунка знаков породило утверждение, что письмена майя нельзя читать, как, скажем, древнеегипетские или китайские иероглифы, ибо им не соответствуют какие-либо единицы языка, а можно лишь толковать тот или иной знак. Следовательно, говорили эти ученые, письмо майя является иконографическим, т.е. каждый знак или группа знаков – это «икона», изображение чего-то совершенно конкретного, а раз так, толкование одного знака ни на йоту не поможет толкованию другого.

Их идейным вождем стал американский профессор Эрик Томпсон, многие годы, вплоть до самых последних лет считавшийся непререкаемым авторитетом в науке о древних майя и их письме. Он громил любую попытку доказать, что письменность майя иероглифическая, используя для этого ошибки своих оппонентов, главным образом в палеографии, иными словами, в умении правильно определить рисунок знака или их сочетания. Томпсон категорически заявлял, что расшифровка новых знаков в письменности майя не упрощает задачу толкования остальных, как это бывает, например, в письме, где употребляется алфавит или в кроссворде. Он безапелляционно объявил, что Ланда ошибся в попытке получить алфавит майя у своего «консультанта», ибо знаки майя обычно передают слова, изредка, может быть, части сложных слов, но, решительно настаивал Томпсон, не буквы алфавита.

Даже крупный американский лингвист, один из пионеров современного языкознания, Бенджамен Ли Уорф, выступивший против этого категорического и безапелляционного суждения своего соотечественника, был подвергнут уничтожающей «критике» Томпсона. На работах Уорфа был поставлен крест. К сожалению, он допустил серьезные палеографические ошибки в своей попытке на практике доказать, что письмо майя было иерографическим и передавало звуковую речь, а не набор разрозненных знаков-ребусов, что и предопределило финал научной баталии.

След, который нашел Брассер де Бурбур, на этот раз, казалось, был утерян окончательно.

С чего начать? Перед вами рукопись на неизвестном языке. Вернее, вы еще не знаете, так ли это, а только предполагаете, что стройные ряды и колонки тщательно выведенных замысловатых знаков и значков, разноцветных рисунков и орнаментов являются рукописью. Иногда проходят годы и даже десятилетия – история знает такие примеры, – прежде чем предположение превращается в уверенность, в твердое убеждение, непоколебимую веру, что это действительно рукопись.

Молодой дешифровальщик, впрочем пока только он один называет себя так, уже который раз вглядывается в серобелые листы фотобумаги, на которых изображены страницы рукописей. Их, рукописей, только три.

Одна хранится в Дрездене. На длинной полосе бумаги, сделанной из луба фикуса и сложенной складками, наподобие веера или мехов у гармошки, волосяной кисточкой на 74 страницах нанесены таинственные знаки и непонятные рисунки. Другая рукопись, хранящаяся в Мадриде, состоит из двух фрагментов – всего 112 страниц – и также сложена складками, однако у нее нет начала, это сразу видно, нет и конца. В еще худшем состоянии рукопись, найденная Леоном де Рони в архивах парижской библиотеки. Это даже не рукопись, а фрагмент из 24 страниц, к тому же сильно поврежденный.

И все. Все, что уцелело от костров испанской инквизиции, уничтоживших 400 лет назад рукописи индейцев Майя.

С чего начать? Как подступиться к ним? Как заставить заговорить этих древних свидетелей выдающейся цивилизации Американского континента? А может быть, американский профессор прав, и они вообще не умеют говорить?

Тогда, много лет назад, выпускник Московского университета Юрий Кнорозов не мог дать ответа на эти и еще многие другие вопросы, возникавшие у каждого, кто хоть раз увидел рукописи майя. Он знал многое – вернее, почти все, что было опубликовано в мировой печати об этих манускриптах, вот уже почти столетие плативших черной неблагодарностью – молчанием всем тем, кто стремился проникнуть в их тайну.

Он изучил древние письмена Старого Света, тщательно присматриваясь к особенностям иероглифики китайцев и

древних египтян; он искал социально-исторические причины возникновения письма у народов, которые прошли примерно тот же исторический путь, что и майя. Он был лингвистом, историком и еще… Он считал, что гуманитарные науки следует вывести на уровень точных наук, и много думал о новом открытии, которое несправедливо оскорбили люди, не сумевшие или не пожелавшие разобраться в этом дерзновенном полете человеческой мысли, приклеив ему ярлык мракобесия… Да, он думал о кибернетике, о возможностях ее применения в лингвистике, о совершенно невероятном на первый взгляд сочетании «думающих» машин с наукой языкознания… Это была мечта, но мечта, построенная на строгом научном анализе молодого ученого, понимавшего, какой невероятно тяжелый труд ждет его впереди, сколько препятствий ему придется преодолеть, сколько неудач и разочарований поджидает его.

Однако он знал, он непоколебимо верил, что рукописи можно заставить заговорить. Только вот как?..

Шел 1950 г.

Что такое дешифровка. В самом деле: что такое дешифровка? В строго научном понимании дешифровка означает отождествление знаков исследуемого письма (текста) со словами языка, записанного, как предполагается, с помощью этих знаков или их сочетаний, совокупность которых в разнообразных комбинациях и составляет изучаемое письмо.

Это, так сказать, гражданское понятие дешифровки. Понятие военной дешифровки[1] возникает лишь постольку, поскольку появляются тексты, совершенно сознательно и пред-

[1] Используемое авторами название «военная дешифровка» чисто условное; авторы прибегают к нему лишь для того, чтобы отличить его от интересующей нас проблемы дешифровки неизвестных исторических письмен, именуя эту последнюю гражданской; сразу оговоримся, что в задачу настоящей книги не входит исследование сложнейшего процесса межгосударственных отношений, внутри которого зародилась в том числе необходимость засекречивать определенные категории документов и в качестве контрмеры возникло то, что здесь называется военной дешифровкой.

намеренно облаченные в хитроумные, специально изобретенные системы необычных для языка знаков (чаще всего цифровых), которые должны воспрепятствовать – и в этом их единственная задача! – прочтению зашифрованного текста.

Преследуя абсолютно различные и несопоставимые цели, оба эти процесса умственной деятельности человек с точки зрения техники их осуществления необычайно близки и схожи, поскольку в обоих случаях решается одна и та же задача: отождествление неизвестных знаков текста со словами языка для последующего прочтения текста. Только поиск параллелей и аналогий, которые могут помочь изучению письма древних цивилизаций, вынуждает нас касаться вопросов, связанных с военной дешифровкой.

Чтобы прочесть зашифрованную депешу, необходимо овладеть шифром, с помощью которого она составлена. История двух мировых войн знает примеры, когда слепой случай нежданно дарил то, чего не могли добыть лучшие разведчики мира, расплачивавшиеся своей жизнью за попытку достать секретны[1] шифр.

Ну, а как быть с древними письменами? Существовали ли шифры, с помощью которых их можно прочитать? Представьте себе, такие «шифры» действительно существовали, и они даже дошли до нас. Это двуязычные записи одного и того же текста – так называемые билингвы. Они родились в процессе общения между разноязыкими государствами или народами как результат возникшей необходимости закрепить в памяти или зафиксировать некое событие (явление), знать или помнить которое должны были люди, говорившие на разных языках.

---

[1] В мае 1940 г. затонул японский корабль, который, согласно официальной версии, якобы вел промысел моржей вблизи Берингова пролива. Вскоре норвежский китобой подобрал труп его капитана (он держался на плаву благодаря спасательному кругу). В кармане «охотника» оказался сверхсекретный шифр японского флота. Норвежцы передали шифр первому американскому военному кораблю, повстречавшемуся им в океане.

Долгие годы и даже столетия – изучением неизвестных письмен ученые занимаются более 2 веков – практически единственным методом дешифровки было сопоставление текстов, написанных на неизвестных письменах, с текстами на известных письменах, оказавшимися на одном и том же камне, плите или доске, т.е. благодаря билингве. Достаточно сказать, что именно так родилось выдающееся открытие Шампольона, благодаря которому была раскрыта тайна египетских иероглифов.

Сказать, что Шампольону повезло, было бы величайшей несправедливостью, ибо этот замечательный французский ученый отдал свою жизнь, всего себя изучению Древнего Египта. Его открытие – результат титанического труда, а не случайная улыбка судьбы. И все же Шампольону повезло, заслуженно, но повезло, коль скоро в его руках оказался камень с двуязычной записью – знаменитая «Розетская билингва».

Ну, а как быть, если билингвы-шифра нет? Да и надежен ли вообще метод сопоставления? Где гарантия того, что разноязычные тексты, высеченные, скажем, на одном камне или нарисованные кистью на одном листе папируса, идентичны? Ведь один и тот же смысловой сюжет можно изложить совершенно непохожими фразами и разными словами даже на одном и том же языке.

В подтверждение давайте придумаем сами какую-либо «надгробную надпись» (как правило, именно такие надписи лучше всего сохраняются и чаще доходят до наших дней). Например, такую:

«Здесь покоится тело царя Ивана» – будет гласить она. Но этот же сюжет, или ситуацию, можно записать на надгробном памятнике, скажем, и так:

«Прах усопшего правителя Ивана приняла эта земля».

Обе фразы даны на одном и том же языке, они передают одинаковое смысловое содержание, однако в первой из них пять слов, а во второй семь, и только одно – имя собственное «Иван» – повторяется. Отсюда легко сделать вывод, что знание остальных слов любой из «надписей» (если бы мы их умышленно зашифровали, скажем, китайскими иероглифами) мо-

жет нам помочь понять содержание другой, но для установления точного текста этой другой «надписи», т.е. для нахождения словесных эквивалентов изображенных в ней знаков, фактически ничего не дает.

А какие «подводные камни» могут еще поджидать дешифровщика в двуязычной надписи, если системы письма принципиально отличны друг от друга?

Следовательно, билингва, поиски которой сами по себе составляют великую трудность, а иногда заведомо бесперспективны (например, на острове Пасхи или среди памятников письменности древней Америки), как и полученные любым другим путем сведения о содержании надписи, текста или целой рукописи, должны быть отнесены лишь к категории косвенных данных.

Они могут помочь в дешифровке неизвестных письмен. Но обладание билингвой отнюдь не означает, что исследователь получил все необходимые для дешифровки данные, т.е. шифр. До недавнего времени работа по дешифровке исторических систем письма как в СССР, так и за рубежом, велась на основе именно таких косвенных данных. Но этот метод не давал возможности и даже в некотором смысле препятствовал изучению древних текстов, о которых подобные данные отсутствовали.

Казалось, что перед учеными-дешифровщиками встали непреодолимые трудности.

Как же быть? Что делать исследователям, если нет двуязычных надписей? Вообще отказаться от идеи дешифровки древних письмен, техника написания которых была утрачена вместе с исчезновением породивших их цивилизаций?..

Нет, с этим нельзя было согласиться. Ведь достаточно вспомнить, что именно дешифровка древних письмен открыла для человечества малоизвестные и вовсе неизвестные цивилизации, например шумерскую! Отказываться от дешифровки нельзя. Но что тогда делать?..

Поиск начинается. Рукопись лежит на столе. И вы опять, уже в который раз, начинаете перелистывать ее стра-

ницы. Снова и снова возникает вопрос: что делать? Как и с чего начать? Каков тот первый вопрос, который следует поставить перед собой дешифровщику?

И вдруг приходит ответ. Он неожиданно прост:

нужно определить систему письма. Прежде всего разобраться и решить, какова зависимость между знаками, таинственно смотрящими со страниц рукописи, в чем сущность этой зависимости и чем могут быть сами знаки?

Например, вот этот похожий на скелет  или этот  – он как будто бы напоминает лицо?  – здесь словно кто-то веревку свернул, а там  чешуя рыбы или кусок циновки? А вот снова, правда, несколько иначе «свернутая веревка» **^–»^^_^^–» ^^_^** – это что-то непонятное: какая-то ракушка или другая морская живность?

Знаки не всегда стоят в одиночку; они то сбиваются в кучу, то вытягиваются цепочкой, то налезают друг на друга в виде «башенки» в два-три этажа.

Давайте последим за одним каким-нибудь значком, например вот этим  . Договоримся условно называть его «скелетом», поскольку он несколько напоминает именно скелет, а точнее, позвоночник с ребрами Знак относительно прост, легко запоминается, и это поможет нам выделять его среди других. Теперь перелистаем Дрезденскую рукопись.

«Скелет» впервые появляется на странице 7; справа к нему «приклеилось» уже знакомое нам «морское чудовище», которое мы будем условно называть «рыбой»  . Листаем дальше рукопись. В этом же сочетании («скелет» 4 – «рыба») оба знака изображены также на страницах 13, 17, 21 и 68, что свидетельст-

вует о несомненной устойчивости такого сочетания На странице 17 есть и другая комбинация знаков к «скелету» присоединен новый знак –  но он уже стоит не сзади, а впереди; эти знаки ц •^(•2-уУ также повторяются, правда, только на двух еще страницах (59 и 73) На страницах 24, 26, 32 и 37 «скелету» явно не повезло: его «оседлали» целых два знака –  . В разных комбинациях-сочетаниях знак  изображен также на последующих страницах.

Что скрывается за всем этим? Что вообще могут обозначать знаки? Обозначают ли они звук, или слог, или корень слова? Может быть, целое слово? А вдруг одни знаки – это буквы, другие – слова, а третьи – корни?

Известно, что система письма может быть не только определенной, т.е. состоящей из однородных единиц, но и смешанной. Знаки могут даже не соответствовать единицам языка, а быть условными символами понятий, и тогда прощай дешифровка! Ведь символы можно лишь интерпретировать, а не дешифровать, и перед нами не письмо, а так называемая пиктография.

Но как определить систему письма? Что может стать той единицей (и единицей чего?), которая позволила бы сопоставить и отличить одну систему от другой? Изображение знака? Нет, это не подходит, ведь даже знаки-буквы одного алфавита бывают не похожи на знаки-буквы другого, родственного, хотя они передают одну и ту же гласную или согласную. Тут и за примерами далеко ходить не надо: русское «У» на испанском выглядит как русское «И», а русское «И» можно написать почти как «У». Еще меньше сходства у согласных: «Ч» – «СН»; «П» – «Р»; «Р» – «R». А с иероглифами дело обстоит куда сложнее, ибо они обязаны учитывать особенности своего языка.

Как же быть? Где и какова та единица, которая... Позвольте, «единица», да, «единица», но как цифра, как число – вот он ответ!

Сейчас определение системы письма кажется неопровержимо логичным началом дешифровки любого неизвестного текста, но для того, чтобы прийти к столь несложному выводу, требовались многие месяцы и даже годы упорного труда, изучения сотен научных работ, освоения основных типов записи языка, известных человечеству, и овладение этими языками.

Ибо знаки повторяются («скелет» повторился 16 раз только в одной рукописи!), и в этом повторении должна быть определенная закономерность, ну хотя бы частота повторяемости. А сколько вообще-то этих самых знаков? Сколько их? Это необходимо выяснить, установить с абсолютной точностью, и только тогда появится возможность «облачить» в числа языковые знаки и определить закономерности языка.

Так родилась блестящая идея, значение которой не сразу можно было оценить!..

Сотни, тысячу раз перелистывает Юрий Кнорозов страницы рукописей майя. Их тщательный анализ, бесконечные проверки и перепроверки показали, что в письме встречается около 300 знаков.

Начались новые размышления, теперь уже с применением выявленных «числовых показателей».

Если бы тексты были «рисуночным письмом», т.е. пиктографией, где знаки передают не звуковую речь, а лишь общие понятия и ситуации, которые могут быть выражены разными, но сходными по смыслу фразами на любом языке (вспомните наши «надгробные надписи»), то, естественно, количество знаков должно было бы быть неизмеримо больше, ибо каждая новая ситуация требовала бы нового знака. В «рисуночном письме» из каждых 100 знаков, как показывает подсчет, 75 – новые, не встречавшиеся ранее. К тому же прирост знаков постоянен: он не зависит от того, возьмем ли мы первую или десятую сотню знаков; рассмотрим ли мы текст с начала, с середины или вообще с конца.

Иными словами, имеющиеся в нашем распоряжении 300 знаков в «рисуночном письме» дали бы текст общей протяженностью примерно в 400 знаков, а чтобы заполнить пиктограммами три исследуемые рукописи майя, понадобилось бы несколько тысяч, а может, и десятков тысяч знаков. Рукописи же майя дают совсем иную картину: знаков только 300!

Тогда предположим, что знаки майя передают только звуки. Кстати, такое предположение было распространено среди некоторых исследователей, да и сам Ланда дает своему списку знаков название «алфавита». Однако и это предположение отвергает математический анализ; число звуков в любом языке мира не превышает 80, а в среднем оно равно 30–40, т.е. в 5–10 раз меньше, чем было бы в текстах майя, если бы каждый из 300 знаков передавал звук.

Слишком много знаков в рукописях майя и для письма, в котором каждый знак передает отдельный слог. Обычно слоговые системы письма обходятся 40–50 знаками, как, например, японские системы «катакана» и «хирагана», индийская «деванагари» или древнее кипрское письмо; как правило, количество слогов не превышает 100–150. Трудно, да и нет оснований поверить, что майя могли позволить себе подобное «слоговое излишество».

Тогда, может быть, майя пользовались морфемным письмом, в котором каждый знак соответствует корню слова или грамматической частице? Но такое письмо согласно подсчетам не может обойтись без 1000 – 1500 морфем, а у майя только 300 знаков. Значит, и морфемное письмо отпадает.

Сделаем еще одно предположение, правда заранее считая его невероятным: может быть, знаки рукописи майя передают целые слова, сочетания слов или даже фразы? Но тогда жрецам понадобилось бы не 300 знаков, а по крайней мере 3 тысячи или, вернее, три десятка тысяч различных знаков только для трех известных рукописей.

Итак, ни пиктограммы, ни звуки, ни слоги, ни морфемы, ни слова... Но тогда что же, что передают знаки майя?

И Юрий Кнорозов делает единственно правильный вывод, который вытекает из разработанной им самим системы. Ответ

может быть только один: система письма индейцев майя – смешанная. Часть знаков должна передавать морфемы, а часть – звуки и слоги. Такую систему письма принято называть иероглифической. Ею пользовались древние египтяне и жители Месопотамии, ею пользуются и поныне на Дальнем Востоке.

Иероглифическое письмо, как и всякое письмо, имеет свои количественные показатели, и они полностью совпадают с показателями письма майя. То, что в 1881 г. Леон де Рони только предположил, а именно, что майя пользовались иероглификой, сходной с иероглификой Старого Света, Юрий Валентинович Кнорозов научно доказал. То, что раньше было лишь аналогией, теперь стало неоспоримым фактом, доказанным точными числами.

Так были сделаны первые шаги по новому пути дешифровки. Он открывал интересные многообещающие перспективы...

Язык и дешифровка. *Поскольку Пернатый змей, ныне К'ук'улькан, покинул свою новую резиденцию Тулапан-Чиконаухтлан и устремился в великий поход, чтобы снова прославить свое священное имя, и нам неизвестно, где и каким станет его новое «гнездо», мы воспользуемся этим обстоятельством, чтобы продолжить разговор о дешифровке неизвестных письмен.*

Он был прерван на том самом месте, когда выяснилось, что молодому советскому ученому Юрию Кнорозову благодаря разработанной им оригинальной системе числовых показателей и ее успешному применению при анализе трех сохранившихся рукописей майя удалось доказать, что письменность древних майя была иероглифической. Это важное открытие имело решающее значение для дальнейшей работы по дешифровке. Был указан определенный и единственно правильный путь, по которому должны идти исследователи в сложном и невероятно тяжелом научном поиске.

Но прежде чем удалось приступить ко второму этапу дешифровки, на повестку дня неожиданно встал вопрос, который на первый взгляд может показаться не то чтобы странным, а пожалуй, даже несколько наивным: а известно ли, на каком, собственно, языке написаны интересующие нас рукописи?

– Ну вот, – скажет читатель. – Говорили, говорили о рукописях майя, а выходит, что еще даже неизвестно, на каком языке они написаны?!.

Как это ни парадоксально звучит, но при дешифровке неизвестных письмен вопрос о языке, на котором они написаны, в одинаковой степени может быть и решающим и ничего не решающим.

Сразу же оговоримся, что знание языка рукописи – идеальное благоприятное условие для ее дешифровки. Если же письмо является буквенно-звуковым, т.е. каждому звуку (или сочетанию звуков) соответствует определенный знак (или их сочетание) и знаки сами по себе не несут смысловую нагрузку, а лишь передают звуковую речь, дешифровка такого письма без знания языка вообще исключается (по крайней мере на сегодняшнем уровне научных и технических возможностей). Однако можно привести совершенно противоположный пример (правда, не с буквенно-звуковой письменностью): шумерские тексты были дешифрованы и полностью переведены, хотя вот уже несколько тысячелетий язык шумеров не звучит на нашей планете. На нем никто не говорит, и в этом смысле его никто не знает. Если бы сейчас удалось каким-то чудом воскресить шумера, с ним можно было бы без особого труда сразу же объясниться письменно, однако, если воскресший оказался бы, к несчастью, неграмотным, его пришлось бы в срочном порядке обучить либо шумерской грамоте, либо одному из современных языков (трудно сказать, чему следовало бы отдать предпочтение).

Поскольку развитое иероглифическое письмо – а письмо рукописей майя было именно таким – передает в том числе и звуковую речь (об этом будет рассказано подробнее далее), знание языка рукописей приобретало решающее значение.

Все исследователи рукописей исходили из того, что они написаны на языке майя, однако на втором этапе дешифровки вопрос стоял уже не о предположениях на этот счет, а о достоверных фактах, которые подтвердили бы их или опровергли. Ибо для науки, даже для решения самой частной на-

учной проблемы, какой бы незначительной она ни казалась, одних предположений недостаточно. Правда, без предположений, без умозрительного поиска не было бы и самой науки.

Однако вернемся к нашему, как оказалось, не такому уж наивному вопросу: на каком языке написаны интересующие нас рукописи? Есть ли в распоряжении исследователей достаточно достоверные данные, позволяющие утверждать, что неизвестные тексты – это тексты на языке майя?

Естественнее всего предположить, что исследуемые тексты написаны на языке тех, кто пользовался ими, т.е. на майя. Это выглядит наиболее логично и убедительно просто. То, что рукописи попали в Европу из Юкатана, территории, на которой в течение многих вв. проживали майя, не вызывает сомнений, но ни о чем еще не говорит.

От испанцев было известно, что рукописи составлялись местным жречеством и являлись сферой его деятельности, но и это не может служить абсолютным доказательством того, что жрецы майя делали свои записи на языке майя. Не только теория, но и практика по сей день дает немало примеров, когда культовая служба велась и ведется не на местном языке, не говоря уже о диалектах, а на каком-то особом, иногда даже мертвом языке.

Возьмите, например, католическую религию. В Чили, Вьетнаме, Италии, Китае, Польше, Франции, СССР, как и в любой другой стране, в которой имеется хотя бы одна-единственная католическая церковь, служба в ней ведется только на латыни. Но на латыни сегодня не говорит ни один народ мира; латынь уже много столетий причислена к мертвым языкам. И если для чилийцев, говорящих по-испански, итальянцев или французов, также принадлежащих к романоязычным народам, латынь – относительно близкая «родственница» и даже прародительница их родных языков, этого никак нельзя сказать ни о языке поляков, ни китайцев, ни вьетнамцев, ни народов Советского Союза, как и любой другой не романоязычной страны.

Может быть, и древние майя, вернее их жрецы, подобно католическим священникам, также у кого-то заимствовали свой

культовый язык и письменность, с помощью которой он закреплялся? Но тогда у кого? У кого они могли их заимствовать?

Цивилизация майя была, несомненно, самой высокой и, пожалуй, самой древней на Американском континенте. Мы говорим «пожалуй» только потому, что, как уже указывалось, пока нет абсолютно достоверных доказательств, подтверждающих прямое родство цивилизации майя с ольмекской культурой – самой древней культурой Америки. И все же есть немало весьма убедительных доводов, настойчиво требующих признания древних майя прямыми наследниками ольмеков, и среди этих доводов важное место занимает бесспорное сходство письменных и цифровых знаков, сохранившихся на ольмекских памятниках, со знаками письменности майя. Из этого следует только один вывод: если ольмеки и майя – ступени одной языковой «лестницы», древним майя, «потомкам» ольмеков, попросту не у кого было ни заимствовать письменность, ни тем более писать свои рукописи на чужом языке: они могли писать только на своем языке, на языке майя.

В пользу такого утверждения, наконец, есть и прямые свидетельства самих испанцев. Вот что написал, например, Ланда в своем «Сообщении о делах в Юкатане»:

«Эти люди (т.е. индейцы майя) употребляли также определенные знаки или буквы, которыми они записывали в своих книгах свои древние дела и свои науки. По ним, по фигурам и некоторым знакам в фигурах они узнавали свои дела, сообщали их и обучали. Мы нашли у них большое количество книг (написанных этими буквами), и, так как в них не было ничего, в чем не имелось бы суеверия и лжи демона, мы их все сожгли; это их удивительно огорчило и причинило им страдание...»

Ланда в «Сообщении о делах в Юкатане» приводит также пример написания упомянутыми знаками нескольких слов. Это слова из языка майя, того языка, на котором они говорили. Следовательно, их письменность была приспособлена передавать их устную речь, т.е. обслуживала ее.

Только теперь, пожалуй, мы имеем достаточно оснований утверждать, что исследуемые рукописи действительно были написаны на языке майя.

Однако на этом, к сожалению, вопрос о языке не исчерпывается. Язык не относится к постоянным категориям. Он невероятно чувствителен к малейшим социально-экономическим явлениям в жизни своего народа и непрерывно изменяется под их воздействием. Но язык не мембрана; он не только улавливает и передает эти изменения, но и закрепляет их в коллективной памяти говорящего на нем народа. Постепенно одни слова отмирают; другие прочно входят в речевой обиход; третьи, полностью сохраняя звуковую и графическую внешность, решительно меняют свое первоначальное значение, передавая совсем иной, порой и противоположный смысл.

Язык живет жизнью народа; вместе с ним он радуется и страдает, строит и разрушает, но если жизнь народа немыслима без языка, сам язык – история знает такие случаи – способен иногда пережить своего создателя и через многие тысячелетия поведать о нем людям, как это произошло, например, с шумерской цивилизацией.

На языке майя сегодня говорят несколько сот тысяч человек, живущих на Юкатане, а на родственных, весьма близких к нему диалектах из общей языковой семьи майя-кичэ – почти 2 млн.

Язык сегодняшних майя значительно отличается от языка XVI в., когда к берегам Юкатана впервые подошли корабли испанских конкистадоров. Первые из них под предводительством Франсиско Эрнандеса Кордоба пытались высадиться на Юкатан ровно 450 лет назад – в 1517 г., однако испанцам было оказано столь решительное сопротивление, что только через 1/4 в. (1541–1546 гг.) им с большим трудом все же удалось завоевать земли, принадлежавшие древнему американскому народу.

По записям испанских миссионеров можно составить довольно точное представление о языке майя того периода. Это позволило установить весьма существенную разницу между языком майя XVI и XX вв. Тем более невероятно предположить, что язык текстов рукописей идентичен языку майя XVI в. (не говоря уже о современном).

Почему? На это есть много причин.

Прежде всего удалось установить, что рукописи были написаны задолго до прихода испанцев. Об этом говорят календарные даты и форма их написания; характер изображения отдельных богов, совпадающий с изображениями этих же богов на стелах, датировка которых известна; упоминание отдельных названий городов (например, в Парижской рукописи часто упоминается город Майяпан, что достаточно убедительно привязывает рукопись к периоду гегемонии этого города); и наконец, состояние рукописей (сохранность «бумаги», красок и др.) помогает определить их возраст.

Основываясь на этих данных, Ю. В. Кнорозов приходит к заключению, что Дрезденская рукопись была написана до XIII в. (XI–XII); Мадридская – до XV (XIV); Парижская – в XIV–XV вв. (период гегемонии города Майяпана).

В истории майя XI–XV вв. были периодом гигантских потрясений, когда на Юкатан одна за другой обрушивались волны событий, резко отражавшихся не только на привычном укладе жизни населявших его народов, но и приводивших к исчезновению целых городов-государств и появлению новых столиц-гегемонов. Это был период ожесточенной междоусобной борьбы и раздробленности, в которую постоянно вклинивались нашествия инородных племен и варваров-кочевников. Язык майя не мог не претерпеть значительных изменений за эти бурные в. их истории.

Совершенно очевидно также, что жрецы пользовались для написания своих текстов не современным им разговорным языком XI–XV вв., когда составлялись рукописи, а каким-то особым, «подсказанным» жрецам самим письмом. В чем тут дело? Не впадаем ли мы в противоречие с тем, что говорилось ранее, в частности о латыни? Попробуем разобраться и в этом вопросе. Необходимо пояснить, что по сравнению с устным языком письмо всегда является куда более консервативной формой его бытия. Причем консерватизм, сам по себе характерный для письма, к тому же, как правило, искусственно культивируется теми, кому оно доступно. Не забывайте, что

речь идет о рабовладельческом обществе, да еще на самом начальном этапе. Следовательно, письменность была достоянием лишь жречества и знати, т.е. господствующих классов. Они не только стремились удалить письмо от простого народа, но и придавали ему характер чего-то недоступного, сверхъестественного, мистического, превращая письмо в еще одно орудие своего господства.

Из сказанного можно сделать вывод, что если рукописи майя и были написаны сравнительно недавно, примерно в XI–XV вв., зато их писали языком, весьма близким или идентичным с древним письменным языком, сложившимся, как полагает Ю. В. Кнорозов, по-видимому, на рубеже нашей эры, а может, и раньше. Отсюда легко понять, что разница между языком текстов рукописей и современным языком майя – по времени их разделяют 2 тысячелетия! – должна быть достаточно велика. Она, например, может достигнуть такой же степени, как между латынью и, скажем, испанским или французским или между языком Киевской Руси и тем, на котором мы с вами говорим. Язык рукописей мог быть мертвым языком; это была местная «латынь», дальняя, но прямая «родственница» языка народа майя, а скорее всего родоначальница всей языковой семьи майя-кичэ.

Следовательно, современному дешифровщику необходимо проследить эволюцию языка (как бы сделать «срез» во времени), его грамматики и лексики, на протяжении 20-ти столетий! И если верхние слои – язык майя XX в., на котором сегодня говорит этот народ, – лежат прямо на поверхности, нижний слой – язык трех известных нам рукописей – так глубоко зарыт в толщу прошедших вв., что добраться до него кажется делом невероятным. В довершение всего возникает заколдованный круг: чтобы дешифровать рукописи майя, необходимо знать особенности языка, на котором они написаны, а единственным достоверным источником познания этих особенностей и, следовательно, древнего языка вообще являются три упорно молчащие рукописи.

Поиск продолжается. И снова, уже в который раз, Юрий Кнорозов просматривает страницу за страницей ману-

скрипты Ланды и других свидетелей и составителей хроник времен испанской конкисты Мексики и Юкатана. Нужно найти хоть какую-нибудь зацепку, пусть небольшой, но подлинный языковой «срез» из более ранних слоев языка майя, предшествовавших испанскому завоеванию.

«...У них есть басни или предания очень предосудительные, – писал в XVII в. испанец Санчес де Агиляр. – Некоторые они записывали, сохраняют их, читают на своих собраниях. Такую тетрадь я отобрал у учителя при часовне селения Сукон по имени Куйтун...»

...«Басни»?.. «Предания»?.. Ну, конечно, это первое упоминание о так называемых «книгах Чилам Балам», как сейчас именуются рукописные тексты, записанные индейцами майя еще в XVI в. О них, например, говорит в своей «Истории Юкатана» Диего Лопес де Когольюдо, автор XVII в. Индейцы писали их на своем родном языке – на майя, но не иероглифами, а латинскими буквами (латиницей). «Книги Чилам Балам» – общепринятое название этих старых текстов, но оно довольно условно. Его возникновение связано с знаменитым чиланом (прорицателем – на языке майя) по имени Балам, который жил в городе Мани во времена испанского завоевания Юкатана, хотя сами «книги Чилам Балам» составлялись, несомненно, позже.

Много «книг Чилам Балам» собрал и исследовал в XIX в. Пио Перес. Он скопировал и опубликовал некоторые из них (1837 г.), и они так и вошли в мировую литературу как «Рукописи Переса». «Книги Чилам Балам» были обнаружены и в более поздние времена. Одна из последних находок датируется 1942 годом, когда в столице Юкатана городе Мериде случайно нашли рукописный текст «Песен из Дзитбальче».

Именно они, «книги Чилам Балам», оказали неоценимую услугу в сложнейшей «археологической» работе по выявлению особенностей языка древних текстов, да и по дешифровке иероглифических рукописей майя.

Когда иероглифическое письмо было запрещено испанскими монахами, а древние книги сожжены, индейцы майя

стали записывать латиницей в «книгах Чилам Балам» свои пророчества, мифы, хроники, восходящие к древнему периоду их истории. Правда, все это оказалось в хаотической смеси с более современными текстами, относящимися к XVI в., и даже с переводами... из испанских книг.

Юрий Кнорозов тщательно, самым детальным образом изучает «книги Чилам Балам». Он отсеивает нужное от бесполезного, исследует каждую фразу, каждое слово. Наконец, впервые делает перевод на русский язык основных текстов из «книг Чилам Балам», восходящих к доиспанским временам. Тяжелый труд вознаграждается с лихвой, тексты содержат именно то, в чем так нуждался ученый: древние слова языка майя, жреческую терминологию (к тому же «озвученную» с помощью латиницы) – неоценимый материал попадает в руки дешифровщика!

Теперь уже сами тексты заново подвергаются полному и всестороннему анализу. Они сопоставляются с современным языком майя и с языком XVI в., и постепенно появляется тот самый многослойный «срез» (подобный археологическому), который разрешает еще одну труднейшую задачу дешифровки.

Юрий Кнорозов изучает грамматику майя; ему удается «препарировать» грамматическую структуру языка, несмотря на ее исключительную сложность, на непривычные для европейца языковые формы и категории. Достаточно привести такой пример: глаголы майя должны иметь показатели субъекта действия и объекта действия одновременно! Объяснить подобные требования языка майя примером на русском языке совершенно невозможно.

Необычайно сложна и лексика: слова как бы располагаются по различным временным слоям (подобно слоям в археологии), начиная с заимствований из испанского и даже английского языков – «верхние слои», кончая слоями, уходящими в глубь веков, к эпохе, предшествовавшей рождению первых городов-государств майя на рубеже нашей эры.

Эти исследования наглядно показали, сколь наивными были попытки читать иероглифические тексты рукописей на языке майя XVI или даже XIX в.

Диссертация, которую так и не пришлось защищать. Худощавый человек невысокого роста с огромным пухлым портфелем пронзительно оранжевого цвета как-то незаметно, боком вошел в просторную аудиторию. Словно опасаясь сквозняка, он старательно прикрыл за собою дверь, проверил, плотно ли она встала на место, и остался стоять у стены. Свой портфель он держал обеими руками за ручку, угрюмо посматривая по сторонам из-под выпуклого, почти квадратного лба глубоко посаженными светлыми глазами. Тому, кто не знал его, было трудно догадаться, кто он и зачем пришел в эту аудиторию Института этнографии Академии наук, где должна состояться защита диссертации. Для маститого ученого он казался слишком молод; для соискателя ученой степени, пожалуй, излишне спокоен. Его нельзя было причислить и к весьма распространенной в наши дни категории людей, одинаково охотно посещающих суды, особенно бракоразводные процессы, крупные и мелкие выставки – предпочтение отдается международным – и, наконец, защиту диссертаций, о которых предусмотрительно оповещает пресса: при всей своей внешней обыденности он, без сомнения, был человеком незаурядным.

– Здравствуйте, – сказал он негромко и, словно извиняясь перед собравшимися, представился: – Кнорозов.

Многие из тех, кто находился в зале, впервые увидели молодого исследователя древних письмен, приехавшего из Ленинграда в Москву для защиты диссертации на соискание ученой степени кандидата исторических наук. Но зато все они, видные советские ученые, хорошо знали не очень многочисленные, однако чрезвычайно интересные труды сотрудника Ленинградского отделения Института этнографии.

Уже первая работа Юрия Кнорозова – сравнительно небольшая статья под скромным названием «Древняя письменность Центральной Америки», опубликованная в 1952 г. в журнале «Советская этнография» (№3), вызвала несомненный интерес в международных кругах ученых-американистов и других специалистов по древним цивилизациям. Дотоле никому не известный молодой ученый из «далекой Советской

России» убедительно доказывал в своей статье, что письменность древних майя – одна из самых волнующих загадок Нового Света – была иероглифической и, следовательно, передавала звуковую речь. Он утверждал, что рукописи и надписи майя можно прочесть и перевести на любой другой язык, в том числе и русский. В подтверждение своих выводов Юрий Кнорозов приводил примеры чтения некоторых иероглифов майя и доказывал перекрестным чтением различных слов (наличие алфавитных знаков) в древних текстах майя.

В частности, «куц» («индюк»)  и «цул» («собака»).

Юрий Кнорозов заявлял, что точно так же могут быть прочтены все иероглифы, но для этого необходимы глубокие исследования письменности древних майя и их языка.

Подобные заявления были расценены как открытый «бунт» против крупнейшего специалиста по древним майя, американского профессора Эрика Томпсона, за которым ходила недобрая слава «великого могильщика» исследователей письма майя. Но русский парень не постеснялся непререкаемого среди современных майистов авторитета Эрика Томпсона. Более того, первая работа Кнорозова, казалось, попросту «бросала перчатку» американскому профессору и многочисленным сторонникам его школы, призывая ученых всего мира не сидеть сложа руки в бесплодном созерцании замысловатых знаков, оставленных жрецами майя, а начать новое всеобщее наступление на их сокровенную тайну. Юрий Кнорозов не скрывал и «оружия», которым намеревался преодолеть вековое молчание древних рукописей, – оригинальную систему дешифровки, основанную на разработанном им принципе «позиционной статистики».

Реакция со стороны Томпсона и его сторонников не заставила себя долго ждать: пытаясь перехватить инициативу, они обрушили на молодого ученого шквал яростных атак. В мексиканском журнале «Ян» появилась статья самого Томпсона, в которой он, в крайне резкой форме «прорецензиро-

вав» работы Юрия Кнорозова, категорически и уже в который раз отрицал наличие в письме майя фонетических знаков и достоверность «алфавита Ланды» Он поспешил заявить, что может опровергнуть любое чтение Ю. В. Кнорозовым иероглифических знаков майя, однако «благородный гнев» профессора, по-видимому, оказался настолько велик, что он до сего дня (!) мешает ему выступить с опровержением чтения хотя бы тех двух приведенных нами слов:

индюк

и собака

Может быть, именно поэтому Эрик Томпсон в своей «научной» полемике вскоре решительно взялся за «аргументацию» совсем иного рода. Он заявил, что поскольку он, Томпсон, располагает абсолютно достоверными сведениями, что в России никогда не было никаких дешифровок, их посему там и быть не может (!). Столь блистательный «аргумент», однако, не вызвал аплодисментов даже в рядах его сторонников, а видный мексиканский ученый Мигель Коваррубиас счел необходимым прокомментировать такой внезапный поворот американского профессора в дискуссии о письменности майя справедливым замечанием, что, «к сожалению, политика вмешалась в вопрос об эпиграфике майя».

Действительно, можно лишь сожалеть о позиции, занятой Эриком Томпсоном в отношении работ Юрия Кнорозова. Дело не в том, что Юрий Кнорозов наш соотечественник и мы гордимся выдающимися достижениями ученого, воспитанного нашей страной. Просто Эрик Томпсон заведомо и крайне отрицательно относится к любой попытке найти ключ для дешифровки письменности майя. Если бы американский профессор был шарлатаном от науки – к сожалению, такие еще встречаются и в наши дни, – можно бы просто не обра-

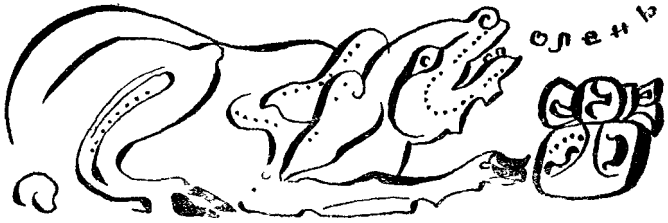
щать внимания на его грубые выпады. Но Эрик Томпсон действительно собрал, исследовал и опубликовал богатейшие материалы по цивилизации майя и знакомство с его научными трудами представляется практически обязательным для современного исследователя американских культур. Это создало Томпсону огромный, а по некоторым вопросам, что называется, непререкаемый авторитет. Однако не сумев однажды постичь тайну древнего письма народа майя, вернее – глубоко и, по всей вероятности, искренне убежденный в том, что только он один постиг ее, и постиг правильно, Эрик Томпсон не находит силы пересмотреть отношение к этому вопросу, предпочитая брать на себя незавидную роль «могильщика» любой «нетомпсоновской» школы по дешифровке письменности майя.

Гнев Эрика Томпсона против работ Юрия Кнорозова был особенно силен еще и потому, что «парень из далекой России» убедительно просто показал, в чем именно заключается основная ошибка возглавляемой американским профессором школы так называемого «ребусного письма». Томпсон и его школа понимали под дешифровкой независимые друг от друга толкования отдельных знаков, по существу сводя изучение древних письмен к бесконечным толкованиям и перетолкованиям произвольно взятых из контекста иероглифов. Такой путь исследования неизбежно заводил в тупик, поскольку был оторван как от задач языкознания, так и от изучения внутренней структуры текста. В итоге малодоказательные толкования и перетолкования порождали не менее малодоказательные опровержения, которые, в свою очередь, порождали столь же малодоказательные опровержения опровержении и так далее и тому подобное...

Иными словами, в подобном «исследовании» попросту смешаны два различных понятия: «дешифровка» и «интерпретация» Первое из них, как уже указывалось, означает отождествление знаков (здесь – знаков майя) со словами языка (майя); во втором случае имеет место толкование значения отдельных знаков, не дающее, однако, точного словесного эквивалента исследуемого языка, а лишь «объясняющее» смысловое значение знака.

Постараемся пояснить это на конкретных примерах. Перелистывая рукописи майя, мы в свое время обратили внимание на знак  ,причем высказали предположение, что он одновременно похож как на кусок плетеной циновки, так и на чешую рыбы.

Если знак  произвольно извлечен нами из текста некоей рукописи или надписи на камне, можно до бесконечности спорить, «циновка» это или «чешуя», приведя соответствующие «доказательства» и «контрдоказательства», одинаково легко опровергающие друг друга. Это типичный случай толкования знака, т.е. попытки установить по его рисунку (и только рисунку!) смысловое содержание, которое хотела вложить в него рука, нарисовавшая знак, скажем, на листе папируса или на лубе фикуса.



В пиктографии, или «рисуночном письме», знаки-иконы не имеют языкового эквивалента, в силу чего такой прием их исследования вполне закономерен. Причем рисовальщик подобного «текста», вновь изображая по ходу своего «повествования», например, ту же «циновку», может в третий, десятый или двадцатый раз нарисовать «циновку» совсем не так, как в первый, ибо ему важно только одно: знак-рисунок должен изображать именно то, что он рисует; ему безразлично, похожи ли друг на друга знаки, изображающие один и тот же предмет, лишь бы «читатель» знаков и в том и в любом другом случае угадал в них «циновку»! Совершенно иначе обстоит дело в иероглифическом письме: знак «циновка» всегда пишется (рисуется) одинаково, потому что это не смысловой, а

языковый эквивалент. И хотя некоторые или даже многие иероглифические знаки (это зависит от степени развитости письма) еще продолжают сохранять смысловую нагрузку и мы даже можем угадать в них изображение того или иного «предмета», они уже передают не понятие «подстилка для лежания», а само слово «циновка», воспроизводя его звучание!

Знак обрел звук и стал фонетическим. В этом качестве он используется и для написания слова, в котором имеется передаваемый им звук (как буквы в алфавите).

Именно таким и является знак  ; он фонетический и передает звук «ш(а)», а изображает циновку или крышу из листьев пальмы, на языке майя – «шаан».

Возьмем еще один хорошо знакомый нам знак  . Это также фонетический знак «ц(у)», изображающий позвоночник и ребра скелета, на майя – «цуул бак». Вот несколько слов, написанных иероглифами майя

– «цу-лу» – собака, домашняя собака

– «цу-лу (каан)» – небесная собака

– «ку-цу» – дикий индюк,

– «цу-ан» – позднее название восьмого месяца календаря майя (древнее название этого же месяца к′анк′ин),

– «ах-цу-бен-цил» – упорядочивающий.

Конечно, и индюк, и собака, и даже небесная собака, как и упорядочивающий что-либо человек, несомненно, должны иметь каждый свой скелет, но не этим объясняется появление знака  в написании перечисленных слов. В каждом из этих слов он передает не смысловое содержание рисунка, а только звук «цу» и, следовательно, служит конкретным алфавитным знаком.

Эрик Томпсон также предложил свои чтения знаков майя. В связи с этим Ю. В. Кнорозову пришлось высказаться по его «дешифровке». Советский исследователь показал, что из тридцати «дешифрованных» Томпсоном, по его утверждению, знаков, в действительности только восемь (!) были прочтены, а остальные двадцать два – истолкованы. Однако из этих восьми знаков самому Томпсону принадлежит чтение только трех. Чтение же пяти других знаков американский профессор заимствовал у исследователей, в том числе у Ланды, де Рони, Томаса, которых подверг «уничтожающей» критике и сурово осудил.

В 1955 г. научный «багаж» Юрия Кнорозова пополнился еще одной замечательной работой. В его переводе со староиспанского языка вышло первое издание на русском языке рукописи Диего де Ланды «Сообщение о делах в Юкатане». Советская историография получила важнейший исторический документ по древним майя, который к тому же является литературным памятником несомненной ценности. С выходом в свет этой книги, опубликованной Академией наук СССР, рукопись Ланды перестала быть достоянием лишь сравнительно узкого круга ученых-американистов; она вошла в новый огромный мир, имя которому – советский читатель.

Но Юрий Кнорозов не только перевел текст рукописи; он подготовил к ней сложнейший справочный аппарат и написал вступительную статью. В результате вместе с рукописью Ланды вышел из печати научный труд огромного значения, содержавший оригинальное, глубокое исследование по истории и цивилизации древних майя и одновременно первый

обобщающий итог работ Ю. В. Кнорозова по дешифровке письменности майя.

Возможно, что при желании и известной настойчивости можно было бы относительно точно подсчитать, сколько тысяч, а вернее, десятков тысяч советских людей за десять лет познакомились благодаря этой книге с самой выдающейся цивилизацией Америки. Но работа молодого советского ученого не только удовлетворяла из года в год растущий интерес советских людей к народам Латинской Америки; она помогла его углублению, правильному пониманию прошлого и настоящего «Бушующего континента», как часто называют Латинскую Америку. И если сегодня ряды советских ученых-латиноамериканистов стремительно растут, ежегодно пополняясь все новыми и новыми молодыми силами, и мы можем теперь говорить о советской школе латиноамериканистики, в этом очевидная и большая заслуга также и Ю. В. Кнорозова и его трудов по древним цивилизациям Америки.

Тогда, в 1955 г., в Институт этнографии для защиты диссертации на соискание ученой степени кандидата исторических наук пришел молодой исследователь, труды которого получили уже мировую известность. Но Юрию Кнорозову так и не суждено было стать «кандидатом». По предложению крупнейших советских ученых ученый совет института тайным голосованием вынес иное решение: соискателю присвоили степень... доктора исторических наук!

Реабилитация «алфавита Ланды». Работа над переводом рукописи Диего де Ланды «Сообщение о делах в Юкатане» оказала неоценимую услугу Юрию Кнорозову в исследованиях по дешифровке древней письменности майя.

После того как им была установлена система письма и в «книгах Чипам Балам» найден сравнительно обширный запас слов древнего языка майя, на котором могли быть написаны рукописи, дешифровщику предстояло приступить к последнему и самому тяжелому этапу своей работы. Он должен был попытаться установить те самые языковые эквиваленты, которые так тщательно скрывались от ученых за причудливыми

знаками письма майя. Иными словами, Ю.В. Кнорозову нужно было правильно распределить 3 сотни знаков майя на три основные категории, из которых складывается любое иероглифическое письмо. Напомним их: это идеографические знаки, передающие корни слов; фонетические – передающие слог или один звук; и знаки-детерминативы, поясняющие смысл слова («лев» – животное; «Лев» – имя собственное).

Начиная изучение иероглифических текстов майя, Юрий Кнорозов, конечно, не мог пройти мимо так называемого «алфавита Ланды». Из многочисленных зарубежных публикаций о майя он знал, что «алфавит» достаточно изучен и не имеет практического значения для дешифровки, коль скоро так утверждали все авторитеты последних лет. Переводя на русский язык сообщение Ланды, Ю.В. Кнорозов подробно ознакомился со всеми комментариями к «алфавиту». К своему удивлению, он обнаружил, что никто даже не попытался полностью прокомментировать «алфавит Ланды» как единый источник.

Чем это было вызвано? Чтобы понять, как могло сложиться столь нелепое положение, нам придется вернуться на целое столетие назад.

Когда в 1863 г. Брассер де Бурбур нашел копию «Сообщения о делах в Юкатане», содержавшую «алфавит Ланды», он решил, что получил в свои руки надежный ключ к чтению текстов майя. Но после первых восторгов наступила пора горьких разочарований. Знаки майя из «алфавита» были настолько искажены переписчиками, что их никак не удавалось обнаружить (отождествить) среди знаков рукописей. Вполне естественно, что у исследователей невольно возник вопрос: а не является ли «алфавит» фальсификацией?

Американский ученый Валентини в 1880 г. написал целую книгу, которую так и озаглавил: «Алфавит Ланды» – испанская фабрикация». В ней он доказывал, что в рукописях Ланды приведены вовсе не знаки письма майя, а простонапросто рисунки различных предметов, названия которых начинаются с той буквы алфавита, под которой они изображены в сообщении (так делают в современных детских азбу-

ках). Например, под буквой «А» в рукописи изображена черепаха (на языке майя «ак»); под буквой «Б» – дорога (на языке майя «бэ») и др. Аргументы Валентини казались настолько серьезными и обоснованными, что, хотя и не все ученые приняли их, они все же произвели достаточно сильное впечатление и ослабили интерес к «алфавиту Ланды». Более того, вскоре и вовсе прекратились попытки отождествить знаки из этого «алфавита» со знаками рукописей майя.

Между тем Брассеру де Бурбуру все же удалось опознать около 1/3 знаков из «алфавита Ланды». Например, знак под буквой «у» очень часто встречался в иероглифических рукописях и как будто мог иметь именно такое чтение. Зато чтение ряда других знаков явно не подходило. Если к этому добавить, что многие знаки из «алфавита Ланды» были опознаны неправильно, то станет понятно, что при попытках подставить чтение по Ланде к иероглифическим текстам получались неразрешимые головоломки.

Было совершенно ясно, что Ланда привел в своем «алфавите» лишь небольшую часть знаков майя, о чем говорил и сам. Некоторые из них встречались в рукописях настолько редко, что ускользали от внимания исследователей, не располагавших в то время ни каталогами знаков, ни справочным аппаратом к иероглифическим рукописям. Во многих разделах рукописей действительно не было знаков из «алфавита Ланды», кроме знака под буквой «у». Сейчас, когда мы знаем, что Ланда привел в своем сообщении менее 1/10 части от общего количества знаков, этому не приходится особенно удивляться; тогда же отсутствие знаков Ланды в рукописях бросало тень на весь «алфавит».

Еще большую неразбериху и путаницу вносили три примера написания слов знаками майя, приводимых у Ланды, два из которых были совершенно непонятны. По словам Ланды, выходило, что для того, чтобы написать слово «лэ» («петля»), майя писали «элээлэ» (?). Это выглядело настолько абсурдным, что никто даже и не пытался объяснить, что, собственно, Ланда мог иметь в виду, когда приводил этот «пример».

Лишь в 1928 г. французский издатель «Сообщения о делах в Юкатане» Жан Женэ взялся прокомментировать эту головоломку. Он высказал предположение, что у майя якобы было два способа написания слов – старый и новый, появившийся уже после испанского завоевания. По «старому способу» майя записывали одним знаком целое слово. Например, слово «лэ» записывалось одним знаком «лэ». По «новому способу» майя почему-то вместо самого слова «лэ» стали записывать названия букв, из которого оно состояло – «эл» – «э». В примере у Ланды, по мнению Женэ, слово «лэ» («петля») записано сначала «новым», а потом и «старым» способами. Поскольку Женэ в своем объяснении пользовался французскими названиями букв, у него получалось, что индейцы майя сразу же после испанского завоевания должны были освоить... французский язык или по крайней мере изучить французский алфавит для своего «нового» способа письма. И хотя предположение Женэ выглядело по меньшей мере забавным, именно он ближе всех подошел к разгадке тайны «алфавита Ланды». Но объяснения Женэ в том виде, как они были изложены им, не внесли никакой ясности; наоборот, они еще больше все запутали.

Неудачи, преследовавшие исследователей «алфавита Ланды», в конечном счете породили всеобщее недоверие к нему, как к достоверному источнику; среди ученых *a priori* считалось, что «алфавит» не заслуживает серьезного внимания.

Точно с такими же настроениями, следуя главным авторитетам современной науки о майя, подошел к «алфавиту Ланды» и Юрий Кнорозов. Полагая, что «алфавит» бесполезен для дешифровки, он все же решил исследовать его, чтобы во вступительной статье и комментариях к переводу «Сообщения о делах в Юкатане» дать ему хотя бы удовлетворительное объяснение, поскольку иначе его собственная работа имела бы весьма существенный пробел. Правда, при этом Ю.В. Кнорозов рассчитывал, что всестороннее изучение «алфавита Ланды» как единого источника может выявить какие-либо новые дополнительные данные, возможно, даже полезные и для дешифровки письменности майя.

В самом деле, знакомство с «алфавитом Ланды» невольно порождало целый ряд недоуменных вопросов. Почему Ланда, сведения которого всегда отличаются исключительной точностью, именно в этом случае допускает очевидную неразбериху – попросту говоря, чепуху? Ведь иероглифы месяцев он привел абсолютно точно, следовательно, Ланда располагал сведениями о письме, а алфавит фальсифицировал? Зачем? Ведь свою рукопись он предназначал францисканским монахам, а их-то вводить в заблуждение ему было совершенно незачем! Что означают абсурдные примеры написания слов? Быть может, индейский «консультант» умышленно мистифицировал самого Ланду? Если так, следовало бы разобраться в существе мистификации, ибо Ланда, как уже говорилось, имел представление о характере знаков майя и обмануть его можно было только очень умело и тонко. Между тем написание слова «петля» в виде «элээлэ» представляется не то чтобы тонкой, а грубейшей и даже абсурдной подделкой!

Словом, вопросов возникало множество, причем какого-либо вразумительного ответа на них не предвиделось. Объяснения Женэ были невероятными хотя бы потому, что после испанского завоевания у майя заведомо не было никакого иероглифического письма – ни «старого», ни «нового». Об этом позаботились испанские миссионеры, возглавляемые провинциалом Диего де Ландой; когда же иероглифическое письмо было уничтожено, индейцы перешли на латиницу.

Бесконечные «зачем» и «почему» лишь усиливали убежденность в необходимости попытаться полностью прокомментировать «алфавит Ланды». Вопроса «С чего начинать?» не было: располагая обширными сводками вариантов написания знаков, взятых из рукописей и других надписей майя, Юрий Кнорозов приступил к работе по отождествлению знаков из «алфавита Ланды» со знаками иероглифических текстов. Тяжелый труд продвигался чрезвычайно медленно, зато результат его оказался невероятным: все знаки алфавита Ланды (наконец с него можно снять кавычки!) были найдены в рукописях!..

Такое положение в корне меняло отношение к алфавиту. Пожалуй, теперь следовало разобраться, по какому принципу он составлялся вообще. Ланда привел в своем списке двадцать семь знаков. Он писал, что они соответствуют буквам испанского алфавита. Над каждым из знаков он написал соответствующую букву. Все буквы идут в основном в порядке испанского алфавита, однако Ланда допустил ряд отклонений. Почему? Вот это и следовало изучить. Именно характер и причины отклонений могли объяснить ход рассуждений составителя алфавита.

То, что в алфавите Ланды отсутствовали некоторые буквы испанского алфавита, например Д, Ф, Г, Р, объясняется просто – этих звуков не было в языке майя, на что неоднократно указывал сам Ланда. Не вызывало особых недоумении и двойное «П»; миссионеры знаком «ПП» передавали отсутствующий в испанском языке особый звук майя. Ланда указывал и на эту особенность языка индейцев и учитывал ее.

Но дальше начинались настоящие головоломки. У Ланды букве «Б» почему-то соответствовал не один, а целых два знака майя. То же самое имело место с буквами «Л» и «Ш» (в староиспанском языке буква «икс» (Х) произносилась как русское «Ш»). Может быть, два разных знака читались одинаково? Теоретически это возможно. Однако если письменность майя была иероглифической, то представлялось более вероятным, что в письме майя были скорее знаки, передающие схожие по звучанию слоги, например: «БА», «БО», «БУ», «БЕ», «БИ», образованные из одного согласного звука в сочетании с различными (или со всеми) гласными. Но в этом случае Ланда должен был бы под одной испанской буквой написать не один или два знака майя, а все пять! Однако он этого не сделал. Почему?

Проще всего предположить, что Ланда взял один или два первых попавшихся знака, однако это не похоже на него. Он был слишком выдающимся знатоком майя и любил все делать основательно и систематически (вспомним хотя бы, с какой тщательностью он провел «операцию» по уничтожению

рукописей майя, если из сотен «еретических книг» до нас дошли только три!). По-видимому, у него все же были какие-то основания для выбора, но какие? Как, по какому принципу он отобрал два знака из пяти?

Сразу же (и в который раз!) захотелось убедиться в правильности предположения, что у майя действительно были слоговые знаки. Гаспар Антонио Чи сообщал, что майя писали с помощью слоговых знаков. Это уже немало, но все же еще недостаточно. Ланда тоже, хотя и с оговорками, подтверждал это же – «они пишут по слогам» – и даже привел пример, поясняющий именно такой способ написания.

Над знаками майя он поставил испанские буквы «МА – И – Н – КА – ТИ». На майя «ма ин кати» означает «я не хочу». В целом пример казался ясен. Правда, индейцы – майя не писали свои знаки в строчку; кроме того, в иероглифических текстах не удалось найти ни глагола «кати» (хочу), ни местоимения «ИН» («Я»). Зато знак «ТИ» стоял в текстах как раз там, где можно было ожидать предлога «ТИ» («В»).

Первый знак из этого примера – «МА» – отсутствует в алфавите Ланды (но мы знаем, что алфавит не полный); под буквой «М» приведен совсем иной знак. Второй и третий знаки из примера имеются в алфавите и стоят они под теми же буквами «И» и «Н». Четвертый знак стоит под буквой «К» (K), а в примере прочтен как «КА», т.е. как слог. Это уже прямое подтверждение предположения о том, что в алфавите Ланды слоговые знаки. Тогда, может быть, и другие знаки алфавита так же передают слоги?.. Ланда сам в трех случаях надписал над знаком майя не букву, а слог. Интересно, чем это объясняется?..

В испанском алфавите после «И» (I) идет буква «хота» (J), передающая звук, отсутствующий в языке майя, а затем следует «К» (K). В языке майя было два варианта звука «К» – твердый и мягкий. Миссионеры обозначили мягкое «К» испанской буквой «С», которая перед «А», «О», «У» произносится как русское «К», а перед «Е» и «И» как русское «С». Твердое «К» (в русской транскрипции оно записывается так – К') обозначалось испанской буквой «К» (K). В алфавите Ланды вслед за

«И» стоит знак майя, над которым написано «КА» (CA) и лишь потом уже идет знак под буквой «К» (K). Но в рассматриваемом нами примере, он прочтен Ландой не просто «К», а как «К'А». Столь скрупулезно тщательный подход к форме написания буквы, передающей, по сути дела, один и тот же согласный звук, но только мягкий и твердый, свидетельствует о том, что Ланда придавал исключительно большое значение даже правильному произношению отдельных звуков, стремясь подчеркнуть это в своем алфавите.

После «П» (P) в испанском алфавите идет буква «Ку» (Q). Эту букву миссионеры не использовали для передачи какого-либо звука языка майя, однако Ланда счел необходимым на ее месте привести два знака майя, над которыми написал «КУ» (CU) и «К'У» (KU). Таким образом, он снова подчеркнул наличие у майя двух вариантов звука «К» (мягкого и твердого).

Теперь уже можно было не сомневаться в том, что знаки алфавита Ланды передают не отдельные согласные звуки, а слоги, например, «КА», «К'А», «КУ», «К'У», «МА», «ТИ», ибо Ланда сам об этом говорит.

Все это лишний раз убеждало, что Ланда тщательно и, видимо, по какому-то специальному признаку подбирал знаки майя и испанские буквы, прежде чем соединял их вместе в своем алфавите. Похоже, что, наконец, стало выясняться то, чем он руководствовался. Однако не будем торопиться. Лучше еще раз все проверим:

на месте буквы «Ку» (Q) – в испанском алфавите она так и называется «КУ» – Ланда привел слоговые знаки «КУ» (CU) и «К'У» (KU), а на месте буквы «К» (K) – она называется «КА» – он поставил слоговые знаки «КА» (CA) и «К'А» (KA).

Так вот оно в чем дело! Вот в чем принцип и секрет алфавита Ланды! Оказывается, он подбирает слоговой знак майя, соответствующий названию испанской буквы?!

Спокойно! Нужно не торопясь, последовательно еще раз проверить столь важный вывод. И потом – может быть, звук «К» – это только исключение, а весь алфавит вовсе и не строится на подобном принципе? Впрочем, это легко узнать. Если

таков принцип всего алфавита Ланды, то знак майя под буквой «Б» читается не как «Б», а «БЭ», поскольку таково ее название. К сожалению, этот знак встречается в рукописях майя только один раз; это явно мало для проверки правильного чтения. Однако и в этом единственном случае все же получилось вполне осмысленное чтение: «ТИ БЭ» (оба знака по Ланде), что означает на майя «В ДОРОГЕ».

Следующая буква в испанском алфавите «С»;

она называется «СЭ». Хотя, как указывалось, она читается двояко (и как русское «С», и как русское «К»), миссионеры в транскрипциях слов или текстов на язык майя (т.е. когда они писали латиницей) всегда употребляли эту букву как мягкое «К» (звук «С» передавался буквой «Z»), Если же Ланда действительно приводил слоговые знаки, соответствовавшие названиям испанского алфавита, он не должен был учитывать эту особенность, и знак майя под буквой «С» следовало читать «СЭ». Это сразу же подтверждается: название месяца «СЭК» было записано двумя знаками «СЭ-КА», причем оба они из алфавита Ланды! Сомнения окончательно исчезли. Алфавит Ланды, наконец, «заговорил» в полный голос, а это означало огромный шаг вперед на пути дешифровки письменности майя!

Однако на этом работа с алфавитом не прекратилась. Когда выяснилось, что знаки майя в алфавите соответствуют названиям испанских букв, Юрий Кнорозов решил, что настало время попытаться разобраться и в двух примерах-головоломках написания слов. Это было важно еще и потому, что ведь сам Ланда привел их в подтверждение (!) правильности своего алфавита, хотя на деле все получилось наоборот. Как раз «примеры» больше всего запутывали исследователей; именно они были той последней каплей, а вернее, тем ушатом холодной воды, который «отгонял» дешифровщиков от алфавита.

В первом из них, по словам Ланды, записано слово «ЛЭ» («петля», «силок»). Знак, над которым надписано «ЛЭ», в алфавите Ланды стоит под буквой «Л» (L); по-испански она называется «ЭЛЭ». Но у Ланды записано не «ЛЭ», а целое «Э-ЛЭ-Э-ЛЭ» (?!?).

Вглядитесь внимательно в этот «комплект» из двух букв! Только очень внимательно, и вы тогда поймете, в чем дело; почему пример стал абсурдным набором двух букв!

В старину в русских школах учитель диктовал ученикам: «Напишите, дети, слово «баба»: «БУКИ-АЗ-БУКИ-АЗв... баба!» Вот эти же самые, но только испанские «буки-аз-буки-аз» и записал писец, видимо, под диктовку Диего де Ланды. Диктуя слово «ЛЭ», Ланда вначале назвал его по буквам, а затем и целиком: «ЭЛЭ» (название буквы «Л»), «Э» (название буквы «Э», совпадающее с ее звучанием) – «ЛЭ» («петля»). Писец, очевидно не очень понимавший такую форму «диктанта», на всякий случай записал все, что произнес будущий епископ, и тогда-то и родилось столь непонятное и абсурдное «Э-ЛЭ-Э-ЛЭ»!

Чтобы проверить свою догадку (назовем ее без лишней скромности блистательной), Юрий Кнорозов начал искать слово «ЛЭ» в рукописях майя и нашел его: оно было записано там с помощью знаков «ЛЭ» и «Э», указанных в алфавите Ландой!

Теперь можно было перейти ко второму примеру, столь же непонятному и абсурдному. Естественно, что сразу же возникла мысль о «диктанте»: может быть, и здесь сплоховал писец? Ланда указывал, что в примере третий знак обозначает на майя слово «ХА» («вода»), а между тем вместо этого над знаком стояло «АК-ЧЁ-АХА» (?!)

Попробуем продиктовать слово «ХА» по буквам, произнося по-испански названия букв: «ХОТ-А»... «ХА». Что-то не получилось, а ведь это единственный вариант произношения названий букв, которые соответствуют нужным звукам слова майя! Правда, три последние буквы-звуки точно совпадают, но что делать с четырьмя первыми?

И тогда исследователя выручают знания и память; они-то и приходят к нему на помощь! В испанском алфавите имеется «немая» буква, изображаемая следующим образом – «h». Она

сохранилась только по традиции и не произносится. Но миссионеры использовали ее при письме на майя латиницей для передачи звука... «Х»! Название же этой буквы «аче!» Теперь снова продиктуем слово «ХА» по буквам: «АЧЕ-А»... «ХА»! Вроде бы все получилось, но только в рукописи у Ланды одна «лишняя» буква: «АК-ЧЕ-А-ХА». Откуда она взялась? Откуда? Попробуйте произнести громко вслух «АЧЭ-А... ХА», и вы легко услышите этот недостающий звук. По-видимому, писцу также показалось, что между «А» и «Ч» он «услышал» еще и «К»; будучи человеком прилежным, он записал его, не сознавая, какой великий грех берет на свою душу из-за этой ошибки!

Так была разгадана еще одна головоломка: третий знак во втором примере следовало читать просто «ХА» («вода»), как правильно указывал сам Ланда.

В результате длительных и мучительно скрупулезных исследований алфавит Ланды был полностью «реабилитирован». Произошло это не сразу и не случайно. Потребовались годы напряженного труда. Невероятно трудным оказалось опознание знаков алфавита, их отождествление со знаками рукописей. Мы уже говорили, что переписчики сообщения допустили много искажений, перерисовывая знаки майя из его алфавита. Однако и сами иероглифические рукописи майя написаны часто небрежно, без должного «каллиграфического» искусства и старания. Не следует забывать, что они ведь не предназначались для чужеземных читателей и для чтения через тысячу лет! Их писали для повседневного пользования. К тому же «почерки» древних писцов не могли быть одинаковыми, как не одинаковы почерки окружающих нас людей.

Однако само по себе опознание знаков еще ничего не давало. Необходимо было понять смысл старинных терминов, которые Ланда употреблял в своей рукописи (например, «слог» он называл «частью»), выяснить, как произносились испанские буквы и как они назывались во времена, когда писалось сообщение. Не менее сложным оказался вопрос о диктовке, о ее форме, ибо о том, что Ланда диктовал, а не сам писал оригинал рукописи, мы можем лишь догадываться.

Наконец, была еще одна грозная опасность, постоянно поджидающая каждого исследователя, преодолеть которую бывает необычайно трудно. Речь идет порой о необоримом соблазне, часто бессознательном, принять желаемое за действительное и внести соответствующие «исправления» в исследуемый документ. Как правило, и к великому сожалению автора «исправлений», они, эти «исправления», впоследствии отвергаются, но не в порядке самокритики, а критики со стороны. Хорошо зная об этом, Юрий Кнорозов после долгих проверок и перепроверок все же рискнул предложить два исправления к алфавиту Ланды. Первое из них заключается в следующем; знак майя под испанской буквой «Т», почему-то стоящей не на обычном для нее месте в конце испанского алфавита, а в самом его начале (сразу после третьей буквы «С»), как выяснилось, по другим данным имеет чтение «КЭ». Повидимому, Ланда и здесь привел два чтения буквы «С», соответствующее ее двоякому чтению: «СЭ» и «КЭ». Основываясь на этом, Ю. В. Кнорозов считает, что при копировании рукописи могла вкрасться простая ошибка: писец спутал испанские буквы и вместо «К» поставил «Т» (возможно, что его смутило, что буква «К» также стояла и в другом месте алфавита).

Вторая поправка Ю.В. Кнорозова относится к предпоследнему знаку алфавита Ланды. В алфавите над двумя знаками майя написана буква «У» (U). Первый из них действительно так и читается – «У». Это подтверждено многочисленными примерами из иероглифических рукописей. Знак под вторым «У» явно не мог иметь такого чтения. Между тем в испанском алфавите предпоследней буквой является «игрек» (Y), читающийся как «йе». Юрий Кнорозов решил, что и здесь также произошла описка, кстати, довольно распространенная и в наши дни (читатель наверняка не раз ловил себя на подобных описках): вместо буквы «Y» писец вывел «U». То, что предпоследний знак майя из алфавита Ланды должен читаться «йе», позднее было подтверждено и другими данными.

А теперь о главном: Диего де Ланда правильно записал весь свой алфавит. Он составлен с большим знанием дела, хо-

тя сам Ланда не придавал ему большого значения, рассматривая его только как иллюстрацию. Единственная ошибка Ланды – это недоразумение с двумя первыми примерами записи слов; две другие ошибки появились позже по вине переписчиков. О том, как «родилась» ошибка самого Ланды, мы можем только предполагать.

По-видимому, в составлении и записи алфавита принимали участие три челов.: Ланда, монах-писец и специально приглашенный для составления алфавита «консультант» по вопросам иероглифической письменности майя; будущий епископ, очевидно, не владел ею. Ланда называл букву испанского алфавита и вместе с «консультантом» подыскивал наиболее близкие грамматические частицы из языка майя. Затем «консультант» рисовал соответствующий знак из иероглифического письма, а писец сверху выводил испанскую букву.

Все шло хорошо; удалось даже учесть особенности произношения некоторых согласных, однако когда дело перешло к написанию примеров, возникло первое недоразумение. «Консультант» написал иероглифами слово «петля» и сказал: «ЛЭ». Писец почему-то не расслышал его и попросил повторить. Возможно, к этому времени все трое устали, однако это не должно было, по мнению Ланды, отразиться на качестве рукописи. И он сам продиктовал не понятое писцом слово вначале по буквам (чтобы было яснее!): «ЭЛЭ»... «Э», а затем повторил слово целиком – «ЛЭ». Это окончательно сбило с толку писца, незнакомого с подобной формой «диктанта», – возможно, это был крещеный индеец, – однако, опасаясь крутого нрава первого провинциала Юкатана, он не решился переспросить его и написал знаками майя буква в букву то, что услышал: «ЭЛЭЭЛЭ»...

«Консультант» нарисовал новый иероглиф. Скорее всего Ланда задумался, как лучше передать испанскими буквами слово «ХА» («вода»). Использовать ли «хоту» или «аче»? «Аче», – решил он, вспомнив пример записи языка майя латиницей. Поскольку эта буква по-испански вовсе не звучала, ему не оставалось ничего другого, как вновь прибегнуть к

диктанту по буквам: «АЧЭ»... «А», – произнес он названия букв, а затем и все слово – «ХА». Изумленный, а может быть даже испуганный, писец – он снова ничего не понял! – буква в букву записал услышанное...

Так было или иначе, но ошибка вкралась в текст «Сообщения о делах в Юкатане», и самое удивительное то, что Ланда не исправил ее. Возможно, он настолько доверял своему писцу, что даже не считывал после него текста? На Ланду, судя по его характеру, это не похоже, но... именно эта ошибка и не очень качественное изображение переписчиками знаков майя в алфавите Ланды поставили в тупик несколько поколений исследователей древней письменности майя! Примеры-головоломки и опознание знаков было настолько трудным делом, что оно оказалось не под силу даже такому знатоку майя, как Эрик Томпсон, составитель наиболее подробного и полного каталога знаков майя.

Начиная свое исследование алфавита Ланды, Юрий Кнорозов и сам не предполагал, какие удивительные открытия ждут его впереди. Но настойчивый поиск молодого ученого, сумевшего через 4 столетия постепенно, шаг за шагом восстановить ход рассуждении провинциала Ланды, подарил миру ценнейший документ об одном из наиболее выдающихся и поразительных достижений цивилизации майя. Вопреки мнению всех крупнейших знатоков письма майя именно алфавиту Ланды, реабилитированному «в далекой Советской России», предстояло сказать свое веское слово в изучении письменности майя.

Несмотря на досадные ошибки в алфавите Ланды и в примерах написания слов иероглифическими знаками майя, Юрий Кнорозов не мог не восхищаться глубокой продуманностью, логичностью и почти безупречной точностью этого документа, который на невероятно малом материале раскрыл сущность иероглифической письменности древних майя. Именно поэтому его заинтересовал вопрос: кто, кроме Ланды, был автором этого документа? Кем был индейский «консультант», как его звали и почему Ланда привлек именно его к своей работе над алфавитом?

Иероглифическим письмом владели только жрецы майя, да и то не все. Кроме них, письму могли быть обучены лишь очень знатные лица, изучавшие науки, как писал Ланда, из любознательности. Но жрецы, уцелевшие от побоищ, были смертельными врагами монахов – своих конкурентов по «ремеслу». Ланда прямо указывает, что «более всего неприятностей, хотя и тайно, монахам причиняли жрецы, которые потеряли свою службу и доходы от нее». Неоднократно упоминавшийся нами «консультант» Ланды Гаспар Антонио Чи получил испанское образование и, конечно, не допустил бы при диктовке таких ошибок. Кроме того, весьма сомнительно, чтобы он знал иероглифическую письменность: с 15-ти лет он уже обучался у испанских монахов.

Знакомство с индейским «окружением» Ланды приводит Юрия Кнорозова к выводу, что «консультантом» по иероглифике майя у будущего епископа мог быть только На Чи Коком, последний правитель Сотуты. Во время конкисты Юкатана он оказал испанцам отчаянное сопротивление, но в конце концов был взят в плен, принял христианство и стал именоваться дон Хуан Коком. Ланда был дружен с ним; они часто и подолгу беседовали; от него он узнал и записал историю Юкатана. Ланда упоминает вскользь, что дон Хуан показывал ему иероглифическую рукопись, доставшуюся от деда, сына последнего правителя могучего города-государства Майяпана (династия Кокомов правила Юкатаном с 1244 г.), погибшего в 1541 г. при разгроме этой столицы майя испанскими завоевателями. Просвещенный правитель Сотуты, имевший иероглифические рукописи, очевидно, умел их читать, но испанской грамоте (а тем более французской – вспомните гипотезу француза Женэ!) не обучался и, конечно, понятия не имел об испанском способе диктовать слова по буквам.

Один из последних знатоков письменности майя. На Чи Коком, хотя и принял христианство и даже «дружил» с провинциалом Диего де Ландой, втайне оставался верен религии и обычаям своего народа. Незадолго до смерти На Чи Коком приносил богам человеческие жертвы, надеясь на выздоров-

ление. Но боги не пожелали сохранить ему жизнь и тем «спасли» его от мучительной смерти, от пыток в застенках инквизиции. Он умер в 1561 г. за несколько месяцев до начала инквизиционного следствия об «отступничестве от христианства», которое вел его «друг» Диего де Ланда. Брат На Чи Кокома, также оставшийся тайным язычником, не ожидая окончания следствия инквизиторов, повесился. Ну, а что произошло в городе Мани 12 июля 1562 г., читатель уже знает.

Иероглифические знаки в «Сообщении о делах в Юкатане» были начертаны рукой последнего потомка когда-то всесильных властителей Юкатана. Он сделал это по просьбе своего «друга» – первого провинциала единой церковной провинции Гватемалы и Юкатана Диего де Ланды. И пока один из них старательно выводил на бумаге замысловатые знаки, умевшие «говорить» языком его древних предков, другой хладнокровно обдумывал, как лучше, быстрее, а главное, раз и навсегда уничтожить все то, что связывало народ майя с его недавним и далеким прошлым. Возможно, они улыбались друг другу, хотя их сердца горели неугасимой ненавистью, и наверняка никто из них не догадывался, что столь удивительный симбиоз четыре столетия спустя поможет приоткрыть завесу над великой тайной жрецов майя.

Таково происхождение уникального источника, известного под названием «алфавит Ланды», и история его реабилитации.

Что такое дешифровка или окончание поиска. Итак, мы подошли к последнему этапу длинного и тяжелого пути. Позади остались многие годы кропотливого и сложного труда, пролетевшие быстро, почти незаметно. Взбираясь на крутую вершину познания тайны письма жрецов майя, молодой дешифровщик, подобно скалолазу, преодолевал многочисленные препятствия. И вот остался последний и самый крутой подъем. Нужно сделать еще несколько шагов. Но как они тяжелы, с каким невероятным трудом дается каждый новый метр этого титанического восхождения! Он требует полной отдачи сил, опыта и знаний, накопленных г.ми. Любая, даже

малейшая ошибка отбросит исследование назад, и тогда найдутся ли силы, чтобы вновь попытаться достичь столь желанной вершины поиска?!

Триста знаков! Много это или мало? Триста знаков! Они похожи на маленьких букашек, живущих своей, пока еще неведомой для нас жизнью. Их нужно освоить, подчинить – они, эти триста знаков, та самая вершина, покорить которую мечтало столько ученых!

Снова и снова начинаются бесконечные сопоставления, требующие скрупулезной точности. Времени не хватает, приходится работать ночами. Глаза устают так, что голову разламывает невыносимая боль и кажется, что ты уже ничего не видишь. Не видишь? Страшная мысль, к сожалению, не лишенная оснований... Врачи уже махнули на тебя рукой, но ведь и они ошибаются! Тысячи, тысячи, тысячи знаков прыгают на серых страницах фотобумаги. Тысячи, тысячи, тысячи, а ведь их всего триста! Как, по какому принципу собираются они вместе, заполняя страницы рукописей или каменные барельефы стел?..

В большинстве языков мира, в том числе и в языках семьи майя-кичэ, склонение и спряжение связано с появлением в начале и конце слога грамматических показателей. В русском языке такими грамматическими показателями являются, например, хорошо знакомые нам окончания падежей, не имеющие сами по себе смысла и относящиеся к какому-нибудь осмысленному (знаменательному) слову. К грамматическим показателям относятся также различные частицы, предлоги, союзы. Именно они, словно сцепщики железнодорожного состава, скрепляют вместе разрозненные отдельные слова, связывая их в осмысленное предложение. При увязке слов друг с другом очень важную роль играет также их порядок в предложении, свойственный данному языку.

Приведем наипростейший пример. Возьмем пять слов: комната, стол, стоять, красный, зеленый. Заложена ли какая-нибудь идея (смысл) в этом наборе слов? По-видимому, нет. Однако «включив» грамматические показатели русского языка, мы получим осмысленное предложение: «В красной комнате стоит зеленый стол».

В тексте, написанном известным или неизвестным письмом, корню слова (если, конечно, это слово повторяется) должна соответствовать устойчивая группа знаков. Грамматическим же показателем в начале или конце слова должны соответствовать меняющиеся и заменяющие друг друга знаки (Ю.В. Кнорозов называет их «переменными») перед или после устойчивой группы знаков.

Вновь обратимся за примером к русскому языку: в русском тексте сочетание трех букв (знаков) «дом» будет устойчивым, а падежные окончания – «дом-а», «дом-у», «дом-ом» – будут передаваться «переменными» буквами (знаками) «а», «у», «ом».

Языку майя, как уже говорилось ранее, не чужды обе грамматические категории, и Ю.В. Кнорозов счел необходимым прежде всего выявить в иероглифических текстах майя устойчивые группы знаков (передающие корни слов древнего языка) и связанные с ними переменные знаки (передающие грамматические показатели). Следовало предположить, что их общее количество не должно быть велико, и их можно будет сопоставить с грамматическими показателями в текстах майя колониального периода («книги Чилам Балам»), записанных латиницей.

Работа по выявлению переменных знаков шла мучительно медленно и была чрезвычайно громоздкой. Ведь каждое сочетание знаков (иероглиф) приходилось прослеживать по всем рукописям и надписям майя. При этом постоянно возникали затруднения.

Мало того, что в иероглифических рукописях часто встречаются стертые и полустертые места, «оборванные» страницы и другой «производственный» брак, причиненный временем и не всегда умелым хранением этих текстов. Выяснились и иные «враги» дешифровщика: некоторые разделы рукописей, особенно Мадридской, были написаны на редкость небрежным почерком и к тому же со множеством ошибок (куда смотрели старшие жрецы?!). Не лучше обстояло дело и с каменными книгами – стелами:

тропические ливни сильно размыли поверхность камней с надписями. На опознание многих знаков, различные проверки и перепроверки приходилось тратить слишком много времени и сил.

Но, может быть, лучше отказаться от этой работы и исследовать только те иероглифы, которые не пострадали от времени или недобросовестности жрецов – переписчиков текстов?

В результате проделанной работы Ю. В. Кнорозов свел иероглифы в группы. В каждую из них входили иероглифы, имеющие одинаковые устойчивые знаки и различные переменные, т.е. различные грамматические показатели. Теперь можно было свести вместе слова с одинаковыми грамматическими показателями. По сравнению со сделанным такая работа была относительно несложной.

Сплошная регистрация всех случаев появления в тексте каждого иероглифа позволила одновременно выявлять и статистические данные о них. Самый простой способ применения статистики для целей дешифровки (уже упоминалось об этом) состоит в том, что подсчитывается, сколько раз каждый из знаков встречается в исследуемом неизвестном тексте. Это абсолютная частота. Заручившись такими данными о неизвестных нам знаках, следует подобным же образом обсчитывать тексты майя, записанные латиницей, т.е. известными нам знаками – буквами. Зачем? Чтобы сопоставить неизвестные знаки с буквами (или группой букв), имеющими ту же частоту в известных текстах!

Однако в ряде разделов рукописей майя настойчиво повторяются отдельные иероглифы, очень редко встречающиеся в других местах. При сплошном подсчете легко может оказаться, что знак имеет большую частоту за счет многократного повторения одного и того же иероглифа, т.е. за счет частого повторения какого-нибудь слова в некоторых разделах текста. В этом случае абсолютная частота знака (равно как и иероглифа, в состав которого он входит) будет отражать не особенности языка, а особенности данного специфического текста с часто повторяющимся отдельным словом или словами (на-

пример, в тексте, рекламирующем, скажем, пылесос, слова «пылесос» и «пыль» будут повторяться значительно большее количество раз, чем в любом другом). Чтобы избежать подобной ошибки, можно при подсчете частоты пропускать повторения одного и того же иероглифа (слова), получая относительную частоту, не зависящую от особенностей текста.

Однако установление абсолютной и относительной частоты знаков было еще недостаточно для достижения конечной цели, стоявшей перед Ю.В. Кнорозовым. Поэтому он считал ближайшей задачей изучение переменных знаков, передающих грамматические показатели. Нужно было выявить частоту переменных знаков, а это означало, что при подсчете частоты нужно учитывать только те случаи, когда знак передает грамматический показатель, т.е. стоит перед или после корня слова.

Вновь прибегнем к примеру из русского языка, Для того чтобы установить частоту показателя дательного падежа – «у» (в словах дом-у, храм-у, пруд-у и т.д.), нужно подсчитать, сколько раз буква «у» встречается в конце определенных слов, но при этом отнюдь не следует учитывать случаи, когда она входит в состав корня (как в слове «пруд»)!

Изучение частоты знаков, занимающих определенное место (позицию) в словах получило название «позиционной статистики». Точный язык цифр – математический анализ снова пришел на помощь молодому советскому исследователю. С помощью позиционной статистики можно было сравнительно легко сопоставить грамматические показатели языка иероглифических текстов майя с грамматическими показателями языка майя колониального периода, сохранившегося в «книгах Чипам Балам».

Но Ю.В. Кнорозов не спешил начать сопоставление грамматических показателей древнего и нового языков майя, хотя выявление переменных знаков и их позиционной частоты давало такую возможность. Он решил еще более основательно подготовиться к преодолению последних и самых трудных шагов, все еще отделявших его от заветной цели. Поэтому он подвергает исследованию порядок слов в предложе-

ниях майя, используя свой же метод позиционной статистики. Но теперь он применяет его уже не к отдельным знакам, а к целым иероглифам.

Выяснилось, что на втором и третьем местах в предложениях всех типов, как правило, стоят иероглифы, не имеющие в своем составе переменных знаков. Были все основания считать, что иероглифы этой группы передают подлежащее. В самом деле, именно подлежащее, т.е. обычно имя существительное в именительном падеже, имеет меньше всего грамматических показателей.

Другая группа иероглифов отличалась, наоборот, наибольшим количеством переменных знаков. Иероглифы этой группы стояли, как правило, на первом месте в предложениях почти всех типов. Судя по большому количеству переменных знаков, эти иероглифы должны были передавать глагольное сказуемое. По ходу дальнейших исследований оказалось, что иероглифы, передающие сказуемое, подразделяются на две группы, каждой из которых свойственны свои грамматические показатели. После иероглифов одной группы в предложениях стояло сразу подлежащее, тогда как после иероглифов другой почти всегда появлялись особые дополнительные иероглифы, а подлежащее отходило на третье место. Естественнее всего было отождествить первую группу с непереходными глаголами, а вторую – с переходными, требующими дополнения. Так оно и оказалось, ибо и в языке майя XVI в. был аналогичный порядок слов в предложении. На первом месте обычно стояло глагольное сказуемое, а подлежащее занимало второе место или третье, если после сказуемого шло дополнение.

Только теперь Ю.В. Кнорозов располагал достаточно четкой классификацией иероглифов. О каждом из них можно было сказать, с какими грамматическими показателями он употребляется, какую часть речи передает и какую роль играет в предложении.

Казалось, можно переходить к последовательному сопоставлению грамматических показателей языка иероглифических текстов, т.е. неизвестного языка и языка майя XVI в., из-

вестного нам. Известного? Однако оказалось, что грамматика «известного» языка изучена довольно слабо, И снова пришлось отложить решающий штурм последней вершины и надолго засесть за изучение грамматики по текстам майя, записанным латиницей, и только после этого заняться подготовкой сравнительных материалов – выявлением набора грамматических показателей и их частоты в текстах XVI в.

Это была наиболее тяжелая и изматывающая работа. Она требовала абсолютной внимательности. Если возникали сомнения в правильности подсчета, нужно было начинать его с самого начала и так по нескольку раз. Но самое обидное: не было никакой гарантии в том, что получаемые с таким трудом данные окажутся полезными и пригодятся для дальнейшей дешифровки. Так оно и было в ряде случаев, когда единственным результатом проделанной работы являлось выяснение того, что изучаемый грамматический показатель не имеет никаких аналогий в древнем языке. Не удивительно, что при первой же возможности в дальнейшем и Ю.В. Кнорозов и другие исследователи стали перекладывать такого рода работу на «плечи» вычислительной техники.

Однако в целом расчеты Ю.В. Кнорозова на то, что сопоставление древних переменных знаков с известными грамматическими показателями (из языка XVI в.) окажется сравнительно легким, вполне оправдались. В центр внимания исследователя попало несколько знаков, передающих употребительные грамматические показатели. Эти знаки оказались как бы в медленно, но верно сжимающемся кольце. Каждая новая, дополнительная характеристика этих переменных знаков была подобна новому, появлявшемуся из засады щупальцу спрута. Они, эти щупальца-знаки, обвиваясь вокруг жертвы, неуклонно приближали свою привязку.

Среди переменных знаков особо выделялся знак *If***.** Он сочетался и с глаголами и с существительными и имел рекордную позиционную частоту. Такую же высокую частоту в текстах XVI в. имел только один грамматический показатель – префикс-местоимение «у» («он», «его»). Здесь не могло быть ошибки – знак определен точно, ему найден языковый эквивалент!

Сопоставление ряда других переменных знаков с известными грамматическими показателями также не составило особого труда. Наиболее часто встречающийся переменный знак **\«/**, передающий предлог, легко сопоставлялся по позиции и частоте с употребительным предлогом «ти» («в», «к»), а переменный знак **Э** в конце переходных (требующих дополнения) глаголов явно соответствовал известному глагольному суффиксу прошедшего времени – «ах».

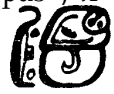
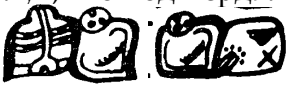
Но не все шло так гладко. Огромные затруднения встречались в тех случаях, когда произношение сильно изменилось. Например, употребительному суффиксу непереходных глаголов **^-^o^** – явно не было прямой аналогии в языке XVI в. Только значительно позже, в результате длительного изучения спряжения в языке майя, Ю.В. Кнорозов сумел выяснить, что суффиксы непереходных глаголов XVI в. («хи», «ни», «и») восходят к одному и тому же древнему суффиксу – «нхи». Иными словами, оказалось, что переменному знаку **^-^д^3*** соответствует исчезнувший суффикс, от которого в языке XVI в. сохранилось несколько «потомков» (с одинаковым значением).

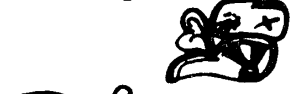
Так была решена ближайшая главная задача. Однако сопоставление грамматических показателей языка иероглифических текстов с известными грамматическими показателями языка майя XVI в. еще не означало действительного чтения знаков. Отнюдь не исключено, что древние суффиксы или предлоги произносились иначе, чем в XVI в. Чтобы установить их действительное чтение, нужно перейти к следующему этапу – чтению слов. Этот этап и был конечной целью – завершением дешифровки.

Но как, на основе каких данных можно попытаться прочесть сами слова? Существует ли такая возможность?

Ю.В. Кнорозов рассуждал следующим образом: если знак, передающий, например, предлог, который в XVI в. произносился как «ти», действительно имел такое чтение, тогда можно прочесть слова, в которых знак употребляется уже не как грамматический показатель, а для записи корневой части слова. Ведь знак должен читаться одинаково во всех случаях!

Но чтобы считать чтение знака окончательно установленным, необходимо прочесть не меньше двух разных слов с этим знаком. Это и есть так называемые перекрестные чтения.

Установив, что знаки **^Ц^. . ' 9J** и др. передают грамматические показатели, которые в XVI в. соответственно произносились, как ти, ка, ан, у, ах, Ю. В Кнорозов, пользуясь заранее составленными сводками иероглифов, сумел подобрать нужные группы знаков. Так, слово  он прочел «му-ти», приписав первому знаку чтение «му»; второй же знак употреблялся для передачи предлога «ти». На языке XVI в. слово «мут» означало «священное животное». Это значение подтвердилось в словах  - «Му-ка» («мук» – «раз») и  «му-ан» («облачный», название месяца). Слово  Ю.В. Кнорозов прочел «у-лу-му» («улум» – «домашний индюк»), приписав второму знаку чтение «лу», что подтвердилось в словах – «цу-лу» («цул» – «собака»)  и – «(бу)-лу-ку» («бу-лук» – «одиннадцать»).

В свою очередь, чтение знака  – «цу» подтвердилось в слове  «ку-цу» («куц» – «дикий индюк»), чтение знака  — «ку» в слове «ку-чу» («куч» – «ноша»); чтение знака «чу» – в слове  – чу-ка-ах (чу-ках» – «захватил») и т.д.

Цепляясь один за другой, знаки майя постепенно открывали дешифровщику свои сокровенные тайны, как раскрывает тайну кроссворда правильно найденное слово. Разумеется, чтение каждого нового неизвестного знака требовало перебора различных вариантов, пока не находился единственно правильный. Однако количество таких вариантов было уже сравнительно невелико, и с каждым новым расшифрованным и прочтенным словом их становилось все меньше и меньше.

Позиционная статистика – оригинальная система дешифровки неизвестных письмен, предложенная советским ученым Ю.В. Кнорозовым, получила всеобщее признание и стала широко использоваться при дешифровке текстов древних народов, письмена которых считались навсегда утерянными. Именно она позволила включить в эту работу «думающие машины», решающие сложнейшие проблемы лингвистики на основе математического анализа.

Теперь непонятные, таинственные знаки неизвестных письмен не кажутся такими недоступными, непокорными. Благодаря титаническому труду Ю.В. Кнорозова мы твердо знаем, что каждый из них должен иметь свойственную только ему вполне определенную частоту (повторяемость) и занимать определенное место в «блоке» – сочетании знаков. Иными словами, знаки имеют свой определенный «паспорт», с вполне точной «пропиской» (позицией в блоке) и частотой (повторяемостью). В иероглифической письменности в соответствии с этим «паспортом» и происходит разделение знаков на корневые, грамматические и фонетические, хотя и возможны случаи, когда один знак может являться владельцем целых двух паспортов.

Настало время подвести некоторые итоги замечательного научного подвига молодого советского ученого.

По-видимому, нет необходимости говорить, какое огромное значение имеет дешифровка и перевод древних текстов для дальнейшего изучения цивилизации майя – самой выдающейся цивилизации до испанской Америки. Уже сам факт доказательства того, что у майя была иероглифическая

письменность, означает, по существу, переворот в науке о майя, а одно лишь прочтение, например, надписей на каменных стелах предоставит ученым, работающим над историей не только древних майя, но и всего Американского континента, совершенно неоценимую документацию.

Однако в этом вопросе есть еще одна очень важная сторона: перевод текстов раз и навсегда положил конец всяким измышлениям расистов о якобы умственной неполноценности аборигенов Америки (к сожалению, подобные «теории» по сей день имеют хождение), поскольку в процессе дешифровки выявились неопровержимые доказательства того, что письмо майя создано местным населением, а не привезено откуда-то извне таинственными «учителями» с востока или запада. Иероглифические знаки, отражающие местную фауну, флору и культуру, убедительней всего подтверждают, что создателями письма, этого величайшего достижения и одновременно проявления человеческого разума, были сами индейцы, а не жители, например, легендарной Атлантиды, как бы заманчиво ни выглядела подобная гипотеза.

Но, работая над дешифровкой письма майя, Ю.В. Кнорозов вышел за рамки локальных проблем. Его исследования внесли существенный вклад в раз работку ряда общих вопросов, связанных в первую очередь с такими науками, как история и лингвистика. Так, в своей монографии «Письменность индейцев майя» (1963 г.) он ясно показал, что иероглифическая система письма появляется не в результате счастливого озарения гения-одиночки, а что это явление стадиальное, свойственное всем древним государствам как Старого, так и Нового Света. Исчезает первобытнообщинный строй, рождаются классы и государство – и как неизбежное следствие этого исторического процесса взамен первобытных рисунков – пиктограмм, появляется письмо, передающее звуковую речь, – иероглифика.

Наконец, Ю.В. Кнорозов разработал и успешно применил оригинальную систему дешифровки неизвестных письмен, названную им позиционной статистикой. Благодаря этому научному открытию появилась возможность исследования и дешифровки практически любого неизвестного письма, ес-

ли, конечно, количества «рабочего материала», т.е. самих текстов, написанных исследуемым письмом, достаточно. Позиционная статистика в отличие от других этимологических методов позволила впервые успешно привлечь к дешифровке электронную счетно-вычислительную технику.

Однако и всего перечисленного оказалось мало. Работа над дешифровкой письменности майя – пусть не удивляется читатель! – отнюдь не являлась для Ю.В. Кнорозова конечной целью его исследований, т.е. самоцелью. Она, эта работа, по существу, была лишь неким «практическим занятием» в его исследованиях в области самых злободневных и острых вопросов сравнительно-исторического языкознания, математической лингвистики и общей теории знаковых систем, функционирующих в человеческом обществе. Эта наука, ее принято также называть «теорией сигнализации», или «семиотикой», рожденная невиданно гигантской вспышкой человеческого разума, бушующей сегодня над нашей землей, столь же актуальна и перспективна, как бионика или выдающиеся достижения в области освоения космоса.

Более того, мы возьмем на себя смелость утверждать, что, например, для успешного освоения космоса и особенно проникновения человека в Галактику нам, землянам, необходимо уже сейчас решать в том числе и основные, принципиальные вопросы теории сигнализации.

«Галактика и лингвистика – что общего между ними?» – возможно, недоверчиво спросит читатель. Но в том-то и дело, что связь между ними есть и носит она отнюдь не эфемерный и даже не теоретический, а чисто практический характер. Вернемся к дешифровке и посмотрим на нее более широким взглядом (с позиции теории сигнализации), и тогда выяснится, что дешифровка исторических систем письма является лишь частной задачей в общей проблеме формальных исследований текстов, которая, в свою очередь, представляется одним из основных путей изучения механизма возникновения осмысленной человеческой речи! Только ли возникновения? По-видимому, этим никак не ограничиваются задачи, стоящие перед новой наукой!

Далее, процесс дешифровки неизвестных письмен, по существу, является обратным процессом, позволяющим восстанавливать ход возникновения письма, графически фиксирующего умственную деятельность челов.. А если так, то именно здесь лежит та тонкая и чрезвычайно сложная «тропинка», открывающая путь к моделированию этой специфической деятельности, Благодаря которой человек стал человеком, т.е. разумным существом. Человек должен создать подобную модель – назовем ее условно «Универсальной системой сигнализации разумных существ», – если он всерьез решил отправиться в Галактику. Он попросту не имеет права уходить в ее бескрайние просторы, не вооружившись тем, что явится предметом первой необходимости при встрече землянина с разумными существами других, пока еще неведомых нам миров. Иначе как он объяснит, что протянутая для рукопожатия рука предлагает другим разумным обитателям вселенной Дружбу и Мир!

Список рекомендуемой литературы

1. Белякова Г.С. Письменность наших предков // Славяне. – М., 1991.
2. Гриневич Г.С. Праславянская письменность. – М., 1993.
3. Древние цивилизации от Египта до Китая // Вестник древней истории. Сб. статей. – М., 1997.
4. Замаровский В. Тайны хеттов. – М., 1968,
5. Истрин В.А. 1100 лет славянской азбуки. – М., 1988.
6. Исчезнувшие народы // под редакцией П.И. Пучкова / Сб. – М., 1988.
7. Керам К. Боги, гробницы, ученые**.** – СПб., 1994.
8. Кузьмищев В. Тайна жрецов майя. – М., 1968.
9. Сусов И.П. Введение в теоретическое языкознание. Тверской гос. Университет. – Тверь 2000.
10. Тайны древних письмен. Проблемы дешифровки / под ред. И.М. Дьякова. Сб. статей. – М., 1976.
11. Флота Я., Новы Л. История естествознания в датах. – М., 1987.

Глава 10.

Тайные операции в криптографии

Предлагаемый читателю цикл очерков, дает начальное представление о специальных методах добывания информации, что во многом связано с историей криптографии.

Особая роль во все исторические периоды отводилась криптографическим методам защиты информации. Проблема защиты информации путем преобразования, исключающего доступ к ней посторонних лиц, волновала человеческий ум с давних времен. Более того, противостояние криптографов и взломщиков шифров всегда являлось двигателем в эволюции методов шифрования, а попытки создания абсолютно стойких шифров сродни попыткам создания вечного двигателя.

Затраты на вскрытие зашифрованных данных, однако, часто превышают стоимость самой информации и тогда прибегают к специальным методам. Необходимость изучения агентурно-оперативных методов работы спецслужб диктуется тем, что нередко затраты, связанные с оперативно-агентурным проникновением в криптографические тайны противника, оказываются значительно меньше затрат на криптографическую разработку методов дешифрования, создания соответствующей техники и др. Кража, подкуп, взлом оказываются «более рентабельными». В этом смысле характерно откровенное высказывание одного из помощников президента США Ричарда Никсона. Он выразил следующую мысль: «Нередко нецелесообразно вкладывать огромные средства в разработку и реализацию «традиционных» методов дешифрования. Один удачный взлом бесплатно решает задачу».

Известный автор шпионских романов о Джеймсе Бонде **Ян Флеминг**, еще будучи офицером английской армии, в 1941 г. высказал простую идею: если шифр трудно вскрыть, его надо выкрасть.

Изложение ведется в сжатом, аннотированном виде, более подробно с заинтересовавшими материалами, читатели могут ознакомиться, обратившись к литературным источникам, указанным в списке литературы.

Данные материалы собирались из опубликованных открытых материалов, систематизировались авторами в течение многих лет совместно с *Ю.И. Гольевым*, *Г.П. Шанкиным*, в связи чем, выражаем им искреннюю признательность.

10.1. Агентурные действия до Первой мировой войны

«Разведчик становится известен миру только тогда,
когда его постигнет крупная неудача».
Л.В. Шебаршин

Русско-германские переговоры. Еще в конце XIX в. объединитель Германии **О. Бисмарк** проявлял особое беспокойство о сохранности секретных посланий, отправляемых из Петербурга. Он писал: «…немецкий шифр не остается неизвестным российскому императорскому двору; ведь я знал по опыту, что даже в здании нашей миссии в Петербурге сохранить наши тайны мог не искусно сделанный замок, а только частая смена шифра. Я был уверен, что не мог телеграфировать в Ливадию ничего, что не дойдет до сведения императора». В Ливадии (Крым) в это время происходили русско-германские переговоры. Бисмарк с сожалением констатировал: «Сохранить тайну шифра в Петербурге особенно трудно».

О. Бисмарк

Сам **Александр II** (император России) не стеснялся в использовании сведений, полученных в результате дешифрования. Он жаловался Бисмарку, что его, императора, резко критикуют немецкие государи в своих шифрованных посланиях в Россию. Чтение шифрпереписки он считал естественным правом государя.

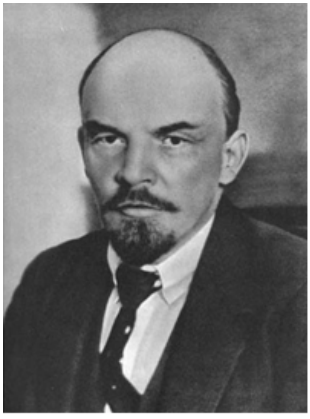
Александр II

Аналогичная мысль о русских дешифровальщиках была высказана немцами уже в конце 30-х гг. XX в. В справке главного управления полиции безопасности отмечалось: «…русские испокон веков являются мастерами шифрования и дешифрования. Уже во время Петра I им удавалось не только доставать шифры всех находящихся в России дипломатических представительств, но и разгадывать их».

РСДРП и Департамент полиции России. Криптографические методы защиты и нападения использовались не только в международной борьбе. Во внутренней политике государств они также играли важную роль.

Характерными в этом отношении являются эпизоды начала XX в., имевшие место в России. Главным органом царского сыска в России в это время являлся **Департамент полиции (ДП)**. Он уделял особое внимание раскрытию шифрованной переписки подпольных революционных организаций, и, в первую очередь, Российской социал-демократической рабочей партии (РСДРП), возглавляемой **В.И. Лениным.**

Важную роль в этой борьбе играли агентурные методы, применявшиеся ДП в отношении революционеров-подпольщиков. В результате внедрения агентов, обысков, арестов и допросов ДП получал значительное количество шифров и ключей к ним. ДП получал шифры и ключи, используемые ЦК РСДРП, а также и другие аналогичные материалы по тайной



В.И. Ленин

переписке между региональными организациями партии. Собственно шифры занимали значительное место в тайной переписке революционеров. Характерна записка, направленная главным специалистом ДП по дешифрованию шифров **И.А. Зыбиным** начальнику саратовского губернского жандармского управления: «…Отобранные по обыску у мещанина Николая Сергеевича Кузнецова записки зашифрованы 4, 15, 25, 29 и 35-ой страницами какой-то неизвестной книги и разбору не поддаются по недостаточности материала. Прошу Ваше Высокоблагородие уведомить в самое непродолжительное время, не было ли обнаружено по обыску у названного Кузнецова, кроме означенных записей, какого-либо издания или легальной книги с пометками на отдельных страницах или загрязненных более других какой-либо страницей от частого, сравнительно с другими, употребления и, кроме того, не встретилось ли одно и то же издание у прочих лиц, принадлежащих к одной с Кузнецовым организации, так как подобное явление в большинстве случаев указывает, что таковое издание служит ключом для шифрованных сообщений» [Спиридонович, 1991]. В данном случае речь идет о так называемом «книжном шифре». Он достаточно прост в использовании. Абоненты (отправитель и получатель) договариваются об этом шифре и ключе к нему. Ключом является заранее оговоренная книга, идентичные варианты которой должны находиться у каждого абонента. Буквы секретного послания приобретают вид координат букв в книге, которые совпадают с секретной буквой. Так, например, если первая буква секретного послания буква «А», то она может приобрести следующий вид: 128.15/32. Это означает, что букву следует искать на 128-й странице книги, в 15-й строке которой на 32-м месте и находится нужная буква.

Этот шифр обладает хорошей криптографической стойкостью и используется практически до наших дней. Одним из недостатков этой системы шифрования является тот факт, что используемая книга может храниться у любого из абонентов. Обнаружение этой книги «раскалывает» всю систему защиты, о чем и пишет И.А. Зыбин.

Н.К. Крупская

Заметим, что главный криптограф «охранки» Иван Зыбин был настоящим гением в своем деле. По свидетельству современников: «Он был фанатиком, если не сказать маньяком, своей работы. Простые шифры он разгадывал с одного взгляда, а вот запутанные приводили его в состояние, близкое к трансу, из которого он не выходил, не решив задачу».

В результате указанных действий ДП дешифровал большое количество документов, в том числе и часть писем **В.И. Ленина,** а также Я. Свердлова, В. Куйбышева, Г. Пятакова и др.

В октябре 1905 г. полиция произвела обыск в редакции газеты «Новая Жизнь», с которой сотрудничал В.И. Ленин. Во время обыска полиция обнаружила записную книжку, которая, по-видимому, принадлежала жене Ленина **Н.К. Крупской**, руководившей организацией секретной связи РСДРП. В этой книжке, в частности, содержались шифры и ключи к ним, которые использовались революционерами в шестидесяти трех городах России. Эти сведения позволили полиции провести массовые аресты членов РСДРП по всей стране.

Продажа посольских шифров Великобритании в России. В июне 1904 г., посол Великобритании в России, **Ч. Хардинг** докладывал в британский МИД о том, что он перенёс «чрезвычайно огорчивший его удар», обнаружив, что начальник его канцелярии продал, за огромную по тем временам

сумму в 1000 фунтов за копию одного из дипломатических шифров. Три месяца спустя Хардинг узнал, что в МВД России был создан специальный секретный отдел «с целью получения доступа к иностранным миссиям в Санкт-Петербурге». Принятые Великобританией меры безопасности к успеху не привели. Секретарь английского посольства С. Райс докладывал в феврале 1906 г.: «Вот уже в течение некоторого времени из посольства исчезают бумаги... Курьер и другие лица, связанные по работе с посольством, находятся на содержании полицейского департамента и, кроме того, получают вознаграждение за доставку бумаг». Подобные случаи происходили и в посольствах Соединённых Штатов, Швеции и Бельгии.

Дешифровальщик России – Эрнст Феттерлейн *(Ernest Constantine Fetterlein)*.

До революции 1917 г. одним из ведущих дешифровальщиков в России был **Эрнст Феттерлейн**. Среди многих его заслуг было дешифрование британской дипломатической почты.

Стоит отметить, что Николай II очень ценил Эрнста Феттерлейна. Даже подарил ему перстень с огромным бриллиантом. Вероятно, Феттерлейн разрабатывал для него и Александры Федоровны специальный шифр для обмена особо секретной информацией.

Первые контакты с английской разведкой Эрнст Феттерлейн вероятно, установил в 1909 г., когда он вместе с Николаем II был в Англии. Возможно, тогда его и завербовала английская разведка. Ничего удивительно в том, что после свержения Николая II он благополучно эмигрировал в Англию и занял ведущее место в одном из подразделений английской разведки GC&CS.

Благодаря Феттерлейну англичане дешифровали значительную часть дипломатической переписки русских во время англо-советских торговых переговоров. Это была чрезвычайно важная информация. Так в самом начале переговоров (июнь 1920 г.) В.И. Ленин писал главе русской делегации Л.Б. Краси-

ну: «Эта свинья Ллойд Джорж (премьер-министр Великобритании – авт.) пойдёт на обман без тени сомнения или стыда. Не верьте ни единому его слову и в три раза больше дурачьте его». Понятно, как к этим словам отнеслись англичане, однако истинный источник информации они, естественно, не могли назвать. Лишь позднее (в августе) кабинет министров дал разрешение на публикацию части дешифрованных документов (восемь телеграмм). Однако и здесь прибегли к уловке. Англичане сообщили, что документы получены агентурным путём. Но этому даже в Англии не поверили. Тем не менее, советские дипломатические шифры были заменены очень поздно, лишь в начале 1921 г. Но уже в апреле этого же года англичане совместно с Феттерлейном дешифровали и их. Позднее, летом 1923 г. были введены новые шифры, но уже через год англичане дешифровали и их.

Российская разведка 1904–1906 гг. В 1904 г. накануне русско-японской войны агент русской разведки **Иван Федорович Манасевич-Мануйлов** сумел раздобыть экземпляр шифра японского посольства в Гааге. Благодаря этому успеху русские получили возможность читать всю перехватываемую дипломатическую переписку Японии. Однако вскоре японцы заподозрили неладное и заменили шифр. Историческая объективность требует упоминания о следующем факте. В некоторых исследованиях (см., например, «Очерки истории российской внешней разведки», т. 1 , под ред. Е.М. Примакова, М., 1999) заслуга Манасевича-Мануйлова ставилась под сомнение. В частности, отмечалось следующее: «Среди закордонных представителей царских спецслужб было немало лиц сомнительного толка – авантюристов, состоящих на агентурной службе отдельных российских ведомств. В этом отношении характерно дело некоего Манасевича-Мануйлова. Манасевич-Мануйлов считался в полиции личностью весьма нечистоплотной, «человеком удивительно покладистой совести», способным на мошенничество, подлог и финансовые спекуляции. В 1905 г. он буквально заваливает своих шефов огромным количеством документов, ока-

И.Ф. Манасевич-Мануйлов

завшихся склеенными обрывками бумаг на японском языке. Последней точкой в его карьере стали присланные им из Парижа фотокопии страниц китайского словаря, означенные в описи как секретные документы» [Очерки, 1999].

Другие источники указывают на эффективность разведывательной деятельности Манасевича-Мануйлова, отмечая при этом, что за свою работу он был награждён орденом Святого Владимира.

А вот какую характеристику дает Манасевичу-Мануйлову посол Франции в России в годы Первой мировой войны Морис Палеолог: «Мануйлов – субъект интересный. Он еврей по происхождению; ум у него быстрый и изворотливый; он был любителем широко пожить, жуир (весело и беззаботно живущий человек – авт.) и ценитель художественных вещей; совести у него ни следа. Он в одно время и шпион, и сыщик, и пройдоха, и жулик, и шулер, и подделыватель, и развратник … А вообще, милейший человек … У этого прирожденного пирата есть страсть к приключениям и нет недостатка в мужестве».

Биография Манасевича-Мануйлова – настоящий авантюрный роман. С 1900 г. он исполнял обязанности агента по римско-католическим делам в Риме. С 1902 г. служил в Париже; получил должность чиновника особых поручений VIII класса при министре внутренних дел. В 1904–1905 гг. занимался контрразведывательной деятельностью против Японии. В июле 1904 г. по приказу директора ДП А.А. Лопухина Манасевич-Мануйлов организовал и возглавил отделение по розыску о международном шпионстве (в составе особого отдела ДП), в задачи которого входило, кроме наблюдения за ино-

странными шпионами, добыча шифров иностранных государств. Это отделение, не имевшее определенного штатного расписания и каких-либо письменных инструкций, было временным образованием, в которое кроме самого Мануйлова был включен жандармский ротмистр М.С. Комиссаров, дешифровальщик В. И. Кривош, отряд филеров, а также завербованная Мануйловым «внутренняя агентура», в основном из обслуживающего персонала зарубежных посольств в Петербурге. В соответствии с его названием, мануйловское отделение интересовали не только и не столько японцы, сколько вообще все иностранцы, чье поведение и связи вызывали подозрения. В июле-августе 1904 г. отделение установило наблюдение и контроль за перепиской шведско-норвежского морского атташе Г.Ф. Краака, итальянского военного агента графа Л. Руджери, ряда американцев и англичан. Результаты не заставили себя ждать. Наблюдение за Крааком, например, обнаружило его частые встречи с американцем Х. Бергом, который по заданию морского министерства России заведовал постройкой подводной лодки на Балтийском судостроительном заводе. Перлюстрация же донесений шведского морского агента показала, что ему известны некоторые секретные сведения, источником которых является Берг. В результате правительство отказалось от услуг американца, которому не помогли и его особо доверительные отношения с великим князем Александром Михайловичем, ведавшим вооружением вспомогательных судов флота. Отделение быстро развернуло свою работу, и уже во второй половине августа Мануйлов представил в департамент добытый агентурным путем шифр американского посольства, а в начале сентября – китайский. Позднее были добыты шведский, болгарский, румынский шифры и часть японского дипломатического шифра. В октябре 1904 г. было получено еще четыре китайских шифра, а также фотокопия книги посольских донесений. В результате появилась возможность контролировать всю переписку китайской миссии. Если же учесть, что через Петербург шли депеши МИД Китая к его представителям в странах Западной Европы, можно

утверждать, что перехватывалась и большая часть корреспонденции китайского внешнеполитического ведомства.

Во время русско-японской войны Манасевич-Мануйлов занимался за границей разведкой и внешней контрразведкой. Его заслуги были оценены в Петербурге, директор ДП А.А. Лопухин докладывал 3 августа 1904 г.: «При открытии военных действий на Дальнем Востоке Департамент полиции при посредстве чиновника особых поручений при министре внутренних дел Мануйлова стал пытаться организовать правильное наблюдение за представителями японского правительства в западноевропейских государствах, и уже в феврале месяце благодаря полному содействию начальника французской секретной полиции Кавара и начальника Разведочного бюро при Министерстве внутренних дел Моро удалось получить копии всех телеграмм японской миссии в Париже, а также, ввиду существующей во французском Бюро секретной агентуры в японской миссии, г-н Мануйлов регулярно стал получать значительное количество документов из парижской миссии. Затем, по предположению французской полиции, г-н Мануйлов расширил свою деятельность и установил правильное наблюдение при посредстве домашней прислуги в японских миссиях в Лондоне и Гааге» [Абрамов, 2005].

В октябре 1904 г. Манасевич-Мануйлов был вновь командирован в Париж с заданием «организовать разведочное бюро в Вене и Париже по наблюдению за действиями японцев» и по разработке грузинского революционера-эмигранта Г.Г. Деканози, подозреваемого в шпионаже в пользу Японии. Русским военным атташе во Франции, Италии и Австрии предписывалось оказывать ему «возможное содействие и помощь». По мнению современного исследователя, «речь, таким образом, шла о развертывании самостоятельного агентурного наблюдения за японскими дипломатами в Западной Европе, что, однако, не означало прекращения сотрудничества Департамента полиции с французскими специальными службами. Необходимость учреждения новой агентуры была вызвана еще и тем обстоятельством, что действовавшая в Западной Европе заграничная агентура Департамента полиции многие

годы наблюдала за русской революционной эмиграцией, и осуществление «военных разведок», по признанию ее заведующего, было для него делом совершенно «необычным»... Выбор Мануйлова для этой цели объяснялся его опытом работы во Франции, а главное – успехами возглавлявшегося им Отделения по розыску о международном шпионстве. Уже в сентябре 1904 г. он... был неофициально признан «заведующим японскими делами» Департамента» [Абрамов, 2005].

В Париже Манасевич-Мануйлов (при содействии дружественных французских спецслужб, предоставивших ему возможность использовать своих агентов, ранее завербованных в японских миссиях, а также с помощью привлеченных им самим к сотрудничеству новых источников информации) смог получить доступ к переписке послов Японии во Франции, Англии и Голландии с министром иностранных дел, донесениям в Токио военных и морских атташе из Парижа и Берлина, документам японских консульств в Амстердаме и Марселе. К лету 1905 г. «агентура» Мануйлова, состоявшая из десятка французов, давала информацию о шведской, сербской, китайской и английской миссиях в Париже, румынском и китайском посольствах в Лондоне, японской и английской миссиях в Брюсселе, германской – в Мадриде и японской в Гааге. Кроме того, выполнялись разовые поручения департамента и продолжались тесные контакты с французской секретной полицией, по-прежнему снабжавшей Мануйлова копиями телеграмм японских дипломатов.

Во время премьерства С.Ю. Витте Манасевич-Мануйлов состоял в его распоряжении. 1 сентября 1906 г. Манасевич был уволен от службы. В годы Первой мировой войны входил в ближайшее окружение Г.Е. Распутина. После назначения Б.В. Штюрмера премьером с 24 января 1916 г. причислен к Министерству внутренних дел и откомандирован в его распоряжение. В августе 1916 г. арестован по обвинению в шантаже, в связи с чем, задним числом уволен от службы. Несмотря на безуспешные попытки покровителей Манасевича-Мануйлова, включая и императрицу Александру Федоровну, прекратить

М.С. Комиссаров

дело, в феврале 1917 г. приговорен к 1,5 годам заключения. После Октябрьской революции арестован при попытке бежать в Финляндию и расстрелян [Глинка, 2005].

И еще одна характеристика: «Журналист по профессии, авантюрист по призванию… Манасевич-Мануйлов переживал неправдоподобные приключения, совершал фантастические аферы, со сказочной быстротой разорялся и богател и был снедаем только одной страстью – к наживе» (В.Д. Бонч-Бруевич).

Сослуживец Мануйлова ротмистр **Комиссаров Михаил Степанович** также занимался добыванием посольских шифров, и небезуспешно. Так, отвечая на вопросы Чрезвычайной следственной комиссии Временного правительства, он отметил: «В распоряжении контрразведчиков оказалось 12 шифров – американский, китайский, бельгийский и др. … Китайский шифр, представлял собой 6 томов, американский – очень толстую книгу … Все иностранные сношения контролировались» [Мерзляков, 2002].

Летом и осенью 1904 г. вместе с Комиссаровым, специально откомандированным в ДП из Петербургского охранного отделения жандармским офицером-розыскником, Мануйлову довелось ставить на «широкую ногу» работу по борьбе со шпионажем.

Комиссаров был на 1 год младше Мануйлова. После окончания Полоцкого кадетского корпуса и 3-го Александровского военного училища он 14 лет прослужил в 1-м артиллерийском мортирном полку русской армии. С начала 1904 г. в Отдельном корпусе жандармов, а в августе 1904 г. он был откомандирован на Фонтанку, 16 и стал отвечать за проведение операций контрразведки ДП. Наряду с представительной внешностью и знанием иностранных языков, он обладал от-

личными организаторскими способностями и гибким умом математика-шахматиста.

«Совершенно секретное отделение дипломатической агентуры» ДП создавалось в глубокой тайне. От его сотрудников требовалось строжайшая конспирация. Наряду с организацией чисто контрразведывательного наблюдения за деятельностью дипломатов и военных агентов, аккредитованных в России, перед людьми Комиссарова ставилась задача добывания посольских шифров. Их дешифровка позволяла контролировать сношения руководителей дипломатических миссий со своими правительствами и министрами. Любая оплошность, непродуманность действий грозили международным скандалом.

Около 2-х лет Комиссаров жил на нелегальном положении на частной квартире под видом иностранца, и работавшие на него служащие иностранных посольств не предполагали, что продают секреты представителю русского правительства. Бумаги, документы и шифры доставлялись ему на квартиру, где по ночам перефотографировалась, а затем направлялись в ДП. Хранить документы на своей квартире Комиссарову было строжайше запрещено, поэтому приходилось работать быстро и без ошибок – плохо переснятая или пропущенная страница могли сорвать процесс дешифрования. Знание русскими позиций сторон, в том числе американцев, дало многое в период переговоров в Портсмуте летом 1905 г., где шел нелегкий дипломатический поединок С.Ю.Витте с японским представителем Дзютаро Комурой. В успехе миссии С.Ю. Витте была большая часть труда сотрудников разведки и контрразведки. По линии МВД императору ежедневно посылались один-два «всеподданнейших доклада» на основании контролируемой переписки.

В 1906 г. российская разведка проникла в британское посольство в Петербурге. Были скопированы шифры и ключи к ним. Англичане догадывались об утечке информации, но так и не смогли принять эффективных мер защиты, поскольку русская разведка имела своих агентов в посольстве, которые «блокировали» расследование.

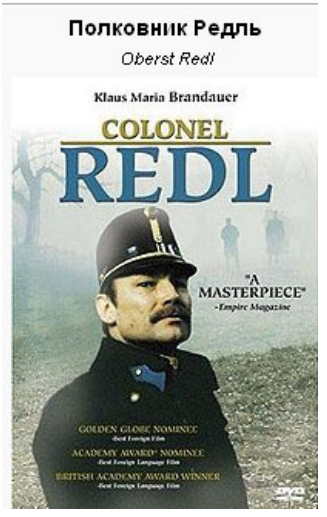
Альфред Редль

Летом 1906 г. англичанам стало известно о существования спецподразделения ДП. «Кто-то, видимо, нас продал, – вспоминал Комиссаров, – потому что наш посол в Лондоне – получил запрос о том, что в Петрограде работает бюро, которое контролирует и хозяйничает во всех посольствах. Между прочим, называли и мою фамилию. В силу этого бюро было раскассировано... Большая часть архива была уничтожена, как секретная» [Мерзляков, 2002].

Российская разведка накануне Первой мировой войны. Накануне Первой мировой войны русские разведчики завербовали высокопоставленного сотрудника австрийской разведки, полковника **Альфреда Редля**. При этом они эффективно использовали информацию о его гомосексуальной ориентации. Редль выдал русской разведке имена австрийских шпионов в России, а также коды и шифры австро-венгерской армии. Российская разведка щедро оплатила работу Редля. За свою информацию он получил более 60000 долл. США (весьма значительная по тем временам сумма). Накануне разоблачения Редль покончил жизнь самоубийством. В предсмертной записке он написал: «Меня погубили легкомыслие и страсть. Помолитесь за меня. За свои грехи я расплатился жизнью. Альфред». Один из руководителей австрийской контрразведки, оценивая последствия деятельности Редля, писал: «Этот проклятый Редль! Он выдал абсолютно всех австрийских шпионов в России, передал в руки противника наши секреты и воспрепятствовал тому, чтобы к нам оттуда просочились нужные сведения...» [Полнар, 1999].

Заметим, что авантюрная биография Альфреда Редля вдохновляла драматургов и кинематографистов. Вольная трактовка биографии Редля (роль которого в фильме исполняет Клаус Мария Брандауэр) основанная на пьесе Джона Осборна

«A Patriot for Me» – это история постепенного избавления от иллюзий, начавшаяся с осознания коррупции и распущенности в армии и закончившаяся болезненным пониманием скорого краха и развала многонациональной полуфеодальной империи, сотрясаемой внутренними и внешними противоречиями.



Афиша фильма «Полковник Редль»

Австрийская разведка перед Первой мировой войной. Перед Первой мировой войной австрийцев интересовала шифрованная переписка иностранных государств. В частности, они предпринимали попытки дешифровать итальянский код. Им удалось перехватить шифрованную переписку послов Италии в Риме и Константинополе. Итальянцы применяли не очень сложный код, но полностью раскрыть его по материалам перехвата австрийцы не смогли, и предприняли следующий шаг. Они поместили в одной из газет, издаваемой в Константинополе на итальянском языке, любопытное сообщение со сведениями военного характера. Расчёт был прост. По предположению австрийцев, итальянский военный атташе в Турции дословно закодирует эту статью и отправит её в Рим. Так и произошло.

Имея шифрованный текст и открытый текст к нему, австрийцы легко довели задачу дешифрования других шифрованных депеш до успешного конца.

Немецкий агент Мюллер. В начале 1914 г. англичане успешно использовали арест международного шпиона, работавшего в основном на Германию, **Мюллера**. При обыске у Мюллера был обнаружен секретный код. Этот код англичане использовали не только для дешифрования, но и для дезинформации противника. Мюллер, как германский шпион, был расстрелян.

Немецкий агент Луи Марэна. Перед Первой мировой войной начальником шифровального отдела министерства ВМФ Франции стал агент Германии профессор Луи Марэна. Он передал немцам весьма важные сведения, которыми противник Франции впоследствии весьма эффективно воспользовался.

Приведенный перечень агентурных действий далеко не полон, поскольку, во-первых, в нем отражены лишь те события, которые стали достоянием гласности и, во-вторых, лишь часть этих событий. По многим из изложенных событий могут быть написаны (и уже написаны) отдельные книги, сняты фильмы.

10.2. Агентурные действия в Первую мировую войну

«Все мы только пылинки в ужасном урагане, несущемся над миром, и он кидает нас навстречу неизвестно чему – падению или воскресению».
Граф фон Чернин

Конфликт между Австро-Венгрией и Сербией из-за убийства в Сараево сербским террористом 28 июня 1914 г. эрцгерцога Франца Фердинанда и его супруги вышел за локально-региональные рамки вследствие вмешательства России, что вызвало цепную реакцию интервенций – Германии, Франции, Англии и других стран. Так начиналось первое в истории человечества всеобщее побоище, получившее название Первой мировой войны.

В начале войны Румыния сохраняла нейтралитет, симпатизируя странам Антанты, к которым впоследствии присоединилась. В Бухаресте находились посольства враждующих стран и активно работали их разведки. В октябре 1914 г. у посланника Австро-Венгрии в Бухаресте графа фон Чернина был похищен портфель, в котором, среди прочих документов, был дипломатический шифр. Портфель с документами вскоре был возвращён, и император Франц Иосиф отказался принять заявление

Чернин граф Оттокар фон и цу Чудениц

Чернина об отставке. Впоследствии выяснилось, что шифрдокументы были сфотографированы, и румыны начали регулярно дешифровать дипломатические послания Австро-Венгрии. Вот как Чернин описывает этот инцидент в своих мемуарах.

«Шпионаж и контршпионаж, конечно, процветал за эту войну. В Румынии им особенно упорно занимались русские.

В октябре 1914 г. разыгрался весьма печальный для меня инцидент. Я ехал в автомобиле из Бухареста в Синайю и моя васиза (среднее между папкой и портфелем – *авт*.), полная документов политического значения, не была, по ошибке моего слуги, положена внутри автомобиля, а привязана сзади. По дороге она была отрезана и украдена. Я немедленно приложил все старания вернуть ее, но это удалось мне только спустя приблизительно три недели и стоило больших денег. Ее нашли в амбаре одного крестьянина и из нее, по-видимому, не пропало ничего, кроме папирос.

Но после занятия Бухареста нашими войсками, в квартире Братиану были найдены копии и фотографические снимки всех моих бумаг. Сейчас же после утери васизы, я предложил уйти в отставку, но император отклонил мою просьбу» [Чернин, 1923].

В 1914 г. немцы продемонстрировали возможность использования криптографии в циничных (с точки зрения морали) целях. Они провели операцию, суть которой заключалась в следующем. В шпионской сети Германии работал голландец Хугнагел. Работа его во Франции оказалась малоэффективной. Немцы решили «подставить» Хугнагела французской контрразведке для отвлечения ее сил и средств от своих основных агентов. Для достижения этой цели был использован простой прием. Немцы знали, что французы вскрыли один из их сек-

Адмирал Эссен командующий Балтийским флотом в 1914 году

ретных кодов. Именно этим кодом они снабдили Хугнагела. В результате Хугнагел был арестован, а основные агенты Германии получили возможность бежать из Франции.

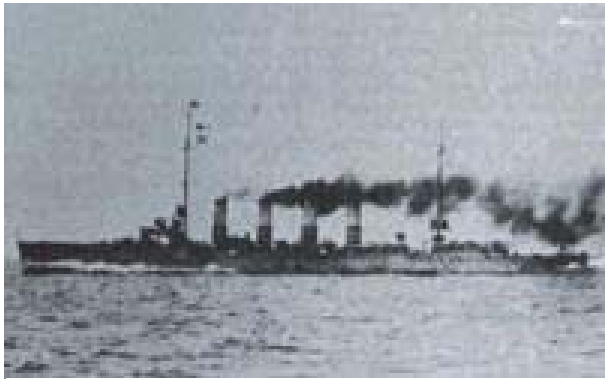
Одним из самых загадочных эпизодов Первой мировой войны стала гибель в Финском заливе германского крейсера «Магдебург». В августе 1914 г. легкий немецкий **крейсер «Магдебург»** налетел на мель в восточной части Балтийского моря у острова Оденсхольм. Русские моряки сумели достать с этого крейсера кодовые книги ВМС Германии.

Этот эпизод подробно описан в многочисленных мемуарах, вот один из примеров.

«27 августа 1914 г. в кабинет командующего Балтийским флотом адмирала Н.Эссена буквально ворвался начальник разведки контр-адмирал А. Непенин.

– У меня очень важное сообщение, Николай Оттович, – начал он свой доклад. – Сегодня ночью на камни возле острова Оденсхольм наскочил немецкий крейсер «Магдебург». В это время в море, на оборонительной позиции Ревель – Гельсингфорс, находились наши крейсера «Новик», «Паллада» и «Богатырь». Они заметили крушение и попытались взять германца в плен. При подходе наших кораблей сопровождавший «Магдебург» миноносец развернулся и ушел полным ходом. Попытка обстрелять его к успеху не привела. Увидев наши корабли, немцы спешно подорвали свой крейсер, и он затонул на средней глубине. На остров удалось выбраться только 89-ти членам команды, остальные 100 погибли.

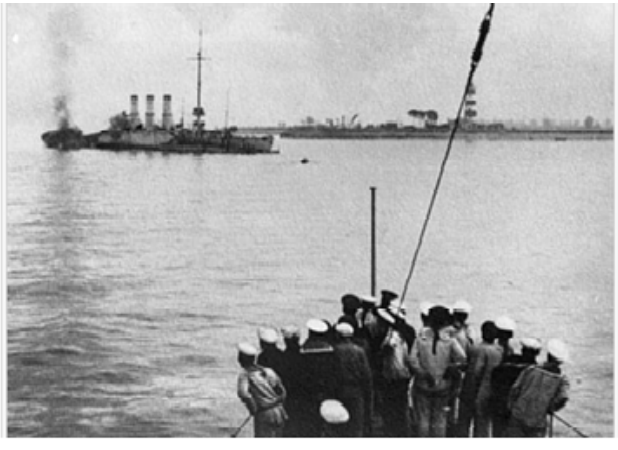
– А что с капитаном немецкого крейсера? – спросил Эссен.



Крейсер «Магдебург»

– Фон Хабенихт жив, но находится в очень плохом состоянии, без сознания – ответил Непенин…

– Что нужно немцам в этом районе? – задумчиво произнес контр-адмирал. – Это же совершенно дикие места. Скорее всего, они хотели прорваться к Петрограду и обходили дальним краем наши минные поля. В темноте сбились с курса и наскочили на каменную гряду. Надо допросить членов команды…» [Габис, 1991].



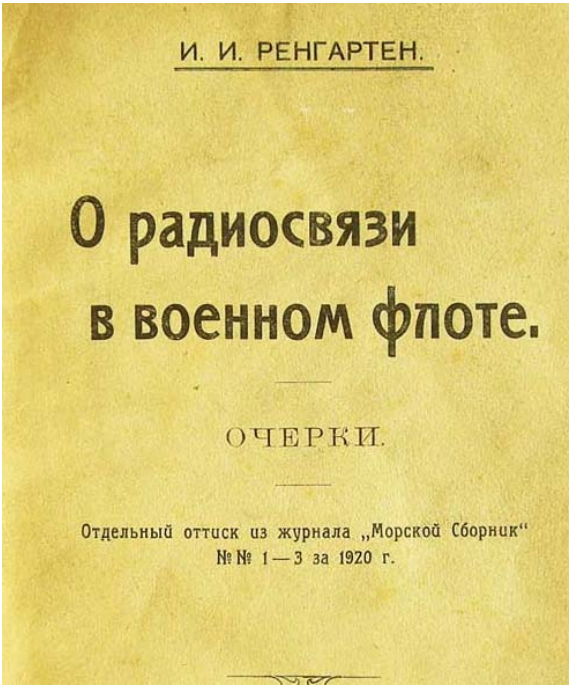
Севший на мель крейсер «Магдебург»

Допрос пленных германских моряков дал немного. Они показали, что действительно шли в северо-восточный сектор Финского залива. На рифы сели по вине радистов, задержавшихся с расшифровкой депеши. В ночной темноте крейсер продолжал идти опасным курсом и наскочил на камни. Но дальше произошло непонятное. Увидев русские корабли, командир «Магдебурга» **Густав Генрих Хабенихт** приказал взорвать крейсер. На предложение команды сохранить корабль, поднять белый флаг и сдаться в плен, что разрешено военно-морским уставом, он не отреагировал. В результате 2/3 команды погибли, а сам командир был тяжело ранен. О конечной цели рейда ни рядовые матросы, ни офицеры «Магдебурга» ничего не знали. Стало ясно, что рассказать о загадочной миссии германского крейсера может только его командир. Понимая, что немецкая агентура в Петрограде попытается убрать Хабенихта, были приняты особые меры предосторожности. Немецкого капитана на миноносце по Неве отвезли в Шлиссельбург и содержали под надежной охраной. Однако через несколько дней командир германского крейсера Густав Генрих фон Хабенихт, не приходя в сознание, скончался в тюремном госпитале.

И.И. Ренгартен

Для того, чтобы скрыть факт захвата кодовых книг с «Магдебурга» от немцев, русские провели следующую операцию. Под видом командира «Магдебурга» в Шлиссельбурге под охраной жил офицер русского флота **Иван Иванович Ренгартен**, исполнявший в то время должность второго флагманского минного офицера (радиотелеграфный офицер – *авт.*) при штабе командующего Балтфлотом. Он свободно говорил по-немецки и был внешне похож на Хабенихта. Как и рас-

считывало русское командование Балтфлота, один из многочисленных немецких агентов узнал о месте нахождения «Хабенихта», и немцы сумели выйти с ним на связь. Это было сделано с помощью немецких газет, которые мнимый командир «Магдебурга» заказывал в шведском посольстве (русские, естественно, любезно предоставили ему такую возможность и при этом сообщили шведам, для кого предназначена пресса). Над буквами одной из статей Ренгартен обнаружил еле видные точки, помеченные буквы складывались в следующий текст: «Где книги? Если уничтожили их сообщите так: если утопили, попросите журнал «Иллюстрированные новости», если сожгли, то «Шахматный журнал Кагана» – номер, соответствующий номеру котла на «Магдебурге».


И. И. РЕНГАРТЕН.

О радиосвязи в военном флоте.

ОЧЕРКИ.

Отдельный оттиск из журнала „Морской Сборник“
№№ 1—3 за 1920 г.

Очерки И.И. Ренгартена

Ренгартен заказал «Шахматный журнал Кагана» №14. Именно в этом котле крейсера были сожжены фальшивые кодовые книги и подлинные обложки в свинцовом переплете. На следующий день после получения немцами этой информации к «Магдебургу» подошла подводная лодка и, высадившаяся на крейсер группа, извлекла пепел от «сгоревших кодовых книг», остатки переплета и куски кожи от обложек.

Естественно, русскому флоту была дана команда: не мешать проведению этой операции. Так немцы убедились в том, что кодовые книги с «Магдебурга» уничтожены.

Еще одна трактовка инцидента с крейсером «Магдебург» приводится в статье М.Ю.Ежова. «По воспоминаниям старшего лейтенанта И.И. Ренгартена, 29 августа водолазом был обнаружен утопленник, который крепко держал в руках сигнальную книгу …. Именно этот экземпляр был передан союзникам (англичанам и французам) вместе с другими документами. В Службе связи и в штабе командующего Балтийским флотом началась работа по вскрытию военно-морского германского шифра. К середине октября 1914 г. усилиями старшего лейтенанта Ренгартена и его помощников была налажена дешифровка составленных по сигнальной книге радиограмм» [Ежов, 2007].

В начале 1915 г. в составе службы связи Балтийского флота была организована отдельная радиостанция особого назначения (РОН), которая занималась радиоперехватом и дешифровкой полученной информации.

Захваченными на «Магдебурге» кодовыми книгами русские поделились со своими союзниками – англичанами. Эта информация легла в основу основных успехов английской дешифровальной службы во время Первой мировой войны, англичане практически всю войну читали радиограммы немецких военных моряков надводного флота. Их расшифровкой и чтением занималось специальное подразделение британской военно-морской разведки, руководимой сэром **Реджинальдом Холлом**, так называемая «Комната 40», где работали лучшие криптоаналитики. Благодаря успехам этого

подразделения (и подарку русских) Королевский военно-морской флот, в частности, смог нанести впечатляющее поражение немцам в Ютландском морском сражении в конце мая 1916 г.

Позднее Дэвид Кан, известный американский журналист и специалист по истории криптологии, автор книги «Взломщики кодов» [Кан, 2000], охарактеризует эпизод с захватом документов на «Магдебурге» как, возможно, самую счастливую удачу во всей истории криптоанализа.

Итак, англичане успешно дешифровали шифрсообщения ВМС Германии. Однако с дешифрованием дипломатического кода дело обстояло сложнее, несмотря на все усилия сотрудников «Комнаты 40» открыть его тайну не удавалось. К добыче немецких дипломатических шифров было решено активно подключить агентуру. Эта операция англичан подробно описана в книге И.А. Дамаскина «Сто великих разведчиков» (гл. **Александр Цек**).

«В самом начале оккупации Бельгии в богатый дом в центре Брюсселя вселился офицер немецкой комендатуры. Хозяином дома был очень зажиточный австрийский предприниматель, чех по национальности, по фамилии Цек, который жил там вместе с сыном Александром и женой – англичанкой. Она, правда, в это время находилась в Англии, где её застала война, и как подданная враждебного государства (Австро-Венгрии) была интернирована.

Как-то раз Александр постучал в дверь комнаты офицера, попросил разрешения войти и сказал, что хочет сообщить об одном важном деле. Оно заключалось в следующем: занимаясь опытами с беспроволочным телеграфом, он сконструировал особый приёмник, который установил на чердаке дома. Поэтому он просит офицера немедленно проинформировать комендатуру, чтобы его не заподозрили в шпионской деятельности…

Военные власти и контрразведка подвергли всю семью Александра Цека негласной проверке. Выяснилось, что его отец, очень богатый австрийский фабрикант, принадлежал к

высшим кругам австрийского общества, был даже принят при императорском дворе. Будучи чехом, он оставался ярым австро-венгерским патриотом и в политическом отношении был безупречен. Благоприятные отзывы были получены и о матери Александра, которая вполне сжилась со своей новой родиной и слыла «доброй австриячкой» …

Александра приняли на службу и зачислили на скромную должность штатского чиновника центральной радиостанции гражданского управления Бельгии. Поначалу он занимался сборкой аппаратов для радиотелеграфа, проявил усердие и недюжинные способности техника и вскоре заслужил полное доверие своего начальства. Его назначили на один из самых ответственных постов приёмщика радиограмм, получаемых германскими властями в Бельгии, как из Берлина, так и от различных военных штабов с театра военных действий. Это была совершенно секретная работа.

Тайный код, который использовался при посылке особо важных правительственных депеш, был лишь у важнейших должностных лиц германского правительства и подчинённых ему организаций. Книги, содержащие коды, находились лишь у командующих армиями, генерал-губернаторов завоёванных территорий и у германских послов в иностранных государствах.

Германский телеграфный ключ был выработан ещё в предвоенные годы. Он состоял из двух книг. В «толстой» буквы алфавита, а также некоторые слова обозначались условными цифровыми знаками. Но этой книгой нельзя было пользоваться без второй, «тонкой». В ней было указано, в какой день г. каким ключом пользоваться, так как цифры первой книги ежедневно меняли своё значение. Кроме того, в различные дни г. ключи «толстой» книги приходилось особым образом сочетать с определёнными цифрами «тонкой». Немецкий код принадлежал к разряду тех, расшифровать которые практически невозможно.

Александр Цек стал одним из тех немногих, кто в изолированном и строго охраняемом помещении днём и ночью был занят расшифровкой тайных правительственных телеграмм,

адресованных генерал-губернатору оккупированной Бельгии Морицу фон Биссингу.

Цека вербовали медицинская сестра Эдит Кавель и её правая рука, издатель-подпольщик Филипп Бокк. В обмен на секретные коды ему предложили безопасность горячо любимой матери и возможность переехать в Англию после удачного завершения операции. Вручили письмо от матери. Цек внимательно выслушал агентов, прочёл письмо, в котором мать просила со вниманием отнестись к тому, что ему скажут её друзья. К этому времени он уже разочаровался в немецких союзниках Австро-Венгрии, в кайзере Вильгельме. Предложение Кавель и Бокка пришлось ему по душе, к тому же добавилось беспокойство за мать. Он дал согласие….» [Дамаскин, 2002].

Александру Цеку было предложено по ночам во время дежурства дословно скопировать ключи «толстой» и «тонкой» книг, что представляло собой титанический труд. Вторая часть задания заключалась в доставке копии книг в Голландию, что и было проделано в августе 1915 г. Копии книг попали в руки майора Оппенгейма, шефа английской разведки в Роттердаме, а от него – Реджинальду Холлу. С этого дня, задолго до вступления Америки в войну, союзники получили возможность расшифровывать секретные радиограммы немецкого правительства.

Сам же Александр Цек пересёк границу и… исчез. Никто никогда его больше не видел. Даже неизвестно, как документы попали в руки английского резидента. Цек словно в воду канул, и никаких следов его гибели или его существования не было обнаружено, что, впрочем, и не удивительно. Если бы молодого человека оставили в живых, он во время войны мог бы сознаться в том, что выдал код англичанам. Другое дело, если бы от него удалось навсегда отделаться.

Зачастую историки называют Александра Цека человеком, решившим исход Первой мировой войны. Вот описание одного из эпизодов, указывающих на справедливость этого утверждения.

«17 января 1917 г. в «Комнату 40» поступила перехваченная телеграмма. Она, как и большинство других, проходила

Артур Циммерман

через американскую фирму связи «Вестерн юнион» и была «пиратским» способом получена англичанами.

Ею занялись дешифровальщики секции А (дипломатический перехват) Найджел ди Грей и Уильям Монтгомери. Уже просмотр первых групп цифр показал, что они содержат набор цифр варианта 13040, ключевого числа немецкого дипломатического кода. Вскоре прочли и подпись под телеграммой (97556). Это был не кто иной, как **Артур Циммерман**, статс-секретарь немецкого министерства иностранных дел. А телеграмма предназначалась германскому шефу в Мексике фон Экардту:

«Справочный №13042. Министерство иностранных дел, 16 января 1917 г. Совершенно секретно. Дешифровать лично. Мы намерены начать с первого февраля неограниченную подводную войну. Несмотря на это я считаю возможным поддерживать нейтралитет США. Если наши усилия в этом направлении будут безуспешны, мы заключим союз с Мексикой на следующих условиях. Мы будем считать её и в войне нашей союзницей и заключим мир. Мы могли бы предоставить ей за это финансовую помощь и постараться возвратить ей утерянные ею в 1848 г. штаты Нью-Мексико и Аризона.

Выработка подробностей этого плана предоставляется на ваше усмотрение. Вам поручается под строжайшим секретом прозондировать на этот счёт мнение Каранцы и, как только он узнает, что с Америкой также нам не миновать войны, намекнуть, что недурно было бы ему взять на себя инициативу начать переговоры с Японией о союзе, довести их до благоприят-

ного конца и тогда немедленно же предложить своё посредничество между Германией и Японией. Обратите внимание Каранцы на то, что начало нашей беспощадной подводной войны делает возможным обессилить Англию и привести к миру в течение нескольких месяцев. Циммерман» [Дамаскин, 2002].

Текст телеграммы сразу же попал к Реджинальду Холлу. Легализовать телеграмму решили следующим образом: в Мексике, с согласия «Вестерн Юнион», получить дубликат телеграммы и предоставить её Вашингтону. О том кто и как расшифровал её, естественно, умолчать. Так и сделали. Очевидно, что публикация такой информации вызвала бурю негодования во всем мире: выходило, что Германия замышляла заговор против ещё одной нейтральной державы и хотела вовлечь Японию в войну против Англии и США.

Существует ещё две версии доступа англичан к дипломатическим кодам Германии и дешифрования телеграммы Циммермана.

Первая из них связана с именем германского консула в Иране Карла Васмуса, который во время Первой мировой войны вел активную диверсионную деятельность против англичан в Иране. Васмус создал широкую шпионскую сеть и причинял столько неприятностей англичанам, что британское командование объявило о награде в 3 тыс. фунтов стерлингов (в дальнейшем увеличив эту сумму до 14 тыс.) тому, кто доставит им консула живым или мертвым. При проведении одной из диверсий, когда отряд Васмуса собирался взорвать английский нефтепровод у Абадана, англичане едва не захватили консула, но тот сумел сбежать. Однако у него не было времени прихватить с собой багаж. Имущество, принадлежавшее Васмусу, было переправлено в Лондон и свалено в подвал министерства по делам Индии. Лишь позднее, в случайном разговоре с офицером, прибывшим из Ирана, адмирал Реджинальд Холл узнал о том, что захвачен багаж Васмуса. Среди вещей оказался шифрблокнот с кодом, который немцы использовали для шифрования донесений по линиям Берлин – Константинополь и Берлин – Мадрид. Эта находка значительно помогла в дешифровании секретных телеграмм в «Комнате 40».

Далее произошло следующее событие. Главный инженер германской радиостанции в Константинополе по какому-то поводу давал обед. После обеда он на радостях разослал шесть одинаковых сообщений своим коллегам на радиостанции немецких консульств по всему миру. Каждую телеграмму он шифровал по соответствующему коду. Одна из них была зашифрована по коду Васмуса. В результате, имея шифрованный перехват и открытый текст к нему, англичане легко вскрыли шифры еще пяти консульств Германии. Это и позволило им впоследствии ознакомиться с содержанием послания Циммермана.

Согласно другой версии, немецкий дипломатический код добыл шпион Антанты по кличке Смит. Смит совершил свой подвиг в Брюсселе (Бельгия) с помощью официантки кафе Ивонны, в которую влюбился немецкий офицер, работавший на радиостанции. Под предлогом обучения радиоделу Смит выудил из него сведения о главных элементах немецкого кода. Эти сведения Смит лично доставил англичанам. Ивонна была позднее арестована.

Приведенные версии не обязательно противоречат друг другу. Могли иметь место все три версии, независимо друг от друга: один и тот же код мог быть добыт разными путями. Тем не менее, по мнению Уинстона Черчилля, решающую роль в прочтении шифртелеграммы Циммермана сыграли кодовые книги с германского крейсера «Магдебург».

Немцы же придерживались лишь двух версий:

- вражеские шпионы получили доступ к открытому тексту телеграммы Циммермана;
- код выдал англичанам упомянутый Александр Цек.

Свой шифр они считали очень сильным и не допускали мысли о возможности его вскрытия.

Англичане не ограничивались только дешифрованием, используя известные немецкие шифры, они дезинформировали противника. Приведем интересный пример.

Осенью 1914 г. английское адмиралтейство было весьма озабочено действиями немецкой эскадры под командованием

вице-адмирала Максимилиана фон Шпее, крейсировавшей около Южной Америки. 1 ноября 1914 г. корабли Шпее уничтожили в морском бою английскую эскадру. После этого немецкая эскадра прибыла в порт Вальпараисо (Чили). Здесь Шпее застала шифртелеграмма из Берлина, предписывающая ему идти к Фолклендским островам с целью разрушить находившуюся там английскую базу.

Максимилиан фон Шпее

Шпее выполнил приказ, но попался в ловушку. 7 декабря 1914 г. его эскадра была уничтожена английскими линкорами, которые перехватили корабли Шпее. Указанную телеграмму, зашифрованную шифром морского министерства Германии, отправил английский агент из Берлина.

Серьёзную дополнительную информацию о немецких шифрах англичане получили в результате захвата германского торгового судна недалеко от Австралии. Уже к началу ноября 1914 г. англичане получали доступ к сверхсекретной информации ВМС Германии.

В последующие месяцы англичане активно искали немецкие шифры. Так, команда британского траулера выловила в море книгу кодов, выброшенную с борта немецкого торпедного катера. В дальнейшем ценную криптографическую информацию англичане получали в результате обследования затонувших немецких подводных лодок. Особо отличился в добывании кодов и шифров с утонувших немецких подводных лодок сотрудник спецслужбы Великобритании – **водолаз Эдвард С. Миллер**. Судовой плотник Миллер был мастером водолазного дела. В 1914 г. его назначили инструктором Британской морской тренировочной школы. Спустя год, в разгар войны, Миллеру приказали обследовать подводную лодку, потопленную у побережья Кента. Водолаз должен был выяснить состояние и обследовать внутреннее устройство непри-

ятельской подводной лодки, в особенности же ознакомиться с её новейшим техническим оборудованием.

Миллер обнаружил подводную лодку, но проникнуть внутрь через пробоину можно было только с риском повредить шланг, подающий воздух. Все же он пошел на риск и обследовал устройство лодки, более того, в капитанской рубке Миллера заинтересовал металлический ящик, который он привязал к тросу и поднял на поверхность. Из поднятого сейфа были извлечены такие ценности, как планы минных полей неприятеля и новые шифркоды германского флота. «Оставьте буек для приметы. Полный ход вперед, – велел командир водолазного судна. – Все это нужно немедленно доставить в Лондон».

Так началась работа морской разведки в «Комнате 40». Был организован специальный отряд для переброски Миллера с его водолазным оснащением в те пункты английского побережья, где случались потопления германских подводных лодок.

Как отмечают специалисты, «коды, которые Миллер извлекал с морского дна, стали могучим оружием в руках флота союзников».

Во время Первой мировой войны, по мнению многих исследователей, получила незаслуженную славу агент Германии, танцовщица **Мата Хари**. Ее «подвиги» многократно описывались в детективно-шпионской литературе, где значительно преувеличивалась ее роль в добывании секретов противника. Обольщая французских офицеров, она, в частности, узнавала от них секретные криптографические сведения. Однако эти сведения не представляли для немцев особого интереса, поскольку более точную и содержательную информацию они получали от других агентов-профессионалов.

Маргарет Гертруда Целле, впоследствии известная под сценическим псевдонимом Мата Хари, родилась 7 августа 1876 г. в голландском городке Лаувардене в семье владельца шляпного магазина.

Авантюрный характер Маргарет проявлялся еще с детских лет. Девушка подрастала, и убогая жизнь провинции ей претила всё больше. Она мечтала о приключениях и дальних странах.

Мата Хари

Как-то раз, читая брачную газету, наткнулась на предложение руки и сердца некоего капитана колониальных войск Рудольфа Маклеода. Некоторое время спустя она уже в качестве его жены постигала экзотику сначала Суматры, а затем Явы.

В 1903 г. она уехала в Европу. В Париже Маргарет Целле-Маклеод устроилась наездницей в цирк, а вскоре перешла на эстраду. Она обладала эффектной восточной внешностью и была очень пластична, использовала в своих выступлениях элементы ритуальных танцев дикарей Явы и Суматры, взяла экзотическое имя Мата Хари, точный перевод которого достаточно туманен, но разными авторами трактуется как «утренний» или «пробуждающийся» взгляд, или «око утра», или «глаз утренней зари», или что-то в этом роде. Всего этого оказалось достаточно, чтобы покорить Париж, а потом и всю предвоенную Европу.

К началу Первой мировой войны Мата Хари была на пике популярности, деньги текли рекой, но быстро исчезали. Видимо, сочетание всех этих качеств – таинственность, красота, связи в высших кругах, нужда в деньгах – и привлекли к ней внимание разведок. Так или иначе, Мата Хари начинает активно работать на Германскую разведку именно в этот период. Заметим, что сами немцы скептически оценивали ее «секретные» сообщения, возмущались значительными расходами на ее содержание. Более того, они пришли к выводу, что Хари является агентом-двойником, работающим в интересах как Германии, так и Франции, что подтверждают и многочисленные источники. В этом случае ее нужно было «подставить», что и было успешно проделано Германской разведкой.

Немцы использовали код, известный французам. Этим кодом они зашифровали сообщение и направили его своему резиденту во Франции, благодаря чему французы «вычислили» Мату Хари. Ее карьера двойного агента, продолжалась недолго – 13 февраля 1917 г. она была арестована французской полицией по обвинению в шпионаже и, по приговору суда, расстреляна. Вот как описывает ее последние дни И. Дамаскин в своей книге «Сто великих разведчиков» (гл. Мата Хари).

Маргарет Целле. Тюремное фото

«Своей смерти Маргарет Целле ждала в одиночной камере Сен-Лазарской тюрьмы. Но до последнего часа она играла роль той же Мата Хари – исполняла ритуальные танцы перед пришедшими утешить её и обратить в свою веру монашками, доктору обещала открыть три секрета: один даст ему любовь, другой золото, третий вечную жизнь, а предложение старика адвоката заявить о том, что она якобы беременна от него, встретила громким хохотом.

Ранним утром 15 октября её разбудили. Она капризно воскликнула: «Как? Так рано! На рассвете! Что за манера?»

Отказалась от сигареты, но выпила стакан грога. На предложение пастора помолиться заявила: «Я не желаю прощать французам. Впрочем, всё равно. Всё – всё равно. Жизнь ничто, и смерть тоже ничто. Умереть, спать, видеть сны, какое это имеет значение? Не всё ли равно, сегодня или завтра, у себя в постели или на прогулке? Всё это обман»…

Перед расстрелом она просила не завязывать ей глаза и улыбалась, глядя в серое промозглое небо» [Дамаскин, 2002].

Грета Гарбо
в роли Мата Хари

Скандальная жизнь Мата Хари вдохновила многих режиссеров к созданию фильмов. В 1921 г. Людвиг Вольф снял фильм «Шпионка Мата Хари» с Астой Нильсен в главной роли. В 1927 г. режиссёр Фридрих Фегер отразил образ обнажённой красавицы в фильме «Мата Хари, красная танцовщица». Затем две кинозвезды эпохи оспаривали честь лучшего воплощения на экране образа Мата Хари: Марлен Дитрих в фильме фон Штернберга «Опозоренная» в 1931 г., и Грета Гарбо 1 год спустя в фильме «Мата Хари» режиссёра Фитцмориса. Так закончившаяся на земле жизнь Мата Хари продолжилась на экране.

Бывший директор ЦРУ Аллен Даллес, скептически относившийся к разведывательной деятельности Мата Хари, в своих воспоминаниях писал: «Дело в том, что ни в мотивах ее действий, ни в применяемых ею методах, да и в «достигнутых результатах»… я не нашел ничего выдающегося. Вызывает обоснованные сомнения даже тот факт, а стоила ли полученная от воздыхателей информация, изложенная ею на бумаге, самой исписанной бумаги… Ее драматическая казнь является, по сути дела, тем, что сохраняет ее в памяти людей… Она не была подлинной шпионкой» [Даллес, 1992].

Франц фон Папен

В марте 1915 г. капитан разведки Германии **Франц фон Ринтелен** прибыл в США. Там он представился военно-морскому атташе посольства Германии капитану Бой-Эдели и военному атташе капитану Францу фон Папену. Исследователи дают чрезвычайно нелестную характеристику фон Папену: «Удивительно, как такой ограниченный и бездарный человек мог сделать хорошую карьеру и, выходя, из казалось бы, самых невероятных и смертельно опасных ситуаций, всю жизнь оставаться «на плаву». Вот уж, если кого и можно назвать «везунчиком», так это его» [Дамаскин, 2002].

С началом Первой мировой войны фон Папен по указанию из Берлина развернул в Америке диверсионную деятельность, которая продолжалась вплоть до 1915 г.

Фон Ринтелен привез новый секретный код для посла и обоих атташе, так как в Берлине считали, что старый код уже скомпрометирован.

Ринтелену удалось организовать ряд успешных диверсионных акций против американских судов, доставлявших оружие противникам Германии (в том числе и России). Однако вскоре он обнаружил слежку за собой. Его сомнения подтвердились, когда он узнал что код, которым он пользовался для связи с Германией, стал известен англичанам. Этот код англичане похитили через свою сотрудницу, которую «подставили» молодому секретарю немецкого военно-морского атташе. Немцы решили избавиться от своего скомпрометированного агента. Фон Папен отправил Ринтелену открытое письмо, адресованное «герру капитан-лейтенанту Ринтелену», а через Бой-Эдели он получил из Германии телеграмму, в которой также прямо указывалось его имя. Кроме того, фон

Папен использовал скомпрометированный код для передачи сообщений Ринтелена, чем воспользовались англичане.

Ринтелен провалился из-за бездарности своего босса Франца фон Папена, использовавшего устаревший код, известный союзникам. Ринтелен полагал, что это было сделано намеренно, о чем рассказал в своих воспоминаниях, изданных в 1933 г.

Воспользовавшись своим швейцарским паспортом и письмом графа Игнатьева, согласно которому был его представителем по продаже «Кларета» в США, Ринтелен, под именем Эмиля Гаше, отбыл на пароходе «Ноордам» в Европу.

13 августа 1915 г. на рейде Рэмсгейта «швейцарский гражданин Эмиль Гаше» был арестован и препровождён в Тауэр, а в апреле 1917 г., уже после вступления Америки в войну, его отправили в США, где в тюрьме Томбс он содержался до 1921 г.

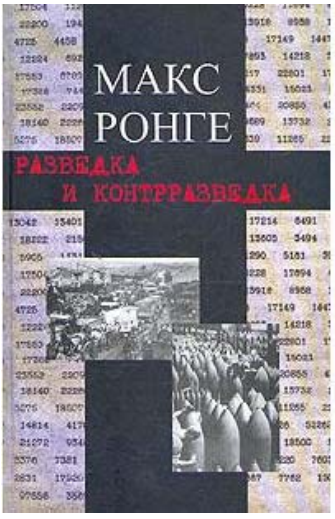
После освобождения Франц фон Ринтелен переехал в Англию, так как решил порвать с германской разведывательной службой и рассказать всё, что он знает о методах немецкого шпионажа. Он остался в Англии и отказался иметь какие-либо дела с нацистами накануне и во время Второй мировой войны.

В середине 1915 г. англичане провели эффектную операцию по дезинформации немцев **«под шифром».**

В отеле голландского города Роттердам, который находился под пристальным вниманием немецких шпионов, остановилось некое «официальное английское лицо», являвшееся дипломатическим курьером. Оно проявило «беспечность», удалившись из номера с дамой и оставив в нем дипломатический багаж. Роль этого «курьера» играл секретарь одного из членов английского парламента Гай Локок.

Немцы не упустили возможности ознакомиться с секретными документами курьера. В результате они получили подложный код, с помощью которого англичане неоднократно вводили в заблуждение германское военное командование. Таким образом, немцам был нанесен серьёзный ущерб.

В начале 1916 г. австрийцы также провели удачную операцию по дезинформации «под шифром». Вот что пишет по



Обложка книги Макса Ронге

этому поводу бывший начальник разведывательного бюро австрийского генерального штаба во время Первой мировой войны **Макс Ронге**: «Для того, чтобы ввести противника (итальянцев – *авт.*) в заблуждение ... ряду радиостанций ... было поручено работать шифром, специально разработанным капитаном Фиглем. Этот шифр итальянцы неизбежно должны были раскрыть, но все-таки ни он, ни содержание депеш не должны были вызвать подозрение в дезинформации» [Ронге, 1993]. В результате итальянцы сосредоточили свои войска на участке ложного наступления австрийцев, оголив направление действительного удара. Он же (Ронге) вспоминает: «В Албании итальянцы пользовались шифром «Менгарини», ключ которого был мною приобретен еще в мирное время. Это сослужило хорошую службу нам и германскому дешифровальному отделу» [Ронге, 1993].

В 1916 г. английский агент **Сидней Рейли** (Зигмунд Георгиевич Розенблюм – еврей, родился в Одессе) добыл военно-морской код Германии. Сведения, полученные в результате дешифрования немецкой переписки, оказались настолько значительными, что западные историки отмечали: «Это было едва ли не самым блестящим образцом разведывательной работы в Первую мировую войну» [Черняк, 1991].

При участии Рейли также был обнаружен шифр румынского военного атташе. Был раскрыт план Корнилова о сдаче Риги немцам и получены другие важные материалы.

Однако еще раньше Рейли нанес ущерб и нашей стране. Накануне русско-японской войны (1905 г.) он выкрал русский код и, с согласия правительства Англии, продал этот код

японцам, что повлекло за собой серьезные негативные последствия для России.

Перебравшись в Петербург, и продолжая работать на англичан, Рейли предложил свои услуги и российской разведке. Крупные деньги он зарабатывал в качестве маклера по различным торговым делам, сочетая это занятие со шпионажем.

Сидней Рейли

Сидней Рейли – «энтузиаст шпионажа и авантюр», как характеризуют его историки.

«Это был человек наполеоновской складки. В жизни его героем был Наполеон…» – так пишет о нем Брюс Локкарт в своих мемуарах «История изнутри». Всей правды о Сиднее Рейли по сей день неизвестно. Достоверно лишь то, что неуёмная жажда приключений ещё в юности забросила его в Латинскую Америку, где его приёмным отцом стал некий Сидней Рейли Каллаган. Отбросив фамилию отчима, юноша взял его имя и стал Сиднеем Рейли. В Америке он начал работать на британскую разведку. Далее, страсть к приключениям переросла в авантюризм, и он стал платным агентом нескольких разведок.

В нашей стране имя Сиднея Рейли более известно в связи с его активной борьбой против большевистской России в 1921–1922 гг., когда при его активном содействии несколько монархических групп, стремились установить прямой контакт с центрами белой эмиграции и, опираясь на их помощь, готовили вооружённое восстание. Эффектная операция, проведенная ВЧК под руководством Артура Артузова, названная «Трест», закончилась захватом Рейли. 5 ноября 1925 г. Рейли был расстрелян.

В середине 1916 г. пионер женского воздушного флота во Франции **Марта Рише** стала агентом французской спецслуж-

бы. Марта Бетенфельд родилась в немецкой семье в Лотарингии. В 1913 г., в возрасте 22 лет, стала одной из первых женщин во Франции, получивших лицензию пилота. В 1914 г. вышла замуж за военного лётчика Анри Рише, который погиб на фронте через 1 год. После гибели мужа Марта, желая любой ценой отомстить немцам, пыталась стать военным лётчиком, однако в боевую авиацию её не допустили. Тогда она предложила свои услуги службе французской контрразведки, где получила псевдоним «Жаворонок» и была направлена в Испанию с заданием «обворожить» барона фон Крона, немецкого военного атташе в Мадриде. Эта операция увенчалась успехом. Пользуясь доверием фон Крона, Марта поставляла службе французской контрразведки сведения чрезвычайной важности. В том числе ей удалось получить секретные коды немцев.

Эту исключительную мастерицу шпионажа наградили орденом Почётного легиона лишь в 1933 г. До этого времени «моралисты» Франции выступали с обвинениями Рише в аморальном поведении при добывании секретной информации.

В феврале 1917 г. в Цюрихе итальянцы проникли в сейф, в котором хранились шифры Австро-Венгрии. Интересно, что специально для взлома сейфа итальянцы выпустили из тюрьмы двух «медвежатников» – де Люка и Палаццо – и отправили их в Цюрих. Однако заплатить взломщикам за их работу итальянская разведка отказалась. Им в качестве вознаграждения были оставлены украденные из сейфа деньги. Взломщики остались весьма недовольны и десяток лет тревожили итальянские суды своими претензиями.

Еще один эпизод времен Первой мировой войны, связанный с дезинформацией «под шифром», имел место в 1917 г. на Ближнем Востоке, где турецкие войска под руководством германских офицеров боролись против англичан.

С помощью различных уловок англичане «ознакомили» турок с подложным английским шифром. Эта агентурная операция включала в себя серию детективных действий (погоня за английским офицером, симуляция ранения и потеря сумки с документами и значительной суммой денег и т.п.).

Своей находкой турки поделились с немцами. «Дешифрованные», с помощью «утерянного кода», английские сообщения существенно дезинформировали немцев. В итоге они проиграли ряд крупных военных сражений.

Во время Первой мировой войны российская контрразведка похитила кодовую книгу американского посла в Румынии. Удивительно, но эту книгу посол хранил не в сейфе, а под матрасом своей постели. Посол, обнаружив пропажу, предпринял «оригинальный ход». Он не сообщил своему руководству о пропаже, а для передачи секретных сведений использовал посла в Вене (коды были идентичными). Для этого ему приходилось часто пользоваться железной дорогой Бухарест – Вена и просить посла в Вене временно передавать ему код для связи с Вашингтоном (свой он, якобы, «забыл» в Бухаресте).

Однако эта игра продолжалась недолго. Посол сознался в своем «проступке» и был отозван на родину.

Немецкий цеппелин времен Первой мировой войны

Брюс Локкарт

В октябре 1917 г. немцы провели один из крупнейших налетов цеппелинов на Англию. На обратном пути два цеппелина получили повреждения и приземлились на побережье Франции недалеко от ставки командования американскими войсками в Западной Европе.

В одном из цеппелинов американцы обнаружили кодовую книгу. Этой находкой они поделились с англичанами. Последние эффективно воспользовались подарком. Англичане захватили, врасплох немало подводных лодок Германии (опираясь на дешифрованную информацию).

В конце 1917 г., после революции, в России был обнаружен архив посольства Англии. В нем оказались действующие английские шифры. В результате был дешифрован ряд телеграмм английского посла в России сэра Джорджа Уильяма Бьюкенена, а затем и сменившего его дипломатического агента Англии Брюса Локкарта.

Британский разведчик Локкарт хорошо известен по его участию в знаменитом «заговоре послов» в 1918 г. Однако его разведывательная деятельность началась раньше и закончилась значительно позже этих событий.

Роберт Гамильтон **Брюс Локкарт** родился 2 сентября 1887 г. в Анструтере, графстве Файф. Его отец был учителем начальной школы, все его предки – шотландцы. «Во мне нет ни единой капли английской крови», – вспоминал Локкарт. Образование он получил в Берлине, затем отправился в Париж, откуда после обучения вернулся в Англию. Когда он вернулся на родину, ему было 23 года. По рекомендации отца поступил на консульскую службу, которую успешно совмещал с литературным творчеством. После г. работы в аппарате министерства Локарт получил назначение на должность вице-

консула, а в 1915 г. занял пост генерального консула Великобритании в Москве. Он стал свидетелем краха царского режима, развала армии, беспорядков в тылу.

В 1917 г. познакомился с Керенским и Савинковым, сотрудничал с Сиднеем Рейли. В Великобритании Локкарт числился специалистом не только по России, значительно позже, в 1939 г., он «вёл» такие страны, как Чехословакия, Венгрия, Югославия, Болгария, Румыния, Греция и Турция. В его задачу входило составление еженедельных политических обзоров по этим странам для МИДа Его официальный титул был «Британский агент…»[Черняк, 1991], но он протестовал против этого звания, так как оно напоминало те печальные времена, когда в Москве его называли «британским агентом» и обвиняли в развязывании интервенции, против которой он, по его признанию, всегда выступал.

Мемуары Брюса Локкарта

10.3. Агентурные действия в период между Первой и Второй мировыми войнами

Если периоды мировых конфликтов – это время активного использования специальных методов в криптографической деятельности и накопления оперативного материала, то периоды между мировыми войнами – это периоды обработки накопленных материалов, их анализа и активной разработки новых методов и средств в криптологии.

Летом 1919 г. ВЧК РСФСР раскрыла подпольную контрреволюционную организацию **«Национальный центр»**. Эта организация была создана в мае–июне 1918 г. в Москве с целью коор-

Н.Н. Щепкин

динации действий антибольшевистских сил в стране. Организация объединяла бывших членов «Правого центра», представителей запрещённых партий кадетов, октябристов и других.

Руководителями «Национального центра» были Д.Н. Шипов, М.М. Фёдоров, Н.Н. Щепкин, среди активных деятелей – П.П. Рябушинский, Д.В. Сироткин и ряд других крупных политических фигур. В мае 1919 г. **Николай Николаевич Щепкин** возглавлял деятельность организации в Москве. Также он входил в состав группы из шести человек, которая координировала деятельность всех московских антисоветских организаций, так называемый «Тактический центр», был членом военной комиссии «Тактического центра» [Думова, 1982]. При обыске у Н.Н. Щепкина была обнаружена «жестяная коробка, содержащая шифрованные и нешифрованные записки, шифр, рецепты проявления химических чернил …». Эти материалы оказали существенную помощь в расследовании деятельности организации.

31 Царица южная восстанет на суд с людьми рода сего и осудит их, ибо она приходила от пределов земли послушать мудрости Соломоновой; и вот, здесь больше Соломона. 3Цар 10:1, 4; 2Пар 9:1; Мф 12:42

2 Он сказал им: когда молитесь, говорите: Отче наш, сущий на небесах! да святится имя Твое; да приидет Царствие Твое; да будет воля Твоя и на земле, как на небе; Мф 6:9

Евангелие от Луки стих 31 и 2

Арестованный по этому делу П.М. Мартынов рассказал об используемом шифре следующее: «Возьмите русское евангелие от Луки, гл. 11 (где «Отче наш») – текст пишется цифрами в два и три цифровых знака; цифра справа всегда означает порядок буквы в стихе, а остальные цифры означают номер стиха. Так, например: 311,26,46,41,311,54 означает, первая буква в 31-м стихе – Ц, шестая буква во 2-м стихе – А (пробелы между словами учитываются – *авт.*) и т.д. Все слово означает «царица»…».

Сэр Остин Чемберлен

Таким образом, подпольщиками использовалась одна из разновидностей книжного шифра.

В 1920-х гг. **англичане** предприняли силовую акцию по захвату документов торгового общества **«Аркос»**. 12 мая 1927 г. полиция произвела обыск в помещении советского торгового представительства в Лондоне и англо-советского акционерного общества «Аркос», заподозренного в шпионаже в пользу СССР. Все служащие «Аркоса» и торговой делегации были задержаны и подвергнуты личному обыску. В тот же день поверенный в делах СССР в Лондоне обратился к министру иностранных дел Великобритании сэру Остину Чемберлену с нотой протеста.

Изъятые при обыске документы не содержали никаких компрометирующих сведений, но, несмотря на это, были использованы британским правительством в качестве основания для обвинения Советского Союза в «подрывной» деятельности в Великобритании, разрыва дипломатических отношений и расторжения всех торговых соглашений. Среди захваченных секретных документов оказались и советские шифры. Эта находка дала англичанам возможность читать шифрпереписку советских дипломатов в Англии. Опубликованные дешифро-

ванные сообщения возбудили общественное мнение и позволили оправдать разрыв дипломатических отношений Великобритании с Россией, которые были восстановлены только в октябре 1929 г.

В начале 1920-х гг. **российской контрразведке** (КРО ОГПУ СССР) удалось добыть ключевую документацию к ряду шифров и кодов иностранных государств, что позволило ОГПУ контролировать телеграфные сообщения ряда иностранных посольств в Москве.

В августе 1921 г. **спецотдел ВЧК** (государственный криптографический орган России – *авт.*) издал приказ, в соответствии с которым все подразделения в центре и на местах должны были направлять в отдел обнаруженные при обысках и арестах шифры, ключи к ним и шифрованные сообщения.

Работа спецотдела началась с детального изучения архивов дешифровальных служб дореволюционной России. Среди архивных документов были обнаружены подлинники и копии шифров Болгарии, Германии, Китая, США и Японии, а также отчеты о работе по их вскрытию и учебные пособия. Этот факт сыграл важную роль в подготовке специалистов – криптографов в послереволюционной России.

Одной из операций **русской разведки** в целях добычи шифра была операция по изъятию шифра из китайского посольства в 1920-х гг., проведенная **Петром Леонидовичем Поповым**, талантливым разведчиком-самоучкой, по профессии судовым механиком с канонерской лодки «Манджур», охранявшей в царское время рыбные промыслы в районе Камчатки. Об этом оставшимся малоизвестным российском разведчике, обладавшим аналитическим складом ума и необыкновенной смелостью, поднявшимся до уровня высококвалифицированного профессионала, подробно рассказал в своей книге В. Гоголь [Гоголь, 1996].

Пользуясь завоеванным авторитетом у китайских властей и посла Китая в СССР Ли Тьяо, Попов получил свободный доступ в китайское посольство в Москве. Изучив обстановку, он составил план получения слепков с ключей от сей-

фа, в котором находились шифрдокументы. Отключив отопление в здании посольства перед очередным визитом туда, Попов, по просьбе хозяев, занялся проверкой всей отопительной системы и получил доступ в зону безопасности. Проверяя там отопительные батареи, он улучил момент и снял нужные слепки с ключей, лежавших на столе шифровальщика. Имея ключи от сейфа, изъятие шифра было осуществлено без затруднений.

В начале 1924 г. резидентом **советской разведки** в Ковно (в то время столица Литвы – *авт.*) стал **Игорь Константинович Лебединский**. Находясь там в течение 2 лет, он проявил себя умелым организатором разведывательной работы, располагал связями с французской, эстонской и латвийской миссиями. Один из информаторов Лебединского, получивший псевдоним **«Василий»**, работал курьером в аппарате военного атташе Франции, через этого курьера советская разведка получала черновики секретной переписки атташе с Парижем, что помогло в раскрытии французских шифров.

Работа курьера, под псевдонимом «Василий», продолжалась до конца 1930-х гг. Сам И.К. Лебединский в дальнейшем работал в Австрии и Германии.

С мая 1924 по ноябрь 1927 гг. военным атташе при полпредстве СССР в Персии (Иране) был **Ардальон Александрович Бобрищев** – бывший офицер царской армии в 1918 г. добровольно вступивший в Красную Армию и состоявший на дипломатической службе. Во время работы в Персии Бобрищев завербовал себе на службу практически всех шифровальщиков Главного штаба Персии. В результате был получен богатый материал, проливавший свет на внутреннюю и внешнюю политику этой страны.

В 1930 г. по идеологическим соображениям перешел на сторону противника начальник контрразведывательного отдела российской спецслужбы ГПУ (Главное политическое управление – *авт.*) **Георгий Сергеевич Агабеков**. Он рассказал о некоторых методах работы ГПУ, связанных с дешифрованием дипломатической переписки. В частности, он раскрыл

Обложка книги Георгия Агабекова букинистическое издание (1996)

детали проникновения ГПУ к афганским дипломатическим шифрам (через переводчика афганского консульства в Ташкенте), а также к правительственным шифрам Персии, путем вербовки шифровальщика при Совете Министров Персии [Агабеков, 1992].

Георгий Агабеков – уникальный исторический персонаж, чья жизнь напоминает авантюрный роман, был первым крупным разведчиком-чекистом, который, выступил на Западе с разоблачением деятельности ОГПУ. Агабеков сотрудничал со спецслужбами Бельгии, Англии, Франции, Голландии, Германии, Румынии, Болгарии. В эмиграции Агабеков опубликовал книги «ГПУ. Записки чекиста» (Берлин, 1930) и «ЧК за работой» (Берлин, 1931). По приговору советского суда в 1937 г. был ликвидирован агентами НКВД.

Мемуары Г. Агабекова – это уникальное свидетельство непосредственного участника многих событий, происходивших в 1920-е гг. В предисловии А.В. Шаврова к книге «ЧК за работой», например, приводятся следующие факты.

«Основным методом работы секретных резидентов была вербовка людей, имевших доступ к секретной информации. Особое внимание чекистов при этом привлекали западные дипломатические миссии, и наибольших успехов ОГПУ достигло именно в перлюстрации дипломатической почты.

Агабеков подробно описал технику такой работы, практиковавшуюся в Иране, когда давал показания представителям западных спецслужб. Глава бельгийской разведки барон

Ферхюльст сначала не поверил, что вся бельгийская дипломатическая почта в Персии перлюстрировалась ГПУ. По свидетельству барона, Агабеков в ответ на это предложил провести эксперимент. Ему был дан запечатанный и прошитый конверт, он вышел в соседнюю комнату и через полчаса вернул его в целости и сохранности, при этом сообщив точное содержание бывшего в пакете документа. Ферхюльст был буквально «покорен» высоким профессионализмом работы бывшего советского резидента. Для Интеллидженс сервис (англ. Intelligence service – собирательное наименование сети разведывательных и контрразведывательных служб Великобритании – *авт.*) также было полной неожиданностью, что с 1926 г. советская разведка имела в своем распоряжении копии почти всех сообщений из Англии, адресованных в Тегеран и даже в Индию. Всего люди Агабекова, работавшие в Мешхеде (город на северо-востоке Ирана – *авт.*), вскрывали ежемесячно свыше пятисот секретных дипломатических писем. Для англичан и бельгийцев это была весьма малоприятная новость, тем более что им было вполне ясно – аналогичные службы ОГПУ успешно действовали в большинстве советских полпредств по всему миру. Советская разведка, видимо, затрачивала на подобные операции небольшие деньги. Во всяком случае, в Мешхеде за каждое переданное ОГПУ английское или персидское письмо местные почтовые чиновники получали всего два доллара, а за любое другое – один доллар. После того, как Агабеков раскрыл эту систему, англичане и их бельгийские коллеги смогли принять меры для прекращения систематической перлюстрации дипломатической почты» [Агабеков, 1992].

В 1925 г. пришел в советскую разведку незаконнорожденный сын графа А.Н. Толстого **Дмитрий Александрович Быстролётов**. Будучи чрезвычайно одаренным человеком. Д.А. Быстролётов имел задатки для того, чтобы стать литератором или художником. Были у него склонности и к естественным наукам.

Гимназию Д.А. Быстролётов окончил в России, в Константинополе – колледж, в Праге получил диплом доктора права, в Цюрихе стал доктором медицины. Он владел более чем 20-ю

Д.А. Быстролётов

языками. В 1937 г. был принят в Союз художников. В 1938 г. – репрессирован. В 1956 – реабилитирован. Скончался Д.А. Быстролётов 3 мая 1975 г.

В 1930 г. Быстролётов стал агентом-нелегалом в Европе. Именно в этом году он обосновался в Германии и наладил регулярное снабжение СССР шифрами европейских стран.

Обладая незаурядной внешностью, он вовлекал в свою работу женщин, представлявших интерес для советской разведки.

Наиболее интересная операция была проведена Быстролётовым в первой половине 1930-х гг. В советском посольстве в Париже работал на высокой должности поверенного в делах **Григорий Зиновьевич Беседовский**, он перешел на сторону французов, украв деньги и наиболее важные документы. Беседовский выдал все секреты посольства и подпольных работников, каких только знал. Погибли люди, делу был нанесен огромный ущерб. Изменник опубликовал книгу. Так случилось, что ее внимательно прочитал И.В. Сталин и написал на полях единственное слово: *«Возобновить»*. Оно появилось напротив рассказа об одной истории, разыгравшейся в парижском посольстве и разглашенной предателем.

Беседовский писал, что в 1928 г. в советское посольство в Париже явился небольшого роста человек, брюнет с красным носом. Незнакомец предложил купить у него шифры Италии за 250 тыс. французских франков, обещая в случае вступления в силу новых продавать и их, но опять за 250 тыс. По словам «носика» главная ценность сотрудничества с ним заключалась в возможности пользоваться этим источником многие годы. Рассчитывая на долговременное сотрудничество, и уверенный в ценности своего предложения он заявил: «Вы располагаете, конечно, на парижской почте своей агентурой и собираете

всякие шифрованные телеграммы, в том числе и итальянского посольства. Я вам доверяю. Возьмите книги, отправляйтесь в свой шифровальный кабинет и дешифруйте пару итальянских шифртелеграмм. Когда убедитесь в подлинности принесенных мною документов, давайте произведем расчет».

Атташе вышел в соседнюю комнату, убедился в подлинности шифров, сфотографировал их, а потом, желая сэкономить деньги, обвинил незнакомца в мошенничестве и выгнал. В Москву фотокопии были посланы с победной реляцией об удачной операции, открывшей советской разведке тайны политики Муссолини, и о сбереженной для советского государства большой сумме денег. Атташе получил орден за хорошую работу, а итальянцы немедленно сменили шифр, поступление новых шифров из-за обмана посредника стало невозможным. Сталин приказал ОГПУ восстановить контакт с посредником, для этого из Норвегии в Москву срочно был отозван Быстролётов.

По прибытии в Москву Быстролётов получил в руки злополучную книгу Беседовского с пометкой вождя вместе с распоряжением найти человека, посетившего парижское посольство со столь необычным предложением. Ему открыли неограниченный кредит и приказали выехать из Москвы в ту же ночь. Это было чрезвычайно сложное задание – найти неизвестного человека, который один раз показался на глаза советскому военному атташе в Париже и про которого только и известно, что он маленького роста, с красным носом. Быстролётов проанализировал ситуацию и, исключая одну страну за другой, нашел отставного офицера швейцарской армии, итальянца по фамилии Росси, с большими связями в Риме. Перед Быстролётовым стояла серьезная проблема, ведь признаться «носику», что перед ним – советский разведчик, было невозможно из-за обмана, произошедшего в Париже. Быстролётов решил выдать себя за японского шпиона, что было возможно, поскольку японцы не могли сами вести разведывательную работу в Европе из-за характерной внешности и поэтому пользовались услугами европейских наемников, которым хорошо платили.

Граф Галеаццо Чиано

При встрече с Быстролётовым Росси рассказал, что торговлю шифрами наладил сам министр иностранных дел Италии **граф Галеаццо Чиано**, женатый на дочери итальянского диктатора Муссолини. По его поручению Росси объезжал все великие державы и, собрав пару миллионов, переходил на средние по величине государства, которым продавал те же шифры дешевле, тысяч по 100, а объехав средние, опускался до мелких и загонял им шифры за пустяки – тысяч по 10. Когда все заинтересованные державы читали итальянскую дипломатическую переписку, граф Чиано менял шифр и Росси пускался в новый обход клиентуры.

После опубликования книги Беседовского Чиано организовал провокацию с исчезновением шифровальных книг в одном из итальянских посольств, нагрянул туда с ревизией и обвинил в краже случайного человека. Невиновный был уничтожен, а Чиано прослыл неукротимым борцом с коррупцией и изменой. Росси стал продавать итальянские шифры Быстролётову, при этом иногда делая «представителю японской разведки» весьма оригинальные предложения. Однажды он предложил начать печатать в Японии фальшивые доллары и был согласен получать не 200 тыс. настоящих франков, а миллион фальшивых долларов.

Следует отметить, что Росси отличался хитростью, изворотливостью и сообразительностью. Пользуясь географической удаленностью Японии и обширностью своих связей, он сначала продавал итальянские шифры японцам в Токио, а затем – их «агенту» Быстролётову в Берлине. Вскоре Росси удалось вычислить, что Быстролётов – советский разведчик, и он решил расправиться с ним. Росси заманил Быстролётова к себе на виллу, жизнь советского разведчика подверглась реаль-

ной опасности, но Быстролётов проявил хладнокровие. Услышав на улице автомобильный гудок, он заявил Росси, что это условный сигнал и если через 10 мин. он не выйдет, то на помощь ему придут товарищи, которые ожидают в машине около дома Росси. Не предвидя такого оборота событий, Росси пошел на попятную и согласился на дальнейшее сотрудничество с Быстролётовым, правда, запросив увеличить ему оплату, на что Быстролётов согласился. В дальнейшем, в качестве компенсации за происшествие на вилле, Росси познакомил Быстролётова с одним французским шпионом, который ради установления дружеских отношений с японской разведкой передал ее «агенту» несколько шифров.

В 1930 г. Быстролётов принял участие в разработке шифровальщика британского МИДа капитана Эрнеста Олдхама (псевдоним **«Арно»**).

В 1929 г. **Эрнест Холлоуэй Олдхам** продал за 2 тыс. долл. США советской разведке английский дипломатический шифр. Этот эпизод так описан в книге Олега Гордиевского и Кристофера Эндрю.

«Эрнест Холлоуэй Олдхам, шифровальщик Управления связи Министерства иностранных дел Великобритании, находившийся в тот момент в Париже с британской торговой делегацией, пришёл в советское посольство, представился как Скотт и попросил, чтобы его принял военный атташе.

Вместо этого он был принят офицером ОГПУ Владимиром Войновичем, представившимся как «майор Владимир». Олдхам заявил, что работает в Форин Оффисе (англ. Foreign Office – Министерство иностранных дел Великобритании – *авт.*) и принес с собой британский дипломатический шифр, который и предлагает купить у него за две тысячи долларов США. Войнович взял шифр и исчез с ним в соседней комнате, где шифр сфотографировали. Возможно, подозревая провокацию, Войнович вернулся к ожидавшему Олдхаму, разыграл возмущение, бросил шифр на колени Олдхаму, обвинил его в мошенничестве и выгнал из посольства. Дешифровщики объединенного подразделения по радиоперехвату ОГПУ определили достоверность шифра, принесенного Олдхамом. Центр

Обложка книги Д.А. Быстролётова букинистическое издание (1993)

сделал Войновичу выговор за то, что тот не заплатил «Скотту» деньги и не установил с ним связь; приказал выдать тому две тысячи долларов и настоял на повторном контакте. К стыду Войновича, офицер ОГПУ, следивший за Олдхамом, когда тот возвращался домой, записал неверный адрес и не смог найти его. Потребовались долгие усилия Ганса Галлени, нелегала ОГПУ в Голландии, известного среди своих агентов как «Ганс», прежде чем Олдхама нашли в Лондоне в 1930-г.» [Гордиевский, 1992].

В течение 3 лет работы с Олдхамом от него были получены шифры, коды, дешифровальные таблицы, еженедельные сборники шифрованных телеграмм британского МИД и другая секретная информация. Однако в дальнейшем Олдхам не выдержал психологической нагрузки, связанной с агентурной работой, и покончил жизнь самоубийством. Используя информацию, переданную Олдхамом, советской разведке удалось завербовать еще несколько сотрудников МИД Великобритании.

В 1930–1936 гг. Быстролётов получил германские шифры и установил оперативный контакт с сотрудником военной разведки Франции. От последнего были получены австрийские, итальянские и турецкие шифрованные материалы, секретные документы нацистской Германии [Шварев, 2006].

Эффективная работа Быстролётова по добыванию западноевропейских шифров позволила советской разведке получать чрезвычайно важную информацию о действиях и намерениях западноевропейских государств в 1930–1940-х гг.

Дмитрий Александрович Быстролётов оставил большое наследие –16 книг и сценарий многосерийного фильма, (см. работы [Быстролётов, 1993, 1996]).

В 1927 г. произошёл крупный провал **советской разведки** в Тегеране (Иран). В результате три завербованных разведкой шифровальщика главного штаба иранской армии были расстреляны, а один приговорён к 15 годам тюрьмы.

Генерал-майор Эрнст Кёстринг

В конце 1920-х начале 1930-х гг. **агент советской резидентуры** в Токио (псевдонимы **«Кротов»**, **«Крот»**, **«Костя»**) регулярно добывал шифровальные таблицы и книги не только японской военной разведки, но и аналогичные материалы из США, Германии и Китая.

Такая эффективность «Кротова» объясняется тем, что он являлся сотрудником одной из спецслужб Японии. Его настоящее имя до сих пор не рассекречено.

Позднее морально-психическое состояние агента стало вызывать подозрения. В одном из донесений токийской резидентуры отмечалось, что «... К. на последние встречи приходит рассеянный, объясняя это усталостью, большой занятостью по работе. Один раз явился пьяный...». Связь с «Кротовым» было решено прервать, агента «законсервировать» на неопределенное время.

В 1935 г. на должность военного атташе посольства Германии в СССР был назначен генерал-майор **Эрнст Кёстринг**. Эрнст Кёстринг родился в 1876 г. в Тульской губернии, где его отец владел имением Серебряные Пруды. Окончив в Москве гимназию, будущий генерал вермахта поступил в Михайловское артиллерийское училище, прослужил некоторое время в русской армии, и перед Первой мировой войной выехал в Германию, где вскоре стал начальником разведки при глав-

В.С. Рясной

ном штабе немецкой армии. По возвращении в СССР в качестве военного атташе посольства Германии он сразу же попал в поле зрения главного управления государственной безопасности НКВД СССР. Контрразведчикам удалось внедрить в кабинет атташе аппаратуру слухового контроля.

Спустя много лет участник этой операции **Василий Степанович Рясной** вспоминал её детали: «В полуподвал жилого дома рядом с особняком Кёстринга пришли строители. Жильцам объяснили, что произошел разрыв труб и нужен серьёзный ремонт. На самом деле с торца дома прорыли подземный ход в подвал особняка, оттуда проникли в кабинет атташе, наставили повсюду «жучков» и успешно замели все следы своего визита» [Залесский, 2000].

Благодаря этой операции удалось получить важную разведывательную информацию. По своей значимости она не уступала информации, поступавшей от советских разведчиков в Германии. Помимо этого, перехваченная информация давала возможность поставлять немцам дезинформацию, что в итоге сыграло важную роль в стратегических просчётах рейха при планировании предстоящей войны против СССР.

В 1934 г. **советской** разведкой был завербован шифровальщик Управления связи британского МИД капитан **Джон Герберт Кинг** (псевдоним **«Маг»**), в результате чего советская разведка получила доступ ко всем секретам британской дипломатии. Кинг передавал не только шифры и ключи к ним, но и копии секретных государственных телеграмм. Они передавались непосредственно И.В. Сталину. Разведка англичан разоблачила Кинга с помощью перебежчика Вальтера Кривицкого (настоящее имя – Гинзберг Самуил Гершевич), ответ-

ственного сотрудника НКВД. Кинг был приговорен к 10-ти годам лишения свободы, но досрочно выпущен за примерное поведение.

Арнольд Дейч

Вербовкой Джона Кинга занимался **Арнольд Генрихович Дейч** (он же Стефан Григорьевич Ланг)**.** Его имя долгое время хранилось в глубокой тайне и стало известно только после развала СССР. А между тем это был выдающийся советский разведчик.

Коллеги по работе звали его Стефаном Лангом. Имя «Стефан» было и оперативным псевдонимом разведчика, которым он подписывал свои сообщения в Центр. Впервые о Дейче было упомянуто лишь в 1990 г. на страницах журнала «Курьер разведки» в связи с рассказом о созданной им группе советских агентов, получившей название «Кембриджская пятерка».

За период работы в Англии Дейч привлек к сотрудничеству с советской разведкой свыше двадцати человек, в том числе и членов знаменитой «Кембриджской пятерки»: Ким Филби, Дональд Маклейн, Гай Берджес, Энтони Блант и Джон Кернкросс.

Все завербованные Дейчем члены «Кембриджской пятерки» успешно работали на Москву в течение длительного времени. Филби стал высокопоставленным сотрудником английской разведки. Блант в период Второй мировой войны работал в контрразведке Великобритании. Кернкросс служил в британской дешифровальной службе, затем координировал деятельность английской разведки в Югославии. Маклейн и Берджес занимали высокие посты в английском МИДе. Они снабжали Кремль ценнейшей информацией о решениях и мероприятиях правительства Великобритании, о деятельности МИД и спецслужб. Американские историки Норманн

Полмар и Томас Аллен в своем капитальном труде «Энциклопедия шпионажа» так оценивают деятельность «Кембриджской пятерки»:

«Эти люди стали одними из самых удачливых тайных вражеских агентов за всю историю США и Великобритании. Им удалось глубоко внедриться в государственные структуры и долгое время добывать сверхсекретную информацию стратегической важности на самых высших эшелонах власти этих двух стран» [Норманн, 1998].

Далее речь пойдет об одном из наиболее известных, в рассматриваемый период, шифраторе **«Энигма»** (рис. 10.1).

Рис. 10.1. **Внешний вид шифровальной машины «Энигма»**

«Энигма» (Enigma – загадка, головоломка) – портативная шифровальная машина. Более точно, «Энигма» – целое семейство электромеханических роторных машин, приме-

нявшихся еще с 1920-х гг. Шифратор был изобретен в 1917 г. Эдваром Хеберном. Промышленная версия создана чуть позже берлинским инженером Артуром Кирхом (в некоторых источниках Артуром Шербиусом – авт.). Хотя шифр «Энигмы», с точки зрения криптографии, был достаточно слаб, но на практике лишь сочетание этого фактора с другими, такими, как ошибки операторов, процедурные изъяны и захваты экземпляров «Энигмы» и шифровальных книг, позволило английским криптоаналитикам вскрывать сообщения, зашифрованные шифром «Энигмы».

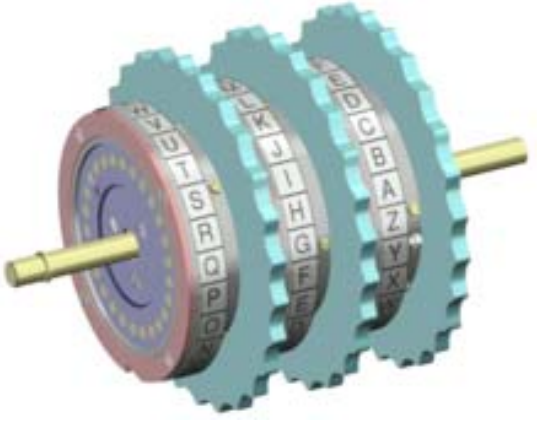


Рис. 10.2. **Три последовательно соединенных ротора «Энигмы»**

На каждой стороне диска «Энигмы», представлявшего собой зубчатое колесо, по окружности располагалось 26 электрических контактов, столько же, сколько букв в латинском алфавите. Контакты с обеих сторон соединялись внутри диска случайным образом 26-ю проводами, формировавшими замену символов. Диски складывались вместе и их контакты, касаясь друг друга, обеспечивали прохождение электрических импульсов сквозь весь пакет дисков на регистрирующее устройство. На боковой поверхности дисков был нанесен алфавит. Перед началом работы диски поворачивались так, чтобы

установилось кодовое слово. При нажатии на клавиши и кодировании очередного символа левый барабан поворачивался на один шаг. После того, как диск делал полный оборот, на один шаг поворачивался второй барабан, после полного поворота второго – третий, как в счетчике электроэнергии.

Пройдя через три диска, сигнал с клавиатуры поступал на так называемый рефлектор – систему проводников, соединяющую каждый контакт с другим контактом на задней стороне третьего диска. Таким образом, рефлектор посылал сигнал обратно через диски, но уже по другому пути. Когда сигнал выходил из системы дисков, он поступал на лампочку-индикатор. Как правило, с «Энигмой» работали три человека. Один зачитывал открытый текст, другой набирал его на клавиатуре, третий считывал шифртекст с ламп и записывал его.

В 1930 г. «Энигма» была модернизирована путем включения в ее конструкцию штепсельной панели из 26-ти пар розеток и штепселей. С ее помощью осуществлялась дополнительная замена перед тем, как знаки открытого текста поступали с клавиатуры на систему дисков и после того как они ее покидали.

Ключами шифратора «Энигма» являлись:

- коммутация дисков (долговременный ключ);
- выбор дисков из комплекта и взаимное расположение их в шифраторе (всего в комплекте имелось пять дисков, в шифратор устанавливались три);
- начальное положение дисков.

До Второй мировой войны и во время нее были выпущены десятки тысяч экземпляров шифратора «Энигма», они применялись во всех видах германских вооруженных сил, а также в «Абвере» и службе безопасности.

В 1931 г. сотрудник шифрбюро министерства обороны Германии Ганс-Тило Шмидт, начал передавать французской разведке материалы по шифрам «Энигмы». Он предоставил им ключевую документацию, инструкцию по эксплуатации и ряд других ценных документов. Однако французские специалисты на основании этой информации сделали категориче-

ский вывод о невозможности вскрытия шифратора. Лишь в 1939 г., после прибытия во Францию польских криптографов, они смогли вскрыть один из ключей «Энигмы», чем доказали ошибочность представлений о невскрываемости шифра.

В середине 1930-х гг. польская спецслужба обнаружила завод в Юго-Восточной Германии, на границе с Польшей, где немцы производили шифрмашину «Энигма» – основной шифратор Германии во Второй мировой войне. В 1933 г. поляки-подпольщики начал изучать то, что производилось на заводе. Эта информация дала возможность польскому генштабу разобраться в устройстве шифратора. В июле 1939 г. поляки передали все материалы англо-французким союзникам вместе с двумя экземплярами аппаратуры. Полученная информация позволила англичанам провести крупнейшую дешифровальную операцию во время Второй мировой войны – операцию **«Ультра»** (дешифрование «Энигмы»). Об этой операции написаны отдельные монографии. Результаты операции «Ультра» существенно повлияли на ведение боевых действий Англии и США во время Второй мировой войны.

В конце 1930-х гг. важные разведывательные материалы начал передавать советской разведке сотрудник МИД Великобритании Джон Кернкросс – один из членов ранее упоминавшейся «Кембриджской пятерки». Наиболее ценная информация – это материалы, связанные с операцией «Ультра», к которым Кернкросс получил доступ. Советское руководство получило возможность изучать важные дешифрованные материалы нацистской Германии. За свою работу Джон Кернкросс был награжден орденом Красного Знамени. В 1951 г., в связи с возникшими у английской спецслужбы подозрениями, Кернкросс покинул Великобританию, в которую вернулся только в 1995 г., где вскоре умер.

В 30-е годы американским специалистам удалось получить открытые тексты телеграмм военного атташе Японии в Лиссабоне (Португалия). Они были извлечены из корзины для мусора. Имея эти тексты, американцы без особого труда раскрыли коды японского посольства.

В те же годы военно–морской флот США широко применял так называемый **«полосковый шифр»** (шифр **«полоски»**). Еще в начале XX в. трудами Паркера Хитта (США) была технологически усовершенствована идея дискового шифратора Томаса Джефферсона (XIX в.).

Шифратор Джефферсона (рис. 10.3) представлял собой цилиндр, разрезанный на 36 дисков. Эти диски насаживались на одну общую ось таким образом, чтобы они могли независимо вращаться на ней. Исходный текст набирался вдоль линейки по одной стороне цилиндра, а шифртекст считывался вдоль такой же линейки с противоположной стороны. Для латиницы количество ключей такого шифратора (36!×26!), т.е. порядка 10^{60}.

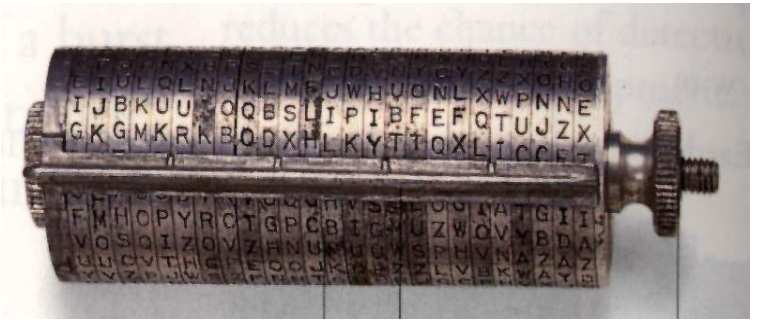


Рис. 10.3. **Шифратор Джефферсона**

Усовершенствованный шифратор Паркера Хитта принял вид «полоскового шифра», значительно более простого в изготовлении. Полоски с удвоенным алфавитом, закрепленные в рамку, гораздо более технологичны, чем диски с алфавитом. Смысл шифрования и расшифрования остался тем же, что и в изобретении Джефферсона, однако сложные диски были заменены на легко воспроизводимые «полоски» из твердого материала, например, картона, металла или пластмассы. Такой шифратор отличался компактностью, его можно было носить в кармане пиджака. Полоски были сменными, их было до сотни,

а выбор тридцати действующих полосок задавался таблицей ключей (суточный ключ).

В конце 1937 г. **японцы** осуществили секретную выемку шифров в здании американского консульства в Кобе (Япония) и перефотографировали американский посольский полосковый шифр. Однако эффективно воспользоваться этой добычей они не смогли, поскольку стойкость шифра определялась ключевой системой, в которую кроме «полосок» входили еще их выбор и расположение на планшете.

Рихард Зорге

В конце 1930-х гг. **советская** разведка завербовала сотрудника МИД Германии **«Винтерфельда»**, имевшего доступ к шифрам. Были получены важные материалы, но впоследствии «Винтерфельд» стал разделять идеи нацистов и прервал связи с советской разведкой.

В конце 1930-х гг. известный советский разведчик **Рихард Зорге**, работавший в Японии под видом немецкого журналиста, заведя любовную связь с секретаршей немецкого посла в Токио, получил возможность знакомиться с шифрперепиской между Берлином и немецким посольством в Японии. Это позволило Зорге постоянно получать важную разведывательную информацию, которую он сообщал в Москву.

Еще в годы Первой мировой войны Зорге служил в вооруженных силах Германии. После демобилизации поступил в Гамбургский университет на факультет политологии. Где успешно защитил докторскую диссертацию. В 1919 г. Рихард Зорге познакомился с немецкими коммунистами и в том же году вступил в Компартию Германии [Колесников, 1965].

В первой половине 1930-х гг. под псевдонимом **«Рамзай»** Зорге работал в Шанхае. За годы работы в Китае под видом немецкого журналиста и «истинного арийца», Зорге хорошо

зарекомендовал себя в нацистских кругах и в 1933 г. вступил в нацистскую партию. Когда Зорге стал видным партийным функционером, Коминтерн направил его в фашистскую Японию, где он работал помощником немецкого посла, генерала Югена Отто. С вторжением японских войск в 1931 г. в Манчжурию коренным образом изменилось соотношение сил на азиатском континенте. Япония сделала серьезную заявку на статус азиатской супердержавы, поэтому интересы советских разведчиков переключаются на Страну Восходящего солнца.

В Японии Зорге стал ведущим немецким журналистом, часто публиковался в нацистской прессе. Накануне войны сумел занять пост пресс-атташе германского посольства в Токио. Всесторонне образованный, с прекрасными манерами и знанием многих иностранных языков, Зорге завел широкие связи с немецких кругах, был вхож в высшие круги нацистского посольства. Создал в Японии разветвленную разведывательную коммунистическую организацию.

В 1935 г. Зорге по вызову начальства кружным путем через Нью-Йорк добирается до Москвы и получает от нового начальника четвертого управления Урицкого очередное задание – выяснить способна ли Япония по своим материальным и людским ресурсам напасть на СССР. Тогда же было решено заменить радиста Зорге, им стал Макс Клаузен, знакомый Рихарда еще по Шанхаю.

Примечательно, что шифр, используемый Клаузеном, не удалось расшифровать ни японским, ни западным дешифровщикам. В качестве ключа Зорге, со свойственным ему остроумием, применял статистические ежегодники рейха, позволяющие варьировать шифр до бесконечности. Кроме того, информация по конспиративным каналам передавалась в Центр на микропленках. Особо важные снимки, например военных объектов или образцов вооружения, с помощью специальной аппаратуры уменьшали до размеров точки, которую специальным составом приклеивали в конце строки письма самого обычного содержания. Как мы сейчас бы определили – использовали методы стеганографии (скрытия самого факта передачи сообщения).

В октябре 1937 г. отказался вернуться в Советский Союз директор Лондонского отдела Интуриста **Арон Шейнман**, бывший нарком внешней торговли СССР. Он передал англичанам сведения об организации советской шифрсвязи.

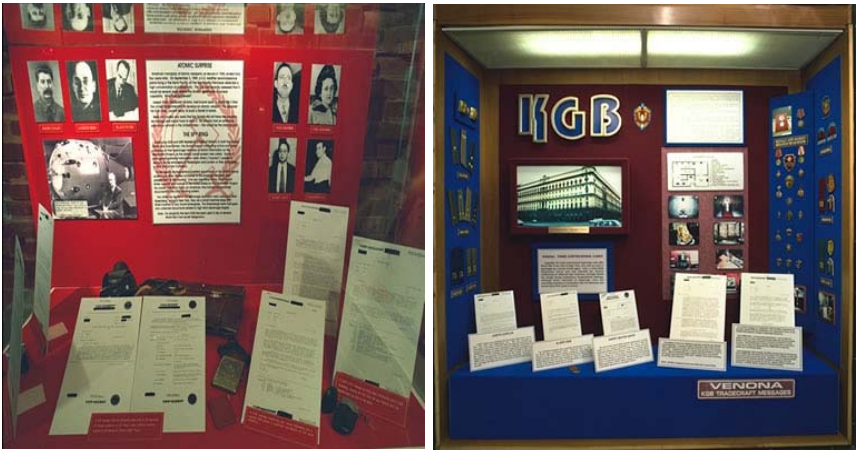
Маршал Г.К.Жуков

В июне 1938 г. начальник управления НКВД по Дальневосточному краю **Люшков Генрих Самойлович**, испугавшись сталинских репрессий, перебежал к **японцам**. Здесь он выступил с рядом статей и интервью, где подробно говорил о массовых репрессиях в СССР. Кроме того, он передал японцам сведения об организации шифрсвязи. Люшков стал гражданином Японии под именем **Ямогочи Тосикадзу**. Однако в 1945 г. при вступлении советских войск в Манчжурию его ликвидировали сами японцы как нежелательный источник информации о методах работы японской разведки.

В 1939 г. в районе Халхин-Гола японские войска вторглись на территорию Монголии, имевшей договор об оказании военной помощи с СССР.

Командующий советскими войсками комкор (будущий маршал) **Георгий Константинович Жуков** разработал план оперативно–тактического обмана противника перед наступлением войск, один из пунктов которого включал в себя вопросы дезинформации противника.

Он вспоминает: «Мы знали, что противник ведет радиоразведку и подслушивает телефонные разговоры, и разработали в целях дезинформации целую программу радио и телефонных сообщений. Переговоры велись только о строительстве обороны и подготовке её к осенне-зимней кампании. Радиообман строился главным образом на коде, легко поддающемся расшифровке». В результате японцы поверили в то, что советские войска укрепляют свою оборону и наступать не собираются. Это стало их грубым просчетом.



Стенды музея АНБ США, посвященные операции «Венона»

Одна из крупнейших операций **американских спецслужб** в области дешифрования советской переписки получила наименование **«Венона»**. Успехи этой операции во многом определялись полученными американцами оперативно-агентурными материалами. Корни этой операции уходят в конец 1930-х гг.

Во время советско-финской войны 1939–1940 гг. финны на поле боя захватили шифровальные блокноты НКГБ. В ноябре 1944 годы они продали их американцам. Американцы, скопировав блокноты, вернули оригиналы своему союзнику – СССР. И хотя в мае 1945 годы шифры были заменены, тем не менее, блокноты помогли американцам дешифровать перехваченные до мая 1945 г. шифрсообщения агентуры НКГБ. Это имело весьма серьёзные последствия для советских спецслужб.

10.4. Агентурные действия в период Второй мировой войны

О Вилли Лемане широкая общественность узнала недавно. Он курировал в гестапо оборонную промышленность и военное строительство фашистской Германии. В течение 12

лет Леман передавал в Москву важные сведения о масштабах подготовки Германии к установлению мирового господства, а также о новейших технических разработках третьего рейха.

Вилли Леман

Вилли Леман (Willi Lehmann) родился в 1884 г. под Лейпцигом в семье учителя. В 17 лет добровольно пошел служить на флот и побывал во многих дальних походах. Во время одного из них был свидетелем морского сражения Русско-японской войны при Цусиме. В 1911 г. Лемана приняли на службу в берлинскую полицию рядовым, но вскоре как способного сотрудника, перевели в контрразведывательный отдел при полицай-президиуме Берлина.

В конце 1920-х гг. Вилли Леман был завербован сотрудниками ИНО ОГПУ – так тогда называлась советская внешняя разведка. Несмотря на то, что основанием для вербовки Лемана стало его крайне отрицательное отношение к набирающим силу фашистам, по заданию центра он вступил в НСДАП и стал работать в гестапо, где дослужился до звания гауптштурмфюрера СС, что приблизительно соответствует званию «капитан». Леман поставлял советскому руководству чрезвычайно ценную информацию, например, о разработках ракет ФАУ-1 и ФАУ-2, информацию о вооружении вермахта и люфтваффе, работах в области судостроения и радиолокации и, естественно, о работе гестапо. Общий объем переданной Леманом в СССР информации составляет 28 внушительных томов. Особенно активно он работал в 1939-1941 гг., в частности, он был одним из многочисленных источников, предупреждавших в июне 1941 г. о нападении Германии на СССР. Среди прочих сведений, в этот период Леман передал сотрудникам советской разведки **шифры РСХА,** главного имперского управления безопасности – одной из главных спецслужб

фашисткой Германии, что позволило советским специалистам дешифровать многие перехваченные немецкие радиограммы. В начале войны Германии против СССР связь с Леманом прервалась, восстановить ее попытались летом 1942 г., для чего в тыл к немцам были заброшены два советских агента – немцы по национальности. Этим людям удалось добраться до Берлина, но там они были арестованы и, не выдержав пыток, сообщили немцам о цели своего задания. С их помощью немцам удалось расшифровать присланное из Центра сообщение с именем агента и способы связи с ним. В декабре 1942 г. Вилли Леман был арестован гестапо и казнен.

Интересно отметить, что по некоторым сведениям Леман послужил одним из прототипов штандартенфюрера Штирлица из знаменитого кинофильма «Семнадцать мгновений весны». Однако создатели фильма вряд ли могли что-либо знать о Лемане – первые сведения о деле **«Брайтенбаха»** (под этим псевдонимом работал Вилли Леман) были обнародованы только через 20 лет после выхода фильма на экраны.

В начале Второй мировой войны США придерживались нейтралитета. На их территории в большом количестве сосредоточилась агентура фашистских государств. Англичан очень интересовала эта агентура.

Английская разведка завербовала жену британского дипломата **Артура Пака** американку **Бетти Торн** (псевдоним **«Синтия»**), которая, будучи со своим мужем в Испании еще в канун гражданской войны, весьма успешно выполнила первое поручение британской разведки, завязав бурный роман с одним испанским офицером высшего ранга. В 1937 г. Пак служил в Польше и Бетти, которой было 27 лет, выделялась среди варшавского дипломатического общества своей высокой культурой, светскостью, необыкновенным обаянием и красотой: волна каштановых волос, большие зеленые глаза и стройная фигура. Тогда она выполнила второе задание штаба разведки в Лондоне. Соблазнив помощника польского министра иностранных дел, она добыла шифровальные ключи к знаменитой германской шифрмашине «Энигма» [Павлов, 1999].

Свою разведывательную деятельность в Вашингтоне «Синтия» начала с добычи итальянского шифра. Установив связь с итальянским военно-морским атташе, человеком уже в г.х, она пошла на риск. После того как итальянский офицер признался ей, что не испытывает симпатий к тандему Гитлер-Муссолини, она рассказала ему о своем сотрудничестве с разведкой, но не британской, а американской, учитывая, что Англия воевала с Италией. Офицер передал ей «для американцев» итальянский шифр. Так британский военно-морской флот получил информацию для дешифровки всех сообщений итальянского средиземноморского флота и в марте 1941 г. этот флот был разбит наголову британским флотом около мыса Матхиан, вблизи греческих берегов.

Гитлер и Петен (слева)

Начальник британской координационной службы безопасности **Уильям Стефенсон** был очень доволен «Синтией», вызвал ее в Нью-Йорк и поставил перед ней новую, как он говорил, чрезвычайно сложную задачу.

Ей надлежало найти путь к добыванию всей переписки – письменной и телеграфной – посольства вишистской Франции в Вашингтоне (пронемецкого режима, созданного во Франции после ее капитуляции в 1940 г. – авт.) с Европой.

Обложка книги Виталия Павлова

«Синтия» начала с того, что тщательно изучила личный состав посольства Виши и решила играть роль американской журналистки, не раскрывая своей связи с Англией и тем более с британской разведкой. Для начала она явилась взять интервью у посла Виши, выдавая себя за журналистку, симпатизирующую правительству Петена (Анри Филипп Петен – глава коллаборационного правительства Виши во время Второй мировой войны – *авт.*). Перед встречей с послом состоялась ее беседа с пресс-атташе посольства, капитаном Чарльзом Брюсом, о котором она уже знала, что он бывший пилот военно-морского перехватчика, и что до начала войны он поддерживал хорошие отношения с британскими летчиками. С этой встречи началась тесная связь «Синтии» с французским капитаном, закончившаяся его вербовкой от имени американской разведки и участием в выполнении задания английских спецслужб. С его помощью она сумела добыть французские шифры. Они сыграли важную роль при высадке союзных войск в Алжире и Марокко.

В 1946 г. «Синтия» вышла замуж за Брюса. В 1963 г. в возрасте 53 лет она скончалась от рака. В 1996 г. немецкий журнал «Шпигель» назвал ее талантливой продолжательницей дела Маты Хари. Подробное описание операции «Синтия» можно найти в книге Виталия Павлова «Женское лицо разведки».

В связи с ролью женщин в добывании секретных материалов вспоминается один интересный исторический эпизод. В средневековом Китае сложилась традиция, согласно которой в качестве послов и посланников нередко назначали евнухов из

императорского окружения. Уж они-то не отвлекались «по пустякам» от выполнения своих государственных обязанностей.

В начале 1940 г. шифровальщик американского посольства в Лондоне **Тайрон Кент** был завербован немецкой разведкой («Абвер») и передал немцам секретные телеграммы, шифры и ключи к ним. Этот красивый, прекрасно образованный молодой человек, сын известного американского дипломата, бывшего генерального консула США в Мукдене, занимавшего значительные должности в американских посольствах в Мадриде и Париже, пошел по стопам отца. Прекрасный спортсмен, умный и общительный, Тайрон неизменно был душой любых компаний. С блеском окончил Принстонский университет, прослушал курс в Сорбонне и завершил образование по курсу экономики в университете имени Джорджа Вашингтона. Продолжив семейные традиции, поступил на дипломатическую службу и в начале 1939 г. отправился в первую командировку в американское посольство в Москве. Там проявил себя с наилучшей стороны, и это оценили в госдепартаменте. И вполне закономерно, когда началась Вторая мировая война, и США приоритетным направлением своей политики сделали Великобританию, Кент, в числе наиболее перспективных молодых дипломатов, уже в октябре оказался в американском посольстве в Лондоне. Там стал шифровальщиком, чему, несомненно, способствовало его блестящее знание французского, немецкого, итальянского и русского языков. Доверив ему самые сокровенные тайны, руководство госдепартамента ограничилось изучением его безупречной анкеты, не удосужившись поинтересоваться его политическими взглядами. А они, судя по всему, оказались крайне расплывчатыми. Окружение Кента в Лондоне составляли главным образом члены «Общества англо-германских связей», «Британского союза фашистов» и других не менее одиозных организаций.

Как-то на одной из вечеринок Кента познакомили с очаровательной баронессой Анной Волкофф. Рожденная в России, она с детских лет была английской подданной. Ее семье

после февральской революции в России удалось бежать за границу и со временем натурализоваться. Тем не менее, она с гордостью носила титул русской баронессы, пожалованный Николаем II ее отцу, адмиралу императорского флота. Ко времени знакомства с Кентом она владела в центре Лондона модным магазином верхней одежды. Анна была не только тесно связана с руководством британского фашистского движения, но и вхожа в высокопоставленные круги страны. Этой красивой и весьма опытной женщине ничего не стоило вскружить голову неискушенному молодому американскому дипломату. И 24-летний Тайрон безумно влюбился в 37-летнюю Анну. Но никто, даже самые близкие ее друзья, и не подозревали, что восхитительная русская баронесса была одним из самых искусных агентов Канариса. Анне Волкофф не потребовалось много времени, чтобы полностью подчинить Кента своей воле. Ей удалось убедить своего пылкого молодого любовника, что его стремление к миру и дружбе между народами не должно ограничиваться словами, нужны поступки.

Джозеф Кеннеди

Каждый вечер, уходя со службы, Кент прихватывал секретные документы. Вместе с Анной фотографировал их, а наутро возвращал в посольство. Поток информации, передаваемый влюбленной парой в Берлин, был поистине неоценим. Кроме переписки между послом Джозефом Кеннеди (отцом будущего президента США Джона Кеннеди) и государственным секретарем Корделлом Хэллом, Кент скопировал сотни шифровок, которыми регулярно обменивались Белый дом и Уайтхолл через американское посольство.

Эта информация была уникальной. Достаточно уже того, что не имей этих ежедневных материалов Кента, Гитлер ни в коем случае зимой 1939–1940 гг. не решился бы на передышку и не получил бы возможность без спешки подготовиться к «блицкригу». Позже на Нюрнбергском процессе именно это засвидетельствовали главные военные преступники Кейтель, Йодль и Редер.

Кент был разоблачен в мае 1940 г. Вместе с ним была арестована и Анна. В ходе расследования возникло предположение, что аналогичную акцию Кент провел в пользу СССР еще в 1938 г., когда он был шифровальщиком американского посольства в Москве. Посол США в Лондоне Джозеф Кеннеди в своих воспоминаниях после окончания войны писал: «В руках Кента находился секретный код госдепартамента США. Из-за предательства Кента после его ареста все дипломатические связи американской дипломатической службы были нарушены, и это в такой ответственный момент – во время событий в Дюнкерке и падения Франции!». Перерыв в работе секретной связи всех американских посольств и миссий во всем мире продолжался от 2 до 6 недель, пока в посольства не прибыли из Вашингтона особые курьеры с новыми шифрдокументами. В условиях военного времени такая замена заняла несколько недель, учитывая их доставку из США через Атлантический океан. Таким образом, США на длительное время лишились секретной связи с Европой. Это повлекло за собой значительные негативные последствия в плане секретного информационного общения с европейским континентом.

В начале 1940-х гг. **агенты США** проникли в помещение японского консульства в Нью-Йорке. Им удалось скопировать наиболее сильный японский шифр, получивший наименование **«Пурпурный код»** (рис. 10.4). В августе 1940 г. армейская дешифровальная служба под руководством видного американского криптоаналитика, автора многих работ в этой области, Уильяма Фридмана добилась выдающегося успеха – вскрыла японский шифр, что дало американской разведке доступ к секретной японской дипломатической корреспонденции ещё до нападения Японии на Перл Харбор.

Аналогичные операции американцы провели и в других японских представительствах на территории США.

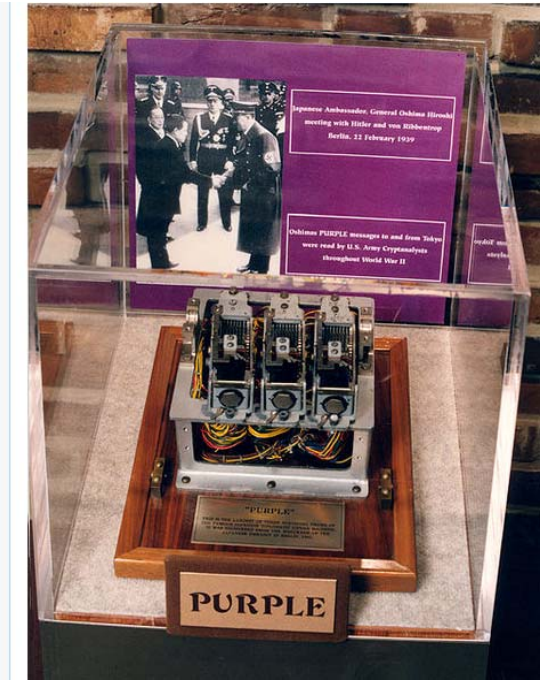


Рис. 10.4. **Часть попавшей в распоряжение союзников в 1945 г. «Пурпурной машины»**

Уильям Фридман

Истории вскрытия Уильямом Фридманом японского военного кода посвящены книги Рональда Кларка (Ronald W. Clark) «The Man Who Broke Purple: The Life of the World's Greatest Cryptologist, Colonel William F. Friedman» (Человек, который пробил Пурпурный: биография величайшего криптолога мира полковника Уильяма Ф. Фридмана, 1977) и Дэвида Кана (David Kahn) «The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet» (Дешифровщики: всеобъемлющая история секретной связи с древних времён и до интернета, 1967).

В 1940 г. сотрудник канцелярии военного атташе США в Риме **Л. Жерарди** был завербован итальянцами и передал им сведения об американском «черном коде» и открытые тексты секретных телеграмм. О роли Жерарди в дешифровании американской переписки стало известно лишь в 1949 г. Выяснилось, что криптоматериалы Жерарди стали известны немецкой разведке – службе «Абвер». Это позволило немцам читать секретные послания американцев в острой военной ситуации. В одной из дешифрованных телеграмм говорилось: «В телеграмме американского военного атташе в Москве, адресованной в Вашингтон, содержится жалоба по поводу отсутствия поставок оружия, обещанного Соединенными Штатами, и говорится, что если СССР не получит достаточную помощь немедленно, то ему придется подумать о капитуляции».

В 1940 г. известный **советский** разведчик **Ким Филби,** один из членов уже упоминавшейся нами знаменитой «Кембриджской пятерки», предпринял неудачную попытку проникнуть в центр криптографической службы Великобритании.

Ким Филби

Вот что он сам писал по этому поводу: «У меня состоялась одна многообещающая встреча с Фрэнком Бёрчем, которую организовал наш общий друг. Бёрч был ведущей фигурой в государственной школе кодирования и шифровального дела – криптографическом учреждении, которое занималось раскрытием кодов противников (и друзей). Однако Бёрч в конце концов отверг меня на том издевательском основании, что не может предоставить мне жалованье, достойное моего труда» [Ким Филби, 1989]. Однако позднее, став одним из руководителей британской разведки, Ким Филби передал советской разведке важные сведения, которые в частности, освещали деятельность английской криптографической службы.

В начале 1941 г. руководитель спецслужбы США **Уильям Донован** прибыл в Болгарию. Имитируя состояние сильного алкогольного опьянения, он «позволил» немецким агентам скопировать имеющийся у него шифр. Затем этим же шифром он передал из Югославии в Вашингтон сообщение о своих успешных попытках втянуть Югославию в войну против Германии. Немцы, естественно, прочли это сообщение и в качестве упреждающего удара 6 апреля нанесли мощный бомбовой удар по Югославии. Погибло более 24 000 человек, и Югославия действительно стала противником Германии.

Уильям Донован

Белград после немецкой бомбардировки
6 апреля 1941 г.

В 1941 г. **спецслужба Швеции** раскрыла один из шифров Германии. Дешифрованные телеграммы доставлялись по разным адресам курьером **Нюбладом,** действовавшим под видом почтальона. Он был завербован советской разведкой, которая поручила ему вскрывать замок портфеля, в котором лежали телеграммы, и оперативно их фотографировать. Пленки тут же передавались советскому разведчику. Дешифрованные материалы, помимо их собственной значимости, позволили советским дешифровальщикам самостоятельно вскрывать этот шифр, несмотря на частую смену ключей. Нюблад в дальнейшем был разоблачён и арестован. Таким образом, Благодаря в общем-то элементарной операции, германские депеши без особой задержки передавались в Москву.

В начале 1941 г. **немцы** провели удачную операцию под названием **«Нордпол»** («Северный Полюс»). Захватив британского радиста-шифровальщика, плененного в оккупированной Голландии, они заставили его работать на себя. Радист, находясь под контролем немцев, передал в Англию большое количество

Харро Шульце-Бойзен

шифрованных сообщений, в которые сумел поставить специальные отметки, свидетельствующие о том, что он работает под контролем противника. Однако англичане приняли эти знаки за последствия искажений в канале связи и не оценили их по достоинству. Радист сумел вставить в один из шифртекстов слово «пленен». Но и этот «крик души» не был понят англичанами. В итоге радиоигра с шифрами привела к тяжким для англичан последствиям. Немцам удалось захватить разведывательные группы английских спецслужб, завладеть новыми радистами и их аппаратурой. Им удалось захватить семнадцать новых засекреченных узлов связи на территории Голландии. Впоследствии эта операция распространилась на территорию Бельгии и Франции, где было захвачено большое количество английских агентов. Около 50-ти из них были расстреляны. Лишь в 1943 г. англичане раскрыли эту игру. Однако европейское подполье к этому времени уже было разгромлено немцами.

В декабре 1941 г. **немецкая контрразведка** обнаружила в Бельгии советскую разведгруппу из известной сети **«Красная Капелла»**. Им удалось захватить радиста и шифровальщицу. Шифровальщица покончила с собой, а радист секретов не выдал. Затем немцы захватили еще два центра связи «Красной Капеллы». При обысках и арестах им удалось выяснить, что использовался книжный шифр. Немецкие контрразведчики обнаружили и книгу – ключ.

Вряд ли найдется европейская страна, в которой так или иначе не писали бы о группе немецких антифашистов **Арвида Харнака** (псевдоним **«Корсиканец»**) и **Харро Шульце-**

Бойзена (псевдоним **«Старшина»**), именуемой «Красная капелла». В разведывательных институтах Запада, утверждает известный французский публицист Жиль Перро [Жиль Перро, 2004], «капелла» изучается как организация, представляющая сплав антифашистского сопротивления с элементами разведывательной деятельности, добившаяся в целом поразительных результатов. «Красная капелла» включала в себя многочисленные, зачастую не связанные между собой группы антифашистского сопротивления.

Леопольд Треппер

Они работали либо самостоятельно, либо в контакте с советской внешней разведкой, а часть из них – под непосредственным кураторством Главного разведывательного управления (ГРУ) Генштаба Красной Армии.

Ещё один эпизод из истории «Красной Капеллы». В июле 1942 г. немцы арестовали **Иоганна Венцеля** – основного радиста бельгийской сети. Он выдал шифры и коды организации. Расшифровав с помощью полученных сведений большое количество перехваченных радиограмм, немцы получили важные сведения о наличии в Берлине советской агентурной сети. Исходя из характера информации, они сумели выйти на обер-лейтенанта ВВС Германии Харро Шульце-Бойзена и ответственного сотрудника министерства экономики Арвида Харнака, которые являлись руководителями указанной сети. Вскоре они были арестованы, осуждены и казнены. Позднее немцы захватили одного из руководителей «Красной капеллы» **Леопольда Треппера**. С его помощью они попытались затеять радиоигру.

Игра началась, но Треппер сумел передать в Москву сообщение, что он работает под контролем немцев. Игра сорвалась, а Трепперу удалось бежать. Однако у советской стороны

возникли подозрения относительно истинной деятельности Треппера. Когда Треппер прибыл в Москву, он тут же попал на Лубянку. 19 июня 1947 г. Треппер был осужден на 15 лет, позднее срок сократили до 10 лет. После смерти Сталина, в 1954 г. Треппер был реабилитирован. Леопольд Треппер умер в Израиле в 1982 г.

В 1941 г. имел место интересный **обмен криптографическими секретами**. Англия передала СССР коды люфтваффе (ВВС Германии) и инструкции по вскрытию ручных шифров немецкой полиции в обмен на захваченные русскими войсками немецкие шифровальные документы. Позднее они передали нашей стране материалы по вскрытию ручных шифров немецкой военной разведки «Абвер», но, ничего не получив в обмен, свернули эту сторону сотрудничества с СССР.

Удивительно, но иногда происходили анекдотические случаи беспечности в охране криптографических секретов. Например, операция «**Магия**» (США) по вскрытию японских шифров во время Второй мировой войны охранялась серьёзной завесой секретности. Однако имели место и следующие факты. В госдепартаменте США были утеряны материалы «Магии». Затем в корзине для мусора военного адъютанта президента были случайно найдены документы, связанные с операцией «Магия». Наконец, в Бостоне агенты ФБР задержали человек, пытавшегося продать криптографическую информацию «Магии».

В свою очередь японцы через своих агентов получили сведения о том, что их дипломатическая переписка читается американцами.

Весной 1941 г. японский посол в Германии **Осима** передал соответствующее сообщение в Токио. Аналогичные сведения передавал в Токио и японский посол в Вашингтоне **Номура**. Однако в Токио не поверили этим сообщениям. Японцы были полностью уверены в надёжности своих шифров. Шифраппаратура не была заменена, и американцы, контролировавшие эту переписку, со вздохом облегчения продолжали свою работу.

**Японский посол в Вашингтоне Номура (слева)
и государственный секретарь США Хэлл (в центре)**

В 1942 г. **немецкая контрразведка** захватила радиста – шифровальщика резидентуры **ГРУ** в Берлине. Под пыткой он выдал шифры. В результате была уничтожена советская разведывательная группа в Германии.

В 1942 г. **шведская разведка** завербовала двадцатилетнюю немку, работавшую секретарём шефа гестапо в немецком посольстве в Швеции (агент «Дядя»). С её помощью шведам удалось вскрыть код, которым пользовалось немецкое посольство в Стокгольме.

Во время Второй мировой войны **немцы** вели целенаправленный поиск русских шифровальщиков. В одном из приказов вермахта говорилось: «Кто возьмет в плен русского шифровальщика, будет награжден крестом, отпуском на Ро-

дину и обеспечен работой в Берлине». Эта работа была небезуспешной, что подтверждает следующий пример.

В октябре 1942 г. в Балтийском море финской подводной лодкой «Весихиими» была потоплена советская подводная лодка С-7, а 5 ноября другая финская субмарина «Ветехинен» в том же районе таранным ударом потопила еще одну советскую подлодку Щ-305. Всего в 1942 г. Краснознаменный Балтийский флот в результате действий немецких и финских противолодочных сил потерял одиннадцать подводных лодок. Это больше чем за любой другой год войны. Такие потери вызвали у командования КБФ подозрения в том, что противнику известны шифры флота. Эти подозрения подтверждались показаниями пленных, среди которых были и бывшие советские военнослужащие, забрасываемые немцами в советский тыл для диверсионной работы. В частности, один из них заявил, что во время нахождения в плену беседовал с командиром подводной лодки С-7, который спасся после гибели подлодки и был пленен экипажем «Весихиими». Командир С-7 утверждал, что командир финской подводной лодки заявил ему о том, что ждал С-7, так как знал координаты боевой позиции советской лодки и время выхода ее из Кронштадта. Также особую обеспокоенность вызвала пропажа 22 мая 1942 г. связного самолета У-2, летевшего из Новой Ладоги в Ленинград. На борту этого самолета находился шифровальщик с комплектом секретных документов по обеспечению скрытой связи. Хотя следует отметить, что этот эпизод вряд ли мог повлиять на гибель советских подводных лодок осенью 1942 г. После безуспешных поисков самолета штаб КБФ принял решение сменить шифры флота, что и было сделано в течение 3 дней. К тому же в 1945 г., после возвращения из плена, пропавший шифровальщик дал показания сотрудникам контрразведки, что он вместе с пилотом У-2 (рис. 10.5) успел порвать и закопать в снег шифрдокументы до того как их пленил финский лыжный дозор. Однако этот факт подтверждает попадание в руки противника советских шифровальщиков и вполне возможно, что немцам и их союзникам финнам все же удавалось добывать действующие шифры КБФ.

Рис. 10.5. **Самолеты У-2 часто использовались для связи (в том числе для перевозки шифрдокументов)**

Иногда в руки немцев попадали и советские шифраторы. Так немецкий пилот ночного истребителя **Вольфганг Янк**, служивший в эскадре NJG 200 и одержавший одиннадцать воздушных побед, во время одного из вылетов сбил советский самолет с группой генералов на борту, летевший в Ленинград. Самолет упал на территорию, занятую немцами, и в его обломках удалось обнаружить неповрежденную шифрмашину. Однако, сведений о типе шифратора и использовании этого трофея немцами нет.

Во время Второй мировой войны **англичане** провели интересную криптографически-оперативную акцию под названием **«Посев»**. Дело в том, что для оперативного дешифрования германской переписки большую помощь оказало бы наличие открытого текста к перехваченным шифрованным сообщениям. Такой открытый текст шифровальщики называли «подсказкой». Для реализации этой идеи англичане предпринимали ряд провокационных действий на море в надежде на то, что противник сообщит о них в своих шифрованных посланиях. В частности, они сбрасывали с самолетов морские мины в тех местах, которые немцы считали свободными от мин. В эти места немцы немедленно направляли свои тральщики, кото-

Адмирал Честер У. Нимитц

рые, успешно обезвредив мины, докладывали своему командованию в шифрованном виде стандартное сообщение: «Проверено. Мин нет».

Аналогичную операцию в 1942 г. провели американцы. Руководству США необходимо было определить направление главного удара японских вооруженных сил. Существовало два возможных варианта: Япония могла попытаться захватить расположенный в центральной части Тихого океана атолл **Мидуэй**, имевший важное стратегическое значение, или провести десантную операцию на Алеутских островах (район Аляски). США в тот период не располагали силами для отражения двух атак, и правильный прогноз действий японцев имел крайне важное значение для дальнейшего хода войны. Суть проведенной американцами операции заключалась в следующем: японский флот пользовался для шифрпереписки кодовыми книгами, частично раскрытыми американцами (в частности они знали кодовую комбинацию «опреснительная установка»).

В американских сетях связи несколько раз открытым текстом было передано сообщение «На Мидуэе сломалась опреснительная установка». Японская служба радиоперехвата на Тихом океане перехватила это сообщение и передала его в Японию, предварительно зашифровав. Американцы, перехватили эту криптограмму и проанализировав шифртекст, определили кодовую комбинацию, обозначающую Мидуэй. В дальнейшем контролируя японские сети связи, американцы отметили, что кодовая комбинация «Мидуэй» очень часто встречается в шифрпереписке японцев и сделали вывод, что главный удар Япония нанесет по Мидуэю, где и были сосредоточены почти все наиболее боеспособные силы США, имевшиеся на Тихом

океане. Сражение 4-5 июня 1942 г. при атолле Мидуэй закончилось тяжелейшим поражением Японии и изменило ход военных действий в пользу США (рис. 10.6).

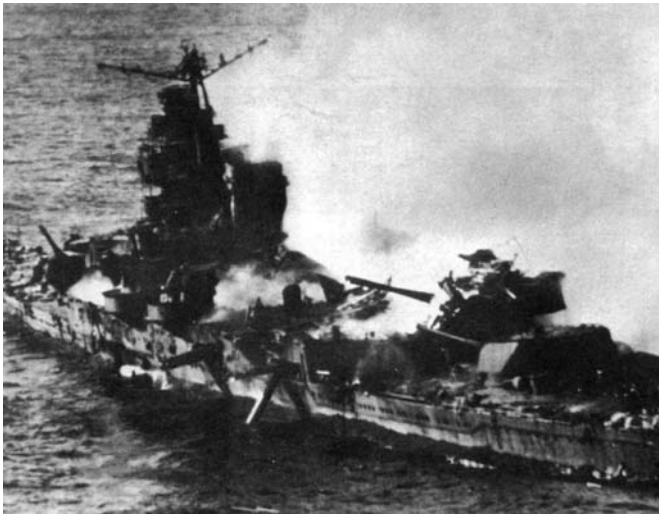


Рис. 10.6. **Японский крейсер, тяжело поврежденный в бою у Мидуэя**

Однако следует отметить тот факт, что подразделение радиоразведки ВМС США в Перл-Харборе дешифровало японский военно-морской код YN-25 еще накануне битвы в Коралловом море (начало мая 1942 г.) и представило в штаб командующего Тихоокеанским флотом США адмирала Честера У. Нимитца прогноз о возможных действиях японцев, но американское командование практически проигнорировало эту информацию и победа в сражении была одержана американцами, в основном, Благодаря цепи счастливых совпадений и ошибок японского командования. Между тем события развивались именно так, как и предсказала радиоразведка, и после победы в Коралловом море адмирал Нимитц стал доверять данным радиоперехвата, что во многом предопределило победу при Мидуэе.

Во время Второй мировой войны **советская разведка** также использовала игру в дезинформацию «под шифром». С этой целью, например, она провела операцию под названием «**Монастырь**». В военную разведку Германии («Абвер») был внедрен агент **Александр Демьянов** (псевдоним **«Макс»**). Он создал в Москве «антисоветскую группу», которая, используя шифры «Абвера», начала активно дезинформировать немцев. При этом использовались материалы, предоставляемые одним из руководителей шифровальной службы «Абвера» полковником Шмитом. Эта дезинформация привела к серьёзным для немцев последствиям во время Курской битвы и при проведении других операций советских войск. В Берлине были очень довольны работой «Макса» и внедренной с его помощью агентурой. 20 декабря 1942 г. адмирал Канарис лично поздравил своего московского резидента с награждением Железным крестом 1-й степени. А Михаил Иванович Калинин тогда же подписал указ о награждении Демьянова орденом Красной Звезды.

Во время Второй мировой войны дезинформацию немцев «под шифром» использовали и **советские партизанские отряды**. Так, руководитель одного из отрядов **Лавринович Эдуард Викторович** поддержал предложение о дезинформации немцев под шифром, в который были внедрены существенные слабости. Немцы этот шифр легко раскрыли. В результате они получили «подброшенную» партизанами информацию, на основании которой расправились со своими преданными слугами – бургомистром Прусовым и предателем Марченко.

В январе 1943 г. **американцы** повредили в бою японскую подводную лодку. Она села на мель около острова **Гуадалканал** в юго-западной части Тихого океана. Наиболее секретная информация, находившаяся на подводной лодке, заключалась в двухстах кодовых книгах. Экипаж закопал часть из них на побережье, занятом американцами. Узнав об этом, японское командование отдало приказ о бомбардировке и торпедировании побережья. Однако американцы проявили оператив-

ность и захватили кодовые книги. Американская дешифровальная операция **«Магия»** получила ценный материал для своей работы. Тайна же самой «Магии» тщательно охранялась. На всех секретных сводках «Магии» содержалось предупреждение: «Нельзя предпринимать никаких действий на основании сообщенной здесь информации, несмотря на временную выг., если такие действия могут привести к тому, что противник узнает о существовании источника».

В конце 1943 г. **немцы** подкупили камердинера британского посла в Анкаре **Эльяса Базна** (псевдоним **«Цицерон»**). «Цицерон» – псевдоним, пожалуй, одного из самых ценных агентов немецкой разведки в период Второй мировой войны. Этим агентом был албанец Эльяс Базна, который работал в Анкаре шофером первого секретаря британского посольства, а затем камердинером посла Великобритании в Турции. Он передал германской разведке фотокопии многих секретных документов. Они содержали достоверную стратегическую информацию. Однако Гитлер не придал ей должного значения. Более того, счел дезинформацией англичан. Базна передал немцам большое количество совершенно секретных документов, которые он извлекал из сейфа посла. Среди них был текст английской шифрованной радиотелеграммы, на полях которой остались очень важные пометки. Эти сведения оказались достаточными для того, чтобы дешифровальщики Германии раскрыли очень важный шифр англичан. Открытые тексты зашифрованных телеграмм посла Великобритании также были эффективно использованы немецкой дешифровальной службой. Однако в стратегическом плане ценнейшая информация не была использована. Полного доверия «Цицерон» у немцев не вызывал. Используя эти сведения, немцы впервые получили достаточно полную информацию об операции **«Оверлорд»** (открытие второго фронта в июне 1944 г., когда войска США и Англии вторглись в Нормандию). Однако немцы весьма своеобразно «отблагодарили» «Цицерона». Они расплатились с ним фальшивыми английскими фунтами, которые принесли агенту сплошные неприятности.

Аллен Даллес

В конце 1943 г. в английскую миссию в Берне (Швейцария) явился **немец**, представившийся ответственным работником МИД Германии. Он заявил, что привёз с собой чемодан, полный документов своего министерства. Однако англичане заподозрили провокацию и выставили посетителя за дверь. Немец обратился к американцам. Руководитель спецслужбы США в Европе **Аллен Даллес** быстро установил подлинность документов. «Если бы вы только видели эти документы, – писал он в Вашингтон, – в их первозданной свежести». Американцы поделились с англичанами своей находкой. Главную ценность представляли расшифрованные документы МИД Германии.

Англичане, осознав свой промах, передали эти материалы своим дешифровальщикам. Это позволило им увеличить эффективность дешифрования посланий МИД Германии. Немец и в дальнейшем успешно продолжал свою «чемоданную» деятельность.

В 1944 г. **агенты ФБР** США тайно проникли в контору **Амторга** (советское торговое представительство) и выкрали шифрблокнот. Это позволило им дешифровать некоторые материалы и вызвать шумиху вокруг якобы противозаконной деятельности представительства.

Агентурные проникновения в посольства порой имели негативный результат. Вот что пишет, например, генерал армии США **Джордж Маршалл** об одной из операций, проведённых американской разведкой в 1944 г. Руководил операцией начальник американской военной разведки в Европе **Уильям Донован**. Дж. Маршалл замечает: «Люди Донована, не поставив нас в известность, учинили «обыск» в служебных помещениях японского посольства в Португалии. Это привело к тому, что японцы сменили код, используемый военным атташе. Хотя с тех пор прошло уже более г., расшифровать но-

вый код нам ещё не удалось. Так что источник информации нами потерян, а ведь он давал возможность судить о положении дел в Европе».

В 1945 г. **агент внешней разведки СССР Руперт** являлся сотрудником американской криптографической службы. Он сообщил, что американцы читают шифрованную переписку МИД Японии с ее послом в СССР. Японский посол добивался от Москвы заключения договора о ненападении. Руководители спецслужбы СССР сочли возможным не мешать американцам. Читая документы, американские руководители убедились в том, что Москва ведет честную игру в отношении США.

Руперт, также сообщил о том, что американцы пытались решить задачу разгадки советского шифра, используя добытый код. Как сообщал Руперт, еще в феврале 1945 г. американцы бросили большие силы на расшифровку советских шифрованных телеграмм периода 1941–1942 гг., когда им удалось добыть одну незашифрованную телеграмму Амторга. Тогда же Руперт сообщил, что США были в курсе всех сообщений японского военно-морского флота, читая японские шифры. Благодаря этому их флоту своевременно становилось известно о планах и перемещениях японского флота и удавалось добиваться победы во всех последних сражениях на море с японцами. Кроме того, читая все телеграммы японского посла в Москве, они могли лишний раз убедиться в том, что Москва вела с ними честную игру, что касалось ее отношений с Японией [Феклисов, 1994].

10.5. Агентурные действия после Второй мировой войны

Предложенный читателю цикл очерков о специальных методах в криптографической деятельности, мы завершаем материалами об агентурных действиях после Второй мировой войны.

«Нас почитают обманщиками, но мы верны;
нас почитают умершим, но вот, мы живы;
нас казнят, но мы не умираем;
мы гонимы, но не оставлены;
мы неизвестны, но нас узнают…»
Из Второго послания апостола Павла к Коринфянам

Во время Великой Отечественной Войны в **СССР** были созданы специальные подразделения водолазов для разведывательно-диверсионных мероприятий в тылу противника. После окончания войны эти подразделения на Черном и Балтийском морях использовались для обследования потопленных немецких кораблей. Одной из главных задач при этом был подъем со дна **шифрмашин**, **кодовых книг** и других документов, относящихся к шифрованной связи.

На Черноморском флоте еще в апреле 1944 г. был создан разведывательный отряд особого назначения (РООН), состоящий из 10 человек. После взятия Севастополя водолазы-разведчики РООН проводили обследование потопленных немецких кораблей и изымали из них различные документы, представлявшие ценность для командования.

В дальнейшем водолазы взаимодействовали с агентурной разведкой, осуществляли поиск, подъем и обезвреживание донных магнитных мин, многократно привлекались к извлечению документов с потопленных кораблей, обследованию портов в целях обнаружения затонувших судов, заграждений и мин.

Решая все эти задачи, подразделение водолазов-разведчиков в полной мере оправдало свое название, проведя за период войны более 200 разведывательно-диверсионных операций с использованием легкого водолазного снаряжения (рис. 10.7).

К сожалению, не сумев по достоинству оценить перспективность этих подразделений, в октябре 1944 г. разведывательное управление ГМШ приняло решение о передаче этих подразделений и их имущества в аварийно-спасательную службу флота. Однако с таким решением были не согласны многие офицеры из руководства флота, они считали, необхо-

димым иметь на флотах и в мирное время подобные части и создать на базе подразделений школу водолазов-разведчиков.

Рис. 10.7. **Экипировка водолаза-разведчика**

В сентябре–октябре 1945 г. ГМШ инспектировал Балтфлот. Комиссия дала заключение: «Разведывательные отряды при разведотделе КБФ в мирное время иметь нецелесообразно».

В сентябре 1945 г. перебежал на Запад шифровальщик военного атташе СССР в Канаде старший лейтенант **Игорь Гузенко** (псевдоним «Кларк»). Ознакомившись с поступившей из Москвы телеграммой о своем досрочном откомандировании из Канады в СССР, он решил не возвращаться на родину. Вечером 5 сентября 1945 г. он похитил из сейфа своего шефа – военного атташе при посольстве СССР в Канаде полковника Николая Заботина (псевдоним «Грант») – папку с более чем сотней секретных документов и телеграмм.

Покинув посольство, Гузенко вместе с женой сразу же отправился в редакцию газеты «Ottawa Journal», полагая, что там сразу же ухватятся за одну из величайших сенсаций в истории журналистики. Оттуда перебежчика передали в руки представителей Канадской королевской конной полиции

Игорь Гузенко

(контрразведка) и британской разведки, которые и провели первоначальные допросы. На первом же допросе в управлении контрразведки Оттавы Игорь Гузенко, рассчитывая получить политическое убежище, выдал весь состав советской военной резидентуры и раскрыл нелегальных агентов. Данные о широкомасштабном атомном шпионаже ГРУ на территории США и Канады, подтвержденные секретными документами из сейфа советского военного атташе, потрясли английских и канадских экспертов [Агеева].

Премьер-министр Канады Макензи Кинг запретил на некоторое время давать какую-либо информацию о перебежчике в прессу. После изучения основных документов, украденных Гузенко, Кинг вылетел в Лондон чтобы подробно проинформировать английского премьер-министра о том, что произошло в Оттаве. Он также посетил Вашингтон, где встретился с президентом Гарри Трумэном, который уже знал о советском перебежчике.

Последствия предательства оказались катастрофическими. Комиссия выявила имена 19 агентов советской военной разведки, из которых 9 были осуждены. Наибольшие потери понесла агентурная группа «Бэк», ориентированная на сбор сведений по атомной бомбе.

В документах, переданных Гузенко, подробно описывались принципы шифрования, применявшиеся в НКГБ и ГРУ. Он также передал тексты секретных депеш атташе. Эти материалы, вместе с купленными у финнов трофейными шифрами, привели к дешифрованию шифров МГБ СССР в ходе уже упоминавшейся нами операции «Венона».

Заметную помощь СССР в локализации последствий дешифрования агентурной переписки оказал известный советский разведчик Ким Филби, руководивший к тому времени одной из

спецслужб Великобритании. Тем не менее, операция «Венона» дала существенные результаты. Так, на основе дешифрованных документов, англичане вышли на крупного советского разведчика Дональда Маклина (псевдоним «Гомер»). Однако Филби успел предупредить своего помощника Дональда Маклина, и тот в 1951 г. вернулся в СССР.

Дональд Маклин

Сегодня о Маклине и всей «Кембриджской пятерке» написано множество книг, сняты фильмы.

Маклин Дональд Дюарт родился 25 мая 1913 г. в Лондоне, по национальности шотландец. В 1934 г. окончил факультет политической истории и филологии Кембриджского университета. Во время учебы принимал участие в левом студенческом движении.

В 1934 г. попал в поле зрения советской разведки. Д. Маклин ответил согласием на предложение о сотрудничестве. С 1935 по 1951 г. работал в МИД Великобритании, где занимал ответственные посты. Работал в британских посольствах во Франции и Египте. В 1950–1951 гг. возглавлял американский отдел Форин-оффиса.

За годы сотрудничества с советской внешней разведкой передал ей большое количество совершенно секретных документальных материалов, в том числе шифрованную переписку МИД Англии со своими посольствами за границей, протоколы заседаний кабинета министров, планы США и Великобритании по вопросам использования атомной энергии в военных целях (http://svr.gov.ru/history/macd.htm).

Дешифрованные сообщения «Веноны» стали первыми наводками на семейную пару **Юлиуса** и **Этель Розенбергов**, обвиненных в атомном шпионаже и казненных на электрическом стуле в 1953 г.

Супруги Розенберг

Таким же образом англичане выявили советского агента **Клауса Фукса**, передававшего в СССР ядерные секреты. Он был осужден.

Клаус Фукс

Во всех этих случаях англичане и американцы в ходе следствия и суда тщательно скрывали основной источник информации – «Венону».

Следует особо отметить следующее обстоятельство. Шифры, используемые советскими агентами, отличались чрезвычайно высокой стойкостью. Защищаемая информация первоначально кодировалась, а затем перешифровывалась так называемой «гаммой одноразового использования». Однако при шифровании допускалось неоднократное использование одних и тех же ключей (кода и гаммы). Американцы установили этот факт, что позволило им дешифровать секретные агентурные сообщения даже без наличия ключей.

Гельмут фон Паннвиц

Приведем небольшой пример указанного способа шифрования. Пусть следует зашифровать слово «АТОМНАЯ». В книге кодов ему соответствует число 3856, а гамма шифра имеет вид 1349. Шифрование заключается в поразрядном сложении этих чисел по модулю 10. В этом случае получаем шифрованное «слово»: 4195. Этот шифр очень стоек, но ошибки при его применении свели эту стойкость «на нет».

Арестованный в 1945 г. ответственный сотрудник главного управления имперской безопасности Германии Гельмут фон Паннвиц передал советской контрразведке вскрытый немцами код, использовавшийся в переписке между Черчиллем и Рузвельтом.

Паннвиц был убежденным антинацистом и никогда не состоял в национал-социалистической рабочей партии. Он был противником идей расового превосходства, известным своей приверженностью христианским традициям и русофильскими взглядами. Подробно о Гельмуте Паннвице читайте в книге Виктора Филатова [Филатов, 2005].

Обложка книги Виктора Филатова

В феврале 1953 г. советская разведка завербовала сержанта армии США

Роберта Ли Джонсона, проходившего службу в Берлине. Джонсон работал писарем- регистратором в секретной части разведывательного отдела Берлинского командования армии США. Он передавал в распоряжение советской внешней разведки все, что могло интересовать ее о военных объектах в ФРГ, где нес службу.

Весной 1955 г. его перевели на службу во Францию, где он довольно быстро истощил свои информационные возможности, передав резидентуре в Париже все сведения об американской военной базе в Рошфоре, все действовавшие там инструкции и приказы, информацию о вооружении, а так же о служивших там американских офицерах и солдатах.

К середине 1956 г. контракт Джонсона с американской армией закончился, и он отбыл в США. Там связь с ним была восстановлена в начале следующего г., и после выполнения им отдельных заданий резидентуры ему предложили вновь поступить на армейскую службу и постараться попасть на одну из интересовавших нашу разведку американских ракетных баз. Служить его направили в Техас.

В соответствии с просьбой парижской резидентуры, в течение 1959 г. агента настойчиво направляли на то, чтобы он заключил новый контракт на службу в Европе. В результате к концу года Джонсон появился в Орлеане, где начался новый этап его сотрудничества с советской внешней разведкой, достигший своего апогея уже в следующем, 1962 г. – операция «Карфаген» [Павлов, 1999].

Позже он завербовал своего друга, курьера вооруженных сил США в парижском аэропорту Орли, **Джеймса Миткенбау**. Эти два человека имели возможность передавать важные

секретные материалы, среди которых наиболее существенными были ключевые блокноты к американским шифрам.

В 1965 г. Джонсон раскаялся в шпионаже и пришел с повинной в американскую контрразведку. Отбывая наказание в тюрьме, он был убит в 1972 г. своим собственным сыном во время свидания. Сын не простил своего отца за предательство.

В начале 1950-х годов советская разведка завербовала шифровальщика военно-морского атташе Англии в Варшаве Гарри Фредерика Хоутона (псевдоним «Шах»). За солидное вознаграждение он передал советской разведке значительное количество шифров военно-морских сил Англии.

В январе 1961 г. ушел на Запад завербованный ЦРУ подполковник польской разведки Михаил Голениевский (оперативная кличка в ЦРУ «Снайпер»). Он передал американцам 300 страниц микрофильмированных документов и выдал английской контрразведке Хоутона, которого арестовали в Лондоне вместе с любовницей Этель Элизабет Джи, работавшей вместе с ним старшим клерком в бюро учета и размножения секретных документов НИИ подводных исследований в Портленде. Произошло это во время передачи агентом в районе знаменитого лондонского Шекспировского театра «Олд Вик» секретных материалов нелегалу советской разведки Гордону Лонсдейлу (Конон Молодый). Вскоре были арестованы и связники Лонсдейла – Питер и Леонтина Крогеры, обеспечивавшие шифрованную связь нелегала с Центром.

В 1954 г. в АНБ США был разоблачен шпион, работавший на Голландию. Им оказался **Джозеф Петерсен**, сообщавший голландцам сведения о чтении американцами голландской дипломатической шифрпереписки. Тридцатидевятилетний Петерсен, бывший преподаватель физики, изучал криптоанализ на заочных военных курсах в 1940-1941 гг., а затем был взят в армейскую дешифровальную службу. После войны Петерсен занялся преподаванием криптоанализа на курсах повышения квалификации министерства обороны. В 1953 г. разработанная им программа обучения стала базовой в АНБ. После поимки Джозеф Петерсен сказал в свое оправда-

ние, что взял всего два секретных документа для подготовки к проведению занятий.

В ходе начавшегося следствия выяснилось, что во время Второй мировой войны Петерсен подружился с полковником Феркуилом, одним из лучших голландских криптоаналитиков. Вместе с Феркуилом Петерсен занимался вскрытием японского дипломатического кода. В этой области у Феркуила был значительный опыт, приобретенный им еще до войны. Через Феркуила Петерсен познакомился с Джакомо Стуитом, офицером связи голландского посольства.

После войны, когда Феркуил возвратился из США в Голландию, в своих письмах Петерсен рассказывал ему о методах преподавания криптоанализа и других деталях, которые, по мнению Петерсена, полезно было знать при создании в Голландии собственной криптоаналитической спецслужбы. Стуит оставался в Америке, и Петерсен продолжал поддерживать с ним дружеские отношения.

В то время для защиты своей дипломатической переписки голландцы применяли шифрмашины швейцарской фирмы «Хагелин». В 1948 г. Петерсен снял копии с двух секретных документов, в которых говорилось об успехах американцев по вскрытию голландских шифрмашин, присовокупил к этим копиям оригинал еще одного документа под названием «Криптоанализ шифрмашины «B-211» фирмы «Хагелин» и показал их Стуиту. Феркуил считал, что Петерсен не имел ни малейшего намерения нанести ущерб Соединенным Штатам, а просто руководствовался желанием помочь своим друзьям защитить родину от шпионажа других государств.

Осенью 1954 г. во время обыска квартиры Петерсена сотрудники ФБР обнаружили обе копии и оригинал. Это был первый серьезный случай нарушения закона сотрудником АНБ. Вероятно, именно поэтому министерство юстиции и министерство обороны приняли решение передать дело в суд, вместо того чтобы решить вопрос в административном порядке внутри АНБ. Возможно, они хотели сделать дело Петерсена показательным. Но, как сказал его адвокат, «приняв такое ре-

шение, они попали впросак», так как арест получил слишком широкую огласку в американской печати (http://www. rfcmd.ru/book_04/21).

Джозеф Петерсен был приговорен к 7 годам тюремного заключения, но в 1958 г. был освобожден досрочно. Главный довод защиты – Петерсен работал в интересах союзника США.

В.М. Петров

В 1954 г. остался в **Австралии** дипломат, сотрудник КГБ СССР **Петров Владимир Михайлович**. В начале своей службы в КГБ он был шифровальщиком, затем работал в советских посольствах в Швеции и Австралии. После расстрела Берии в 1953 г. Петров стал опасаться, что его заподозрят в причастности к заговорам Берии. Это и побудило его к побегу. С собой Петров захватил ряд документов, касающихся советской разведывательной деятельности в Австралии, которые рассматривались парламентской комиссией, но не были рассекречены австралийцами. Также он передал западным спецслужбам известные ему шифры и агентуру СССР. В 1956 г. Петров получил австралийское гражданство. Впоследствии Петров с женой жили в Австралии под изменёнными именами, не общаясь с журналистами.

В середине 1950-х годов ЦРУ и ФБР США завербовали одного ответственного сотрудника посольства Франции в Вашингтоне. С его помощью АНБ США длительное время контролировало французскую дипломатическую переписку, поскольку регулярно получало шифры Франции.

Аналогичную операцию против французского посольства американские спецслужбы провели в начале 1980-х годов. Был завербован французский разведчик, работавший в посольстве Франции в Вашингтоне. С его помощью были скопированы шифрдокументы посольства. АНБ США получило возмож-

Джордж Блейк

ность дешифровать дипломатические документы Франции. Франция не осталась в долгу. Её разведчики проникли в американское посольство в Африке и добыли американские криптографические документы.

В 1954–1955 гг. **американцы** и **англичане** построили на 7-метровой глубине специальный тоннель, позволивший им с территории Западного Берлина подсоединиться к линиям связи Москва-Берлин. Этой операции они присвоили название «Золото». Однако об этой акции узнали советские спецслужбы. Главную роль здесь сыграл офицер спецслужбы Англии Джордж Блейк, добровольно предложивший советской разведке свои услуги. Советское руководство решило провести игру с целью дезинформации противника. Никаких препятствий для перехвата не создавалось. Эта игра прошла успешно и закончилась в апреле 1956 г. В 1961 г., с помощью перешедшего на Запад сотрудника польской спецслужбы Михаила Голениевского, англичане арестовали Блейка и приговорили его к длительному тюремному заключению. Однако в 1965 г. Блейк бежал и оказался в СССР.

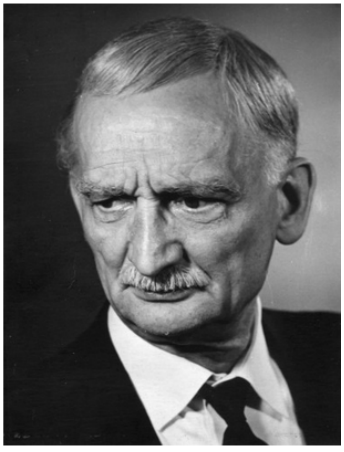
Интерес к делу и истории Блейка не спадает. Зарубежная, и прежде всего, конечно, английская, пресса часто возвращается к теме разведывательной деятельности Блейка, поскольку еще многие вопросы остались без ответа. Когда он стал советским разведчиком? Не был ли он уже в молодости внедрен в английские спецслужбы? Почему не оправдала себя система проверки при зачислении его на службу в Интеллидженс сервис?

Большое мужество проявил Джордж Блейк, опубликовав в 1990 г. свои воспоминания, когда его представления о про-

грессе социалистического общества подверглись столь жестокому испытанию нашей действительностью в период перестройки [Блейк, 2006].

Обложка книги Джорджа Блейка

Летом 1957 г. в результате предательства своего связного Реино Хейханена в США был арестован знаменитый советский разведчик Рудольф Иванович Абель (настоящее имя Вильям Фишер). В момент ареста в гостиничном номере Абеля находились шифрблокноты и расшифрованный текст, полученной накануне радиограммы из Центра. Обманув бдительность сотрудников ФБР, Абелю удалось уничтожить бумагу с принятым сообщением и действующий шифрблокнот, однако он не смог уничтожить шифрблокноты для следующих сеансов связи. Абелю удалось передать информацию о провале в советское посольство, поэтому воспользоваться захваченными шифрблокнотами в криптографическом плане американцам не удалось, но эти блокноты послужили важной уликой на суде по обвинению Абеля в шпионаже в пользу СССР. По другой версии шифровка из Центра для Абеля попала в руки американцев несколько ранее. Абель по ошибке расплатился с продавцом газет полой 5 центовой монетой, в которой хранилась шифровка. Продавец удивился тому, что монета слишком легкая и начал ее разглядывать, при этом он уронил монету и оттуда выпал листок с нанесенными на нем цифрами. Продавец газет отнес монету и шифровку в полицию, а оттуда она попала в ФБР, однако продавец не смог вспомнить от кого он получил монету, а дешифровать криптограмму американцы не смогли. Только после предательства



Р.И. Абель
(Вильям Фишер)

Хейханена, знавшего ключ к шифру, сотрудникам американских спецслужб удалось ознакомиться с текстом сообщения. Эта шифровка, вместе с другими документами, захваченными у Абеля, послужила уликой для обвинения в суде. Суд приговорил Абеля к 30 годам тюрьмы, но в феврале 1962 г. его обменяли на сбитого над СССР пилота разведывательного самолета U-2 Фрэнсиса Гарри Пауэрса.

После возвращения в СССР, лечения и отдыха Абель вернулся к работе в центральный аппарат внешней разведки и находился на боевом посту до конца своей жизни. Его заслуги были отмечены орденом Ленина, тремя орденами Красного Знамени, двумя орденами Трудового Красного Знамени, орденами Отечественной войны I степени, Красной Звезды и многими медалями. Скончался. Вильям Генрихович Фишер (Рудольф Иванович Абель) 15 ноября 1971 г., похоронен на Донском кладбище в Москве.

В начале 1960 г. шофер начальника секретариата АНБ США сержант Джек Э. Данлеп предложил свои услуги советской разведке. Услуги были приняты, и за поставленные материалы Данлеп получил шестьдесят тысяч долларов. Он передал советским спецслужбам подробные описания шифрмашин США, руководства по их эксплуатации и ремонту, ряд других документов.

Джек Э.Данлеп родился в 1928 г., и в дальнейшем связал свою судьбу с армией. За воинскую доблесть и преданность своему долгу во время войны в Корее его наградили орденом «Пурпурное сердце» и медалью «Бронзовая звезда». В 1958 г. Данлеп становится шофером генерал-майора Гаррисона Б. Ковердейла, начальника секретариата штаба АНБ. В его обязан-

ности входила доставка секретных документов в различные подразделения АНБ. Когда в 1960 г. Данлеп предложил продать документы АНБ, принявший его сотрудник ГРУ, работавший под дипломатическим прикрытием, сразу оценил открывшиеся перспективы и немедленно выплатил ему аванс, обговорив условия дальнейшей связи. Сведения, поступавшие от Данлепа, имели огромную ценность. Летом 1960 г. Данлеп неожиданно разбогател, но будучи отцом семерых детей, он постоянно нуждался в финансовых вливаниях. На полученные от ГРУ деньги он купил прекрасно оборудованную моторную крейсерскую яхту и несколько дорогих автомобилей. И хотя его оклад в АНБ составлял всего 100 долл. США в неделю, столь дорогие покупки никого не удивили. Первые подозрения в отношении Данлепа возникли в начале 1963 г., после того как он из опасения, что по окончании срока службы его могут перевести в другое место, решил стать гражданским служащим. Дело в том, что все гражданские служащие, поступавшие на работу в АНБ, проверялись на полиграфе (детекторе лжи). Во время такой проверки Данлеп признался «в мелких хищениях и фактах аморального поведения». В результате в отношении Данлепа было начато расследование, которое установило, чтоего расходы не соответствуют доходам.

Понимая, что кольцо вокруг него сжимается, Данлеп в июне 1963 г. попытался покончить с собой с помощью снотворного. Но эта попытка оказалась неудачной. Он повторил попытку самоубийства, используя револьвер, но вмешательство приятелей и на этот раз спасло ему жизнь. И лишь третья попытка удалась. 22 июля 1963 г. он подсоединил кусок резинового шланга к выхлопной трубе своей машины, второй конец просунул в щель переднего окна, завел мотор и отравился выхлопными газами. Через три дня его со всеми воинскими почестями похоронили на Арлингтонском национальном кладбище (http://www.agentura.ru/dossier/russia/gru/imperia/coldwar/).

Вполне возможно, что о предательстве Данлепа так никто бы никогда и не узнал, если бы через месяц после смерти его вдова не обнаружила в доме тайник с совершенно секрет-

ными документами, которые он не успел передать своему оператору. Она незамедлительно принесла их в АНБ. Началось расследование, установившее факт сотрудничества Данлепа с ГРУ [Млечин, 1991].

Кроме того разоблачению Данлепа способствовали сведения, полученные от агента в ГРУ (СССР) Дмитрия Полякова (с псевдонимами «Цилиндр» в ФБР и «Бурбон» в ЦРУ).

В ЦРУ Полякова называли бриллиантом, поскольку этот агент нанес вреда больше, чем все остальные перебежчики и предатели, вместе взятые – 25 лет на американцев работал генерал ГРУ Дмитрий Поляков. После его разоблачения и ареста следователи, скрупулезно подсчитывающие ущерб, нанесенный предателем, пребывали в некотором оцепенении – перед ними проходили цифры и имена в количестве, зашкаливающем за возможности агента-одиночки. В начале 1988 г. Военная коллегия Верховного суда СССР приговорила Полякова за измену Родине и шпионаж к расстрелу. Официально о расстреле Д.Ф.Полякова было сообщено в газете «Правда» в 1990 г.

В начале 1960-х годов офицер разведки ГДР Герберт З. (псевдоним «Кранц»), познакомился в Париже с молодой девушкой Гердой О. Она служила в шифровальном отделе МИД ФРГ. Вскоре они поженились. «Кранц» открылся Герде, и она под псевдонимом «Рита» стала работать на супруга. Три месяца она работала шифровальщицей в Вашингтоне, и, Благодаря ее деятельности, разведка ГДР была в курсе отношений США – ФРГ. В начале 1970-х гг. «Риту» перевели на работу в Варшаву. Там она влюбилась в журналиста – агента разведки ФРГ, и во всем призналась ему. Однако у нее хватило порядочности предупредить об этом «Кранца», который успел бежать в ГДР.

В те же 1960-е гг. офицер армии США Дж. Хелмич, имевший доступ к криптоматериалам, предложил советской разведке купить имеющиеся у него документы. За период с 1963 по 1966 гг. Хелмич продал техническую документацию, ключи, диски шифровальной машины и другие материалы. В общей сложности за свою работу он получил более 130 тыс. долл. США. Лишь в начале 1980-х годов Хелмич был разоблачен и осужден в 1981 г. на пожизненное заключение.

А.И. Лазарев

В начале 1960-х годов **советская** разведка провела операцию **«Карфаген»**, целью которой было агентурное проникновение в диспетчерский центр связи американского военного ведомства во Франции. В ходе этой операции удалось получить сведения о шифрах, используемых армией США и войсками НАТО. Руководил операцией резидент КГБ в Париже **Лазарев Анатолий Иванович.** В операции участвовал, уже упоминавшийся нами, сержант армии США Роберт Ли Джонсон, который и определил успех всей операции. Работая во внешней службе охраны, Джонсон сумел проникнуть в секретный сейф центра связи. Советская разведка разработала для него специальную аппаратуру для раскрытия шифра защиты сейфа. По оценкам американцев, этот человек нанес США «потери огромные и непоправимые». Подробно об операции «Карфаген» и ее участниках можно прочитать в статье Валентина Двинина [Двинин, 2006].

За операцией «Карфаген» последовала новая операция **советской разведки – «Олимп».** Этой операцией руководил начальник венской резидентуры КГБ Павлов Виталий Григорьевич. Объектом операции являлись посольства и представительства иностранных государств в Австрии. В ходе операции был завербован агент «N» – сотрудник австрийской государственной полиции, имевший доступ к секретным документам. К проведению операции был подключен ранее завербованный агент «Гермес», специалист в области электронной защиты иностранных посольств. «Гермес», в свою очередь, завербовал шифровальщика одного из иностранных посольств в Вене.

В результате операции были получены шифры этого посольства, что позволило советскому руководству сделать пра-

Роберт Ли Джонсон

вильные выводы о политике страны (под кодовым названием «Олимп») на международной арене.

Подробно об операции «Олимп» можно прочитать в книге генерал-лейтенанта Виталия Григорьевича Павлова, который 50 лет прослужил во внешней разведке КГБ. В своей книге он рассказывает об одной из наиболее засекреченных страниц деятельности этой организации: об операциях тайных физических проникновений на иностранные объекты, представляющие интерес для СССР [Павлов, 2010].

Министерство обороны **США** в августе 1960 г. вынуждено было официально признать, что два сотрудника американской радиоэлектронной разведки АНБ дешифровальщики **Бернон Фергюсон Митчелл** и **Уильям Гамильтон Мартин** по неизвестной причине не вернулись на работу из отпуска. Позднее выяснилось, что они пошли инициативно на контакт с КГБ в 1959 г. во время отдыха в Мексике. Оба сотрудника АНБ вскоре через Кубу перебрались в СССР, где попросили политического убежища и дали пресс-конференции с разоблачением деятельности АНБ по планомерному дешифрованию корреспонденции стран-союзников США. После этого Митчеллу и Мартину предоставили советское гражданство.

В дальнейшем судьбы Мартина и Митчелла сложились по-разному. В августе 1960 г. решением Политбюро ЦК КПСС № 295 им было предоставлено политическое убежище и ежемесячная зарплата в 500 рублей. Осенью Митчелл получил работу в институте математики при Ленинградском университете, а Мартин там же стал готовиться к защите докторской диссертации по статистике. Вскоре Мартин сменил фамилию на Соколовский и женился на девушке, с которой познакомился на черноморском курорте. Супругой Митчелла, стала Галина Владимировна Яковлева, тридцатилетняя помощница профессора Ленинградской консерватории.

Однако жизнь перебежчиков в СССР оказалась не такой, как они предполагали. И если Мартин сумел приспособиться, то у Митчелла дела обстояли хуже. Он не сумел адаптироваться к советской действительности и несколько раз обращался за разрешением выехать на Запад, в котором ему постоянно отказывали. В 1979 г. он в очередной раз обратился в американское консульство в Ленинграде за информацией о возможности вернуться в США. Однако госдепартамент США категорически отказался содействовать его возвращению и даже лишил его американского гражданства.

Обложка книги Виталия Павлова

В открытом письме американскому народу Митчел и Мартин особо отметили следующий факт: «В конце концов наше внимание привлек случай, когда правительство Соединенных Штатов заплатило деньги шифровальщику, работающему в посольстве одной дружественной страны в Вашингтоне, с тем, чтобы получить информацию, которая помогла в дешифровании шифрсообщений этого союзника» [Полмар, 1999]. Митчел и Мартин посчитали такие действия «аморальными и беспринципными».

В 1962 г. **советские** контрразведчики на Кубе зафиксировали работу агентурного передатчика, работавшего по принципу **«радиовыстрела»** (сверхбыстродействующая и узконаправленная передача – авт.). Кубинцы захватили агента, в результате чего в руки советских специалистов попал шифратор новейшей модификации.

В 1963 г. сотрудник **АНБ США,** американец ливийского происхождения **Виктор Норрис Гамильтон** (родился в Бейруте в 1919 г., настоящее имя Фузи Дмитрий Хиндали) попросил у **СССР** предоставить ему политическое убежище. Оно было ему предоставлено. Гамильтон назвал многие страны,

дипломатическая переписка которых перехватывалась и дешифровалась в АНБ. Эти данные были опубликованы и вызвали большой резонанс в политическом мире. В частности, в письме Гамильтона, опубликованном в газете «Известия» 23 июля 1963 г., были такие строки: «АНБ вскрывает шифры ближневосточных стран, что является прямым результатом криптоанализа. Вместе с тем АНБ получает и оригиналы шифров из каких-то секретных источников. Это означает, что кто-то ворует для американцев шифры. Особо следует подчеркнуть: американские власти пользуются тем, что штабквартира ООН находится на территории США. Зашифрованные инструкции Греции, Иордании, Ливана, ОАР и Турции своим представителям в ООН попадают в руки госдепартамента еще до того, как доходят до своих истинных адресатов…».

Олег Пеньковский

Помимо публикации письма, Гамильтон выдал все известные ему сведения о структуре АНБ, шифрах, имена руководителей и др. Вскоре КГБ были предприняты шаги по натурализации Гамильтона. Ему выдали паспорт с новым именем, присвоили псевдоним «Кир», предоставили квартиру на Комсомольском проспекте, определили приличное денежное содержание. Кроме того, к Гамильтону была приставлена круглосуточная охрана, так как считалось, что американцы начнут поиски перебежчика.

Вскоре у Гамильтона стали наблюдаться отклонения от нормального поведения, в результате в конце 1963 г. он был помещен в знаменитую «кремлевку» с диагнозом вялотекущая шизофрения, где провел около 10 лет. Позднее он был переведен в обычную психиатрическую больницу в Подмосковье, где впоследствии и скончался.

В мае 1963 г. в Москве состоялся суд над полковником ГРУ ГШ ВС СССР **Пеньковским Олегом Владимировичем**. Он был

Роберт Липка

приговорен к расстрелу за измену Родине: предатель успел передать ЦРУ США важные сведения о вооруженных силах СССР (в том числе и ядерном потенциале Советского Союза), а также информацию о деятельности **советских криптографических служб.**

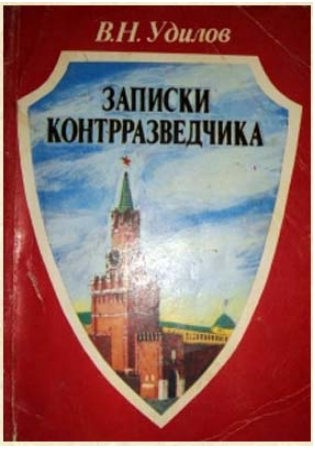
По официальным данным, его арестовали 22 октября 1962 г., в самый критический момент Карибского кризиса. Но он уже сыграл главную игру своей жизни. Суд установил, что с апреля 1961 г. по осень 1962 г. полковник Пеньковский отснял и передал в ЦРУ 110 кассет фотопленки – более 5 тыс. снимков документации, более 7 тыс. страниц секретнейших материалов. Военные эксперты НАТО отмечали, что полученная от Пеньковского информация привела к кардинальному переосмыслению всей стратегии НАТО в Европе и ее пересмотру. И практически все западные исследователи единодушно увязывают имя Пеньковского с ракетным кризисом вокруг Кубы в 1962 г.

С середины 1960-х гг. молодой сотрудник разведслужбы армии США, служивший в АНБ, **Роберт Стефен Липка** передавал важные секретные документы, зашифрованные в АНБ, **советской** разведке. Эти материалы представляли большой интерес для руководства СССР. Однако Липка продавал их достаточно дешево, не осознавая их важности.

Осенью 1965 г., Липка пришел в посольство СССР в Вашингтоне и предложил продать секретные материалы АНБ. Предложение Липки было незамедлительно принято. Связь с новым агентом, получившим псевдоним «Дан» (позднее «Рук» – шахматная ладья), поддерживалась с помощью тайников, в которых он оставлял материалы и забирал деньги – от 500 до 1000 долл. США за каждый пакет. Всего за период с 1965 по 1967 гг. с Липкой было проведено около 50-ти операций по связи, во время которых было получено более 200 важных документов

АНБ, ЦРУ, госдепартамента и других правительственных ведомств США. За время сотрудничества с советской разведкой Липка получил около 27 тыс. долл. США (http://fictionbook.ru/author/aleksandr_ivanovich_kolpakidi/delo_hanssena).

Липка был разоблачен лишь в 1993 г., когда на него донесла его бывшая жена, рассказав, что он работал на русских. По другим сведениям Липку выдал генерал КГБ **Олег Калугин**.



Обложка книги Вадима Удилова

Бывший сотрудник КГБ **Удилов Вадим Николаевич** в своих мемуарах описал историю тайного проникновения в здание посольства США в середине 1960-х гг. Как пишет в своей книге Удилов, пришлось предпринять весьма серьезные оперативно-технические действия. Операция заняла достаточно много времени. В последний момент, после вскрытия сейфа шифровальщика, возникла неожиданная проблема. Шифрблокноты были снабжены специальной защитой: каждый по краям обшит украинской вышивкой. Рисунок вышивки был составлен из переплетенных нитей пяти цветов. Пришлось прервать операцию и создать аналогичную вышивку. Затем операция вновь возобновилась. В конечном счете, удалось перлюстрировать несколько шифрблокнотов, не оставив улик.

В 1966 г. **ЦРУ** совместно с **АНБ США** провели уникальную операцию с целью дешифрования переписки посла ОАР (Египет и Сирия) в Монтевидео (Уругвай) с МИД ОАР в Каире. Вот что рассказал по этому поводу бывший сотрудник ЦРУ США **Филипп Эйджи**, принимавший непосредственное участие в этой операции: «Посольство ОАР пользуется изготовленной в Швейцарии (фирмой «Хагелин», рис. 10.8 – *авт.*) портативной шифровальной машиной… АНБ оказалось не в состоянии «расколоть» эту систему шифрования математиче-

ски, однако, располагает эффективным методом дешифрования… Смысл этого метода заключается в следующем. Если с помощью чувствительных приборов зафиксировать вибрацию шифратора во время его работы, то эта информация существенно облегчит дешифрование». Американцы провели тонкую агентурно-техническую операцию с целью регистрации вибрации с ножки стола, на котором располагался шифратор посольства. Шифрпереписка была дешифрована.

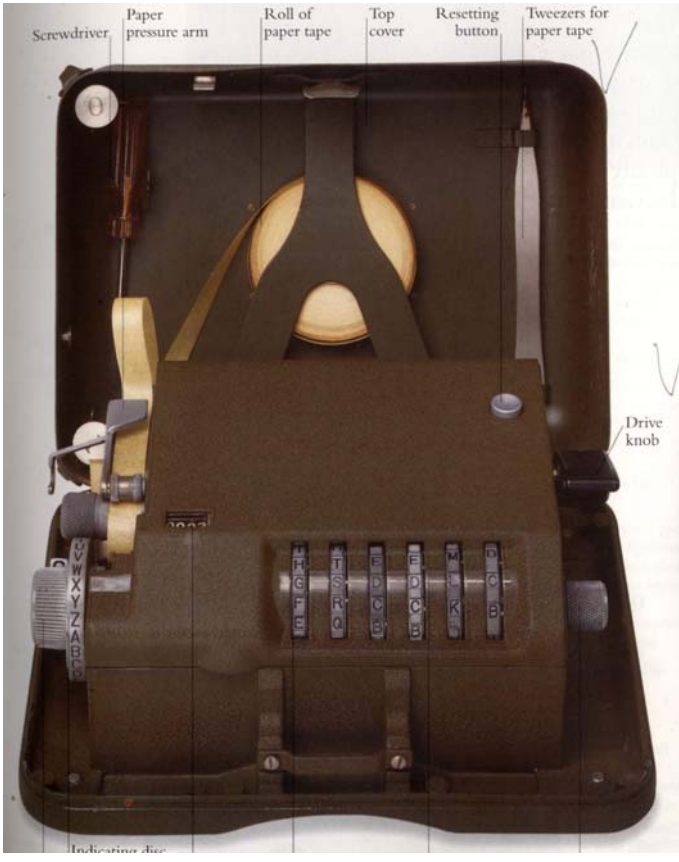


Рис. 10.8. **Шифратор фирмы «Хагелин»**

Филипп Эйджи

В 1977 г. Филипп Эйджи приобрел мировую известность, выпустив первую из своих книг «Inside the Company: Agents Dayry» (русский перевод «ЦРУ изнутри: Дневник агента», первое открытое издание 1977 г.). В книге, которая позже была переведена на 26 языков, приводился список американских агентов в Латинской Америке, занявший 22 страницы издания. В ответ правительство США объявило Эйджи предателем и заявило, что некоторые названные им агенты позже были убиты. В действительности же его считали причастным к гибели лишь одного сотрудника ЦРУ, резидента в Греции, чье имя действительно упоминалось в книге.

В связи с публикацией Эйджи в США был принят закон, предусматривающий длительное тюремное заключение и крупный штраф за разглашение подобных сведений.

В 1980-е годы Эйджи совместно с рядом других «диссидентов» из западных спецслужб, в частности, агентом ЦРУ испанцем Луисом Гонсалесом Матта, издавал международный журнал «Covert action» («Тайные операции»), в котором рассказывал о ставших достоянием гласности операциях спецслужб разных стран.

В начале 1968 г. в прибрежных водах **КНДР** было задержано американское судно радиоразведки **«Пуэбло»** (рис. 10.9). На борту находились специалисты-криптографы США, а также секретная техника, в том числе и шифраторы. Уничтожить аппаратуру и документы команда не успела. Северные корейцы получили важные материалы и аппаратуру, в том числе американские шифраторы KW-7, KWR-37, KG-14, а также ключи к ним. Эти сведения стали достоянием **советской криптографической службы** и дали импульс к дешифрованию военно-морской переписки США.

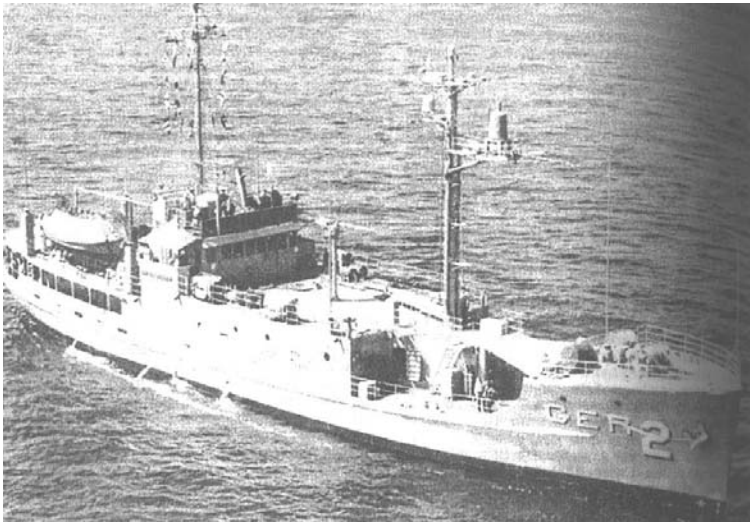


Рис. 10.9. **Американское судно радиоразведки «Пуэбло»**

В связи с операцией по захвату «Пуэбло» представляет интерес следующий факт. После того, как командир корабля сообщил, что не успевает уничтожить шифраторы и другую технику шифрования, руководители спецслужб США всерьёз обсуждали вопрос о потоплении корабля путем авиационного налета. Однако это предложение не было реализовано, так как группа захвата прикрывалась северокорейскими истребителями.

В начале 1968 г. **советской** разведкой был завербован на идеологической основе сотрудник АНБ США **Кристофер Бойтс**. Он занимался обслуживанием шифрованной связи с космическими спутниками США. Бойтс передал советской разведке ключи к шифрам, используемые АНБ США для связи со спутниками, а также копии сообщений, получаемых АНБ через спутники. В дальнейшем Бойтс, получил 40 лет тюрьмы и отбывал срок в федеральной тюрьме штата Колорадо США.

В 1968 г. **советской** разведкой был завербован сотрудник ШКПС (основной криптографический орган страны – *авт.*) Великобритании **Д.А. Прайм**. Он передал большое количест-

во материалов о деятельности английской криптографической службы.

Прежде чем приступить к своим агентурным обязанностям, Прайм провел неделю на квартире в Карлсхорсте (район в составе берлинского административного округа Лихтенберг – *авт.*), где его обучали работе с радиопередатчиком, технике шифровки сообщений, изготовления микроточечных донесений и работе с микрофотокамерой. Там же ему объяснили, как пользоваться «почтовыми ящиками». После каждого дня занятий его запирали в квартире на ночь. По завершении обучения, перед тем, как вылететь в Англию, Прайм, которому был присвоен псевдоним «Роулендз», получил «дипломат» с комплектом одноразовых шифрблокнотов, набором материалов для тайнописи и 400 фунтов наличными.

Первые 6,5 лет пребывания в ШКПС Прайм провел в лондонской группе обработки (ЛГО) – специальном дешифровальном подразделении, которое находилось в Сент-Данстанз Хилл. В ШКПС Прайма недолюбливали и считали человеком замкнутым и необщительным. Правда, по двум причинам он не вызывал подозрений. Во-первых, как потом с обезоруживающей простотой было написано в докладе комиссии по вопросам безопасности, «из-за специфики работы и потребности в персонале с узкой секретной специализацией в ШКПС брали немало неординарных и эксцентричных личностей» [Гордиевский, 1992]. Во-вторых, его замкнутость объясняли неудачной женитьбой и раздражением по поводу того, что повышение по службе вместо него получали более способные лингвисты.

Ни разу за 7,5 лет, которые Прайм проработал в ЛГО, с сентября 1968 по март 1976 гг., или за 1,5 г. работы в ШКПС в Челтнеме, с марта 1976 по сентябрь 1977 гг., он не попал под подозрение.

После ухода из ШКПС он устроился таксистом и виноторговцем и прервал контакт с КГБ на 3 года. Однако в 1980 г. КГБ возобновил связь с Праймом и убедил его встретиться со своим оператором в Вене, где Прайм передал КГБ больше пятнадцати кассет с пленкой и некоторые фотокопии и записи, которые он хранил у себя после ухода из ШКПС.

Уличили Прайма в шпионаже только после того, как он был арестован за развратные действия в отношении несовершеннолетних девочек летом 1982 г.

После ареста в 1982 г. ущерб, нанесенный Праймом, был «оценен» в 38 лет тюремного заключения. Этот случай стал причиной того, что в апреле 1984 г. правительство Маргарет Тетчер приняло решение о проверке всех сотрудников спецслужб на полиграфе. До этого англичане сопротивлялись давлению АНБ США, требовавших прохождение такой проверки для сотрудников ШКПС (следует отметить, что сотрудники АНБ подвергались периодическим проверкам на детекторе лжи).

Во второй половине XX в. *американцы* провели операцию по добыванию советских шифров, которая заслуживает отдельного внимания. В начале 1968 г. в Тихом океане погибла советская подводная лодка *К-129* (рис. 10.10). Американцы предприняли дорогостоящую операцию по ее подъему с большой глубины. Они не скрывали, что их основная задача – проникнуть в шифровальныйотсек подводной лодки.

Они рассчитывали обнаружить в нем шифры и ключи, имея которые смогли бы дешифровать радиообмен подводных лодок с берегом. Этот радиообмен они перехватили и записали ранее. Кроме того, они смогли бы детально ознакомиться с шифраппаратурой военно-морского флота СССР.

Только в середине 1974 г. специально созданное уникальное судно «*Гломар Эксплорер*» (рис. 10.11) подняло субмарину. Однако при подъеме она разломилась, и удалось поднять только носовую часть лодки. Американцы рассчитывали ознакомиться с советским шифровальным оборудованием, однако их постигла неудача. По одной из версий, командир этой лодки отличался очень высоким ростом, и по его просьбе капитанскую каюту расширили (чтобы туда уместилась его койка) за счет шифровального помещения, а шифроборудование перенесли в другой отсек, который остался в той части подлодки, которую поднять не удалось. Впоследствии судно «Гломар Эксплорер» использовалось для поиска древних затонувших кораблей.

Рис. 10.10. **Подводная лодка К-129**

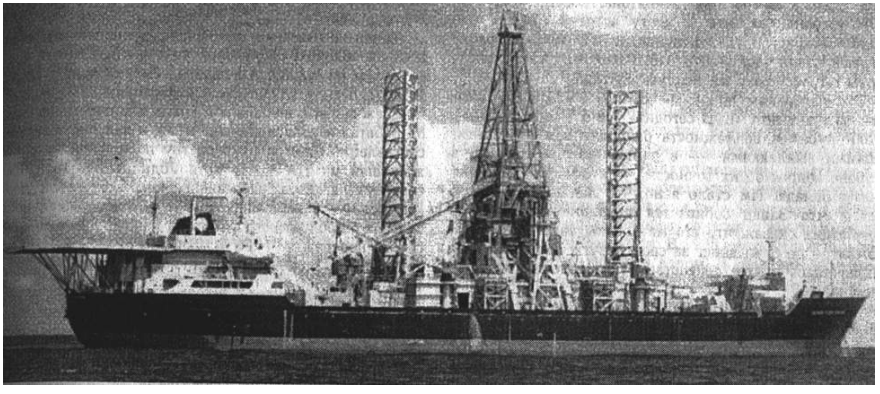


Рис. 10.11. **Судно для специальных подводных работ «Гломар Эксплорер»**

Питер Райт

Английский разведчик **Питер Райт** в своих мемуарах рассказал о том, как в 1970-х гг. английская контрразведка добывала шифрматериалы чехословацкого посольства в Лондоне. Однако через полгода чехословацкая контрразведка обнаружила факт утечки криптографических секретов, после чего этот канал утечки был ликвидирован.

А вот еще один эпизод, который описывает Питер Райт в своей скандально известной книге «Охотник за шпионами» (Spy Catcher, The Candid Autobiography of a Senior Intelligence Officer, Peter Wright with Paul Greengrass, Viking Penguin Inc.1987).

«В 1951 г. перед визитом американского госсекретаря в Москву технические специалисты Госдепартамента США проводили рутинную проверку кабинета своего посла. Они использовали стандартный перестраиваемый генератор сигналов для выявления средств подслушивания.

На частоте 1800 МГц был выявлен эффект акустической завязки. К их великому удивлению, в деревянном декоративном гербе США, который висел над рабочим столом посла, было обнаружено необычное устройство.

Однако настройка этой «Вещицы», как ее окрестили в тот момент, была очень нестабильной…»[Щелков].

На гербе был изображен белоголовый орел, прямо под клювом которого просверлено отверстие, позволявшее звуковым волнам достигать подслушивающего устройства. По началу, американские специалисты были просто обескуражены, не в силах установить, как оно работает: в нем не было источников питания, напрочь отсутствовали привычные радиодетали.

Эту непонятную находку весьма символично окрестили **The Thing –** «вещица» (рис. 10.12) или «нечто» (вполне подхо-

дит для названия современного фильма ужасов про вторжение пришельцев).

Рис. 10.12. **«Вещица»**

И только Питеру Райту незаурядному английскому специалисту по специальной технике удалось раскрыть принцип работы этой «вещицы». Впоследствии британская спецслужба воспроизвела копию этого устройства под названием «Сатир» для использования как английской, так и американской разведками.

Операцию по дешифрованию дипломатической переписки **англичане** провели в **египетском посольстве** в Лондоне. Это произошло накануне Суэцкой войны 1956 г. Франции, Англии и Израиля против Египта. Дешифрование египетских депеш позволило англичанам своевременно добывать информацию, весьма актуальную для стран – противников Египта. При этом англичане читали не только переписку Египта с посольством в Лондоне, но и с посольствами в Москве и других странах. Это позволило им быть в курсе советско-египетских отношений в этот критический период.

В 1973 г. **польская разведка** получила шифр одной из латиноамериканских республик. Этим приобретением она поделилась с СССР. Указанная страна представляла интерес

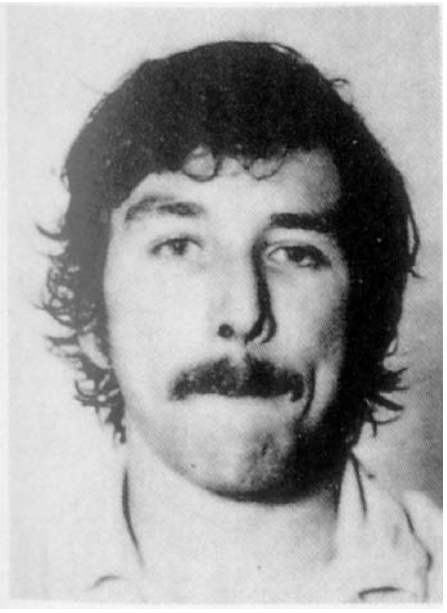
для советской разведки, поскольку было известно, что ЦРУ США использовало посольство этой страны в Москве для прикрытия действий американских разведчиков. Шифр вскоре был сменён, и возникла необходимость в приобретении новых шифров посольства. Советская спецслужба совместно с поляками провела акцию проникновения в посольство этой страны в Варшаве. Необходимые шифрдокументы были получены. Сотрудничество советской и польской разведок было продолжено. Были осуществлены проникновения в варшавские посольства других стран (операция **«Гренада»** и др.).

Интересный эксперимент провели специалисты криптографической службы **СССР** в 1973 г. во время эвакуации советского посольства из Чили. Перед эвакуацией шифраторы посольства были «надежно» разрушены. «Останки» были привезены в Москву. Специалисты в короткое время восстановили эти шифраторы. Методы уничтожения шифраппаратуры в критических ситуациях были серьёзно модифицированы.

В 1975 г. **советской** разведкой был завербован сотрудник АНБ США **Кристофер Бойс**. Он передал советской разведке материалы с фотокопиями ключей для американских шифрмашин. Информация, предоставленная Бойсом, в значительной мере раскрыла многие стороны деятельности АНБ и способствовала принятию мер по более надежной защите линий связи СССР.

В январе 1977 г. при попытке забросить пакет на территорию советского посольства в Мехико был задержан некий **Эндрю Ли**. При обыске у него нашли секретные документы калифорнийской компании TRW, которая вела разработку одной из самых сложных спутниковых станций перехвата «Рионит».

Эти документы передал Ли именно Бойс, который был его другом. Бойс имел доступ в специальную экранированную комнату, в которой были установлены шифраторы для связи со штаб-квартирой ЦРУ и АНБ. Ли и Бойс признались, что в обмен на такого рода документы советская разведка предлагала им наркотики.



Кристофер Бойс после ареста (слева) и Эндрю Ли (справа)

Изучение полученных материалов привело советских специалистов к выводу о том, что «Рионит» способен осуществлять из космоса перехват в диапазоне ВЧ и СВЧ, в том числе и телеметрическую информацию с запущенных ракет. Советская сторона немедленно начала шифровать свои телеметрические сигналы. В результате следствия выяснилось, что Бойс и Ли работали на советскую разведку 2 года. Бойс получил 40 лет тюрьмы, а Ли – пожизненное заключение.

В конце 70-х годов шифровальщик посольства США в Боготе **Джеффри Барнетт** продал сотруднику советской разведки за 100 тыс. долл. США копии открытых текстов шифртелеграмм резидента ЦРУ в Колумбии. Сопоставление копий с соответствующими зашифрованными вариантами позволило советским криптоаналитикам пробить такую брешь в системе обеспечения безопасности связи американского посольства, что залатать ее можно было только с помощью полной замены по-

Ричард Никсон

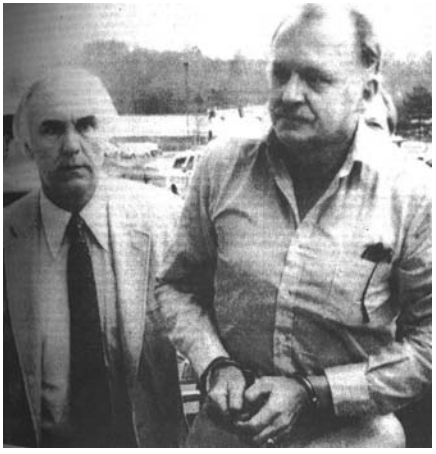
сольских шифровальных машин. Выдал Барнетта в июне 1979 г. завербованный резидентурой ЦРУ в Джакарте подполковник КГБ **Владимир Пигузов**. Барнетта приговорили в США к 18 годам тюрьмы (в 1990 г. его отпустили на поруки), а Пигузова в СССР – к расстрелу.

В 1970-е гг. *американские спецслужбы* активизировали оперативно-агентурные мероприятия по проникновению в здания иностранных посольств. По этому поводу 29-летний помощник президента США Ричарда Никсона *Т. Хьюстон* высказался весьма откровенно: «Мы тратим миллионы долларов на раскрытие иностранных кодов с помощью машин. Один удачный взлом бесплатно решит задачу».

В середине 1970-х гг. *советская* разведка, используя подкуп, завербовала шифровальщика японского МИД (псевдоним *«Назар»*). Помимо передачи проходивших через его руки секретных посланий МИД Японии, «Назар» поставлял информацию, позволявшую советским криптоаналитикам быстро замечать и разгадывать изменения в японских дипломатических шифрсистемах. Объем документов, поставляемых «Назаром», был так велик, что возникли проблемы с их оперативным переводом.

Чрезвычайно важную информацию о деятельности АНБ США передал *советской* разведке сотрудник АНБ США *Рональд Пелтон*, проработавший в этой организации 14 лет. Этот шаг он предпринял с единственной целью – заработать деньги. В 1979 г. он предложил свои услуги советской разведке. Именно он раскрыл одну из уникальнейших операций АНБ по съёму информации с подводного кабеля секретной связи СССР в Охотском море. Эта операция получила кодовое наименование *«АЙВИ БЭЛС»*. В середине 1980-х гг. он был разо-

блачен и приговорен к 3-м пожизненным срокам заключения. В приговоре суда отмечалось, что Пелтон нанес стране «неоценимый ущерб».



Рональд Пелтон (справа)

Одна из крупнейших агентурных акций *советской* разведки, связанных с добыванием криптографических сведений, была проведена при помощи офицера ВМС США **Джона Уокера**. Уокер, имевший доступ к сверхсекретным криптоматериалам, жил не по средствам и постоянно нуждался в деньгах. В конце 1960-х гг. он предложил свои услуги советской разведке. Он сумел организовать целую шпионскую группу, в которую входили его сын **Майкл Уокер**, его брат капитан-лейтенант **Артур Уокер** и друг Джона Уокера – старший радист **Джереми Уитворт**. Все трое служили в ВМС США. Эта группа передавала СССР, используя миниатюрную фотокамеру (рис. 10.13), действующие ключи шифров ВМС США, описания шифрмашин, инструкции, секретные сообщения, подлежавшие шифрованию и полученные после расшифрования Группа проработала около 18 лет.

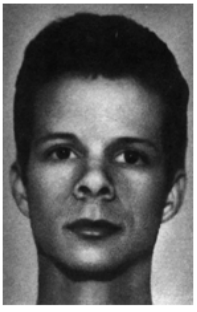
Рис. 10.13. **Миниатюрная фотокамера, которой пользовался Дж. Уокер**

Джон Уокер

В начале 1980-х гг. Джереми Уитворт, служивший на атомном авианосце **«Энтерпрайз»**, передал СССР через Джона Уокера ключи от шифров корабельной компьютерной системы военно-морского флота США. Сама система компьютерной защиты была несовершенной, и это позволило получить важные секретные материалы. По оценке американских спецслужб с помощью переданных СССР материалов русские дешифровали более 1 млн американских секретных сообщений. Джон Уокер был разоблачен в 1985 г. с помощью его жены-алкоголички Барбары. Вслед за этим была раскрыта и вся группа. Джон Уокер был приговорен к пожизненному заключению, а его сын к 25 годам тюрьмы. По другой версии Джона Уокера выдал, уже упоминавшийся нами в связи с делом Липки, Олег Калугин. По оценкам американских специалистов, Джон Уокер «продал КГБ военные секреты, которые дали русским возможность расшифровать примерно один миллион депеш во время Вьетнамской войны».

Джереми Уитворт

Артур Уокер



Майкл Уокер

В завершение описания этого эпизода приведём выдержки из интервью американского корреспондента Пита Эрли с генерал-майором КГБ СССР в отставке **Борисом Александровичем Соломатиным**. Генерал-майор Борис Александрович Соломатин 37 лет проработал в советской внешней разведке. Был резидентом в Дели, Риме. Возглавлял резидентуры в двух важнейших для КГБ точках – в Нью-Йорке и Вашингтоне. Бывший заместитель начальника 1-го главного управления КГБ СССР – предтечи Службы внешней разведки. Вышел в отставку в 1988 г. Соломатин в 1960–1970-х гг. был резидентом разведки КГБ СССР в США. Именно он играл главную роль в «обработке» Джона Уокера. В интервью, данном в апреле 1995 г., Соломатин вспоминает: «Джон Уокер по собственной воле пришел в посольство СССР в Вашингтоне… Он ничего не говорил о любви к Советскому Союзу… Он ясно сказал, что хочет денег. Уокер предлагал нам шифры, а это самый важный объект разведки».

На вопрос о том, не возникли ли подозрения о том, что Уокер – двойной агент, Соломатин ответил: «Я не знал тогда и сейчас всё ещё не знаю ни одного примера, когда какая-нибудь контрразведка использовала в качестве двойного агента челов., имеющего доступ к шифровальному делу. Шифры и шифровальная техника (рис. 10.14 – *авт*.) слишком важны и слишком секретны, чтобы кто-нибудь стал рисковать ими, даже если используются ложные шифры». Далее он продолжает: «Более семнадцати лет Уокер обеспечивал возможность читать наиболее важные военные секреты. В истории шпионажа последнего времени, пожалуй, не было провала в области безопасности связи такого масштаба и такой продолжительности во времени».

В 1980 г. на сторону **американцев** перешел майор **Шеймов Виктор Иванович**, сотрудник 8-го главного управления КГБ СССР. Шеймов был специалистом по обслуживанию технических систем защиты информации в советских посольствах за границей и в зарубежных резидентурах КГБ.

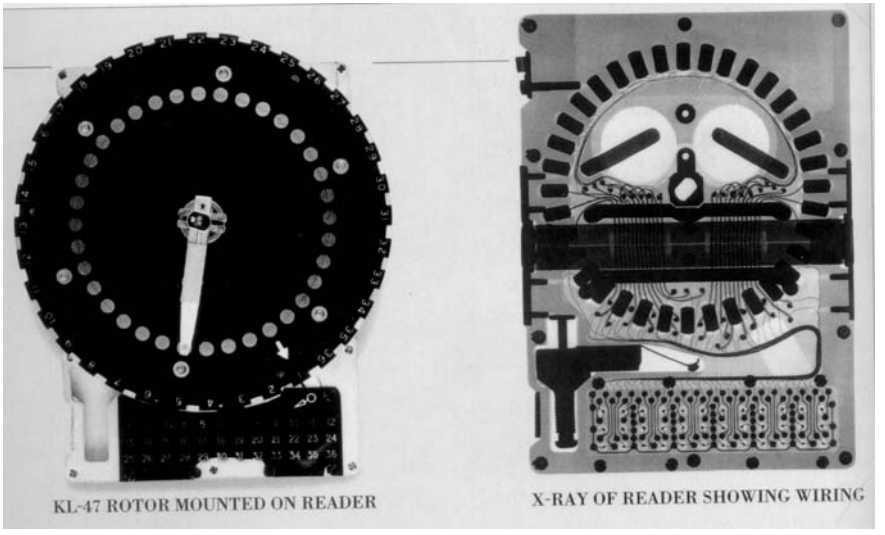


Рис. 10.14. **Детали шифроборудования, сведения о котором Дж. Уокер передал советской разведке**

По имеющимся в открытых публикациях данным, в 1979 г. в Варшаве он самостоятельно вступил в контакт с сотрудниками спецслужб США, а уже в середине мая 1980 г. сотрудникам ЦРУ удалось благополучно вывезти Шеймова, его жену и пятилетнюю дочь прямо из Москвы.

Он передал американцам весьма ограниченные известные ему сведения о работе криптографической службы СССР. Серьёзных последствий для СССР это предательство не повлекло. Оценивая предательскую деятельность Шеймова, начальник 8-го ГУ КГБ СССР Н. Н. Андреев в газетном интервью отметил: «Шеймов был рядовым сотрудником, допущенным к весьма ограниченному кругу служебных секретов. Некоторое время он занимался обслуживанием шифровальной техники, а затем был переведен в подразделение, ведущее строительно-монтажные работы в совзагранучреждениях ... после его исчезновения мы позаботились о безопасности тех точек, где бывал Шеймов ... И все же, на мой взгляд, предательство

Шеймова бросило определенную тень на сотрудников «восьмерки». А эти люди, поверьте мне, хоть и молоды, но честные и бескорыстные. До Шеймова иностранные разведки тоже пытались соблазнить, переманить на свою сторону наших шифровальщиков… Но в последнее время такие попытки участились. Так, наши шифровальщики в США, вернувшись из городского магазина, обнаружили в кармане конверты, в которых были приглашение к предательству и аванс за соглашение – бриллиант».

В 1982 г. в ЮАР был арестован начальник военно-морской базы в Саймонстауне командор (капитан первого ранга) **Дитер Феликс Герхард**. Ранее он был военно-морским атташе ЮАР в Лондоне. Герхард был завербован **КГБ СССР** в 1965 г. и имел доступ к информации центра электронной разведки в Сильвермайне, а также к данным о каналах обмена информацией между западными разведками, и к **кодам НАТО**. Вся эта информация стала известна спецслужбам СССР, которые этой информацией воспользовались.

В начале 1980-х годов советской разведкой с помощью разведуправления МГБ ГДР был завербован сержант армии США **Джеймс Холл**.

Холл в 1982 г. проходил службу в западном Берлине, вышел на связь с ПГУ КГБ СССР и предложил свои услуги – информацию по базе радиошпионажа в Тойфельсберге (рис. 10.15), где имел доступ к сверхсекретной информации.

С 1983 г. Холл также начал сотрудничать со Штази (министерство государственной безопасности ГДР – *авт.*). После четырех лет работы восточногерманская разведка решила отметить его заслуги вручением медали «За боевые заслуги» министерства госбезопасности ГДР и 5 тыс. долл. США. За 4 года службы в Тойфельсберге Холл передал Штази и КГБ сотни сверхсекретных документов, в том числе информацию по проекту «Троян» – мировой сети электронного наблюдения, которую в военное время можно было использовать для определения местонахождения бронетехники, ракет и самолетов путем записи передач их раций. Кроме того, в результате дея-

тельности Холла была выведена из строя компьютерная программа, которая имела целью определение слабых мест в системе советских военных коммуникаций.

Рис. 10.15. **Тойфельсберг, Берлин. Центр радиошпионажа 1951–1990 гг.**

В 1984 г. Джеймс Холл поступил в полное распоряжение Штази. В апреле 1985 г. его перевели в группу разведки в форт-Монмут (Нью-Джерси), и он возобновил связь с КГБ.

В феврале 1988 г. Холл окончил школу уорент-офицеров (категория приравнивается к российским прапорщикам – *авт.*) и был направлен в разведывательный отдел 24-й пехотной дивизии, где его связь с КГБ прервалась. К тому времени от КГБ и Штази, в общей сложности, он получил 300 тыс. долл. США. В декабре 1988 г. Холл был взят с поличным американской контрразведкой, сотрудники которой представились ему агентами КГБ, решившими восстановить связь. В 1989 г. Холл был приговорен к 40 годам пребывания в военной тюрьме США форт-Ливенуорт.

В середине 1980-х гг. **израильской** разведке **«Моссад»** удалось завербовать помощника военного атташе посольства Сирии в Лондоне Халеда. Последний продал посольские шифры, и израильтяне начали свободно читать всю

Джонатан Поллард

посольскую переписку. Халеду не хватало регулярных выплат «Моссада». Пользуясь своим положением, он «позаимствовал» из сейфа посольства 15 тыс. долл. США. Прикрывая своего агента, израильтяне возвратили деньги, но предупредили Халеда, что они будут вычитать из его денежного вознаграждения некоторые суммы выплат до погашения долга. Если же Халед совершит в посольстве еще хотя бы один противозаконный проступок, его убьют. Халед подчинился приказу, и после этого случая больше не «заимствовал» ни цента.

В 1980-х гг. агент ГРУ *СССР* **П. Ангелов** стал связником завербованной сотрудницы шифровального центра премьер-министра Канады **Макензи Кинга**. Она влюбилась в Ангелова и передавала ему секретные материалы, проходившие через нее. Все было бы хорошо, если бы Ангелов не пожаловался в Центр: «Она все время целоваться лезет». Из Центра последовал лаконичный ответ: «Если для дела нужно, то и ведьму поцелуешь. Приказано – целуй».

В конце 1985 г. **американские** спецслужбы арестовали **Джонатана Полларда**, еврея по национальности, сотрудника шифровальной службы американских ВМС. Поводом для ареста явилось обвинение в шпионаже в пользу Израиля. В результате расследования выяснилось, что Поллард крал и передавал Израилю все, что попадалось ему под руку: коды американского военного флота; сведения о средствах радиоразведки США; данные о частотах, на которых американские военные и шпионские ведомства передавали информацию и прочие сведения. Поллард был приговорен к пожизненному заключению. Однако под давлением всемирных еврейских организаций прези-

дент США Клинтон в 1994 г. принял решение о том, что Поллард заслуживает сокращения срока наказания, поскольку шпионил в пользу дружественной державы.

Ф.Д. Бобков

В конце 1980-х гг. советские контрразведчики обнаружили американское подслушивающее устройство в пункте сосредоточения кабелей связи секретных телефонных переговоров. Американским разведчикам удалось установить его на значительном расстоянии от Москвы, под землей – в распределительном колодце, где сходились линии правительственной связи и оперативной связи КГБ СССР. В этом колодце была установлена аппаратура, способная записывать телефонные переговоры на магнитную ленту. Сотрудники ЦРУ США извлекали из колодца кассеты с записью и устанавливали чистые. По этому поводу один из бывших руководителей КГБ СССР Бобков Филипп Денисович писал: «Это был несомненный успех американских спецслужб, свидетельствовавший о профессионализме сотрудников разведки, работавших в Москве».

Рис. 10.16. **Китайский истребитель J-8**

1 апреля 2001 г. над Южно-Китайским морем в районе острова Хайнань произошло столкновение китайского истребителя J-8 (рис. 10.16) и **американского самолета радиоэлектронной разведки EP-3E**. Вероятно, американский самолет вел слежение за новейшими кораблями ВМС Китая – эскадренными миноносцами российской постройки (проект 956Э «Современный»), а китайский истребитель пытался ему помешать. В результате инцидента китайский самолет упал в море, пилот погиб, а американская машина получила серьезные повреждения и совершила вынужденную посадку на китайском военном аэродроме на острове Хайнань. Китайская сторона утверждала, что столкновение произошло в ее территориальных водах, американцы говорили о международном воздушном пространстве. В руки китайских специалистов попала новейшая аппаратура электронного наблюдения и различное **криптографическое оборудование**. На самолетах подобного назначения устанавливаются самые совершенные шифраторы, а также различная аппаратура для обработки перехваченной информации. Экипаж самолета из 24-х человек, среди которых 8 профессиональных криптографов, не успел до посадки уничтожить секретные блоки аппаратуры, как того требует инструкция. Несмотря на требования США о немедленном возвращении самолета и экипажа, китайские военные подробно изучили все системы и аппаратуру самолета, а также допросили членов экипажа.

Эти мероприятия позволили китайской стороне получить важную информацию о методах работы и технических возможностях аппаратуры электронной разведки США и применяемом американцами криптооборудовании. Описанный эпизод по своему значению можно сравнить с захватом судна «Пуэбло», о котором было рассказано ранее. Экипаж был отпущен в Америку через несколько недель после инцидента, а самолет возвращен США в разобранном виде через несколько месяцев. Следует отметить, что это был первый случай попадания сверхсекретного американского самолёта в руки потенциального противника, хотя американские самолеты радиоэлек-

тронной разведки с конца 1950-х гг. вели полеты вдоль границ СССР (России), Китая, Северной Кореи и других стран, нередко вторгаясь в их воздушное пространство. Всего американцы потеряли в разведывательных операциях более 200 пилотов и членов экипажей. Отмечено, по крайней мере, два случая уничтожения самолетов электронной разведки.

Рис. 10.17. **Американский самолет радиоэлектронной разведки EP-3E и фрагмент повреждений, полученных им в результате столкновения с китайским истребителем**

2 сентября 1958 г. советскими истребителями был сбит самолет **C-130A-II «Hercules»**, он упал и сгорел в 55 км северо-западнее города Еревана, все 17 членов экипажа погибли. В сентябре 1997 г. директор АНБ генерал-лейтенант Кеннет Майнихэн около штаб-квартиры Агенства (рис. 10.18) открыл памятник экипажу этого самолета. 15 апреля 1969 г. северокорейские истребители сбили самолет **EC-121M «Warning star»**, он упал в море, погибло 13 человек. В обоих случаях ни совет-

ским, ни северокорейским специалистам не удалось получить доступ к оборудованию сбитых самолетов.

Рис. 10.18. **Штаб-квартира АНБ**

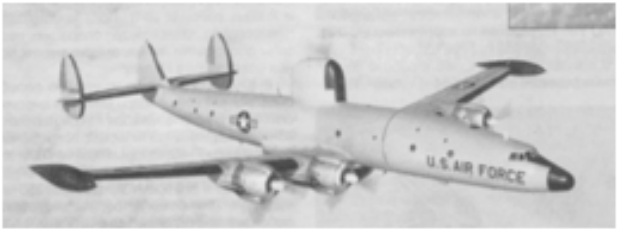


Рис. 10.19. **Самолет радиоэлектронной разведки EC-121**

По сообщению программы «Время» 5 февраля 2002 г., в ноябре 2001 г. на Дальнем Востоке в одной из частей 11-й армии ВВС и ПВО **России** было похищено несколько **блоков спецсвязи «воздух-земля»**, установленных на истребителях **Су-27**. Официальные лица заявили, что похитители выявлены, однако сами блоки не найдены. Неизвестно также, кому они предназначались. Ранее спецслужбы США пытались ознакомиться с криптооборудованием, установленным на советских самолетах.

Одна из таких попыток увенчалась успехом 6 сентября 1976 г. В этот день летчик одного из авиаполков ПВО, базиро-

вавшихся на Дальнем Востоке, старший лейтенант **Виктор Беленко** угнал в Японию истребитель-перехватчик МиГ-25. Беленко взлетел с аэродрома Чугуевка для выполнения обычного тренировочного полета. Отклонившись от маршрута МиГ, перешел на малую высоту, став невидимым для радаров, и через некоторое время приземлился на японском аэродроме **«Хакодате»**. Несмотря на требования СССР о немедленном возвращении самолета и летчика, японская сторона всячески затягивала переговоры по этому вопросу. Японские и американские специалисты разобрали самолет и изучили его. Особый интерес у американцев вызвало **криптооборудование**, используемое в аппаратуре государственного опознавания. Через некоторое время самолет был возвращен в СССР, а летчику было предоставлено политическое убежище в США.

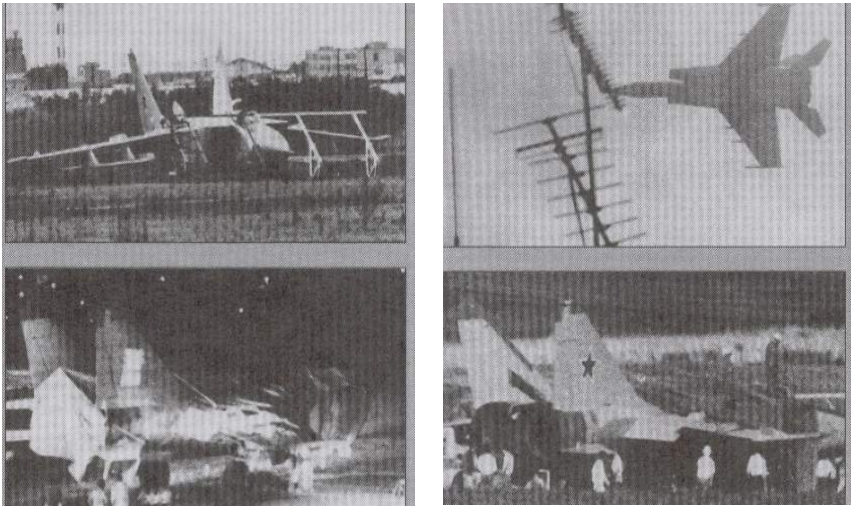


Рис. 10.20. **Фотографии МиГ-25, угнанного Виктором Беленко, на японском аэродроме «Хакодате»**

Советскому Союзу пришлось потратить значительные средства на смену аппаратуры государственного опознавания на своих самолетах. Вместе с тем это событие ускорило посту-

пление на вооружение новой модификации МиГ-25 с новым радаром и улучшенными характеристиками, а также позволило продать самолеты старой версии союзникам СССР.

20 мая 1990 г. летчик 176-го Гвардейского истребительного авиаполка капитан **М. Зуев** угнал истребитель МиГ-29 в Турцию. Несмотря на настойчивые просьбы американцев, турецкая сторона не позволила им ознакомиться с самолетом, поэтому в отличие от описанного ранее случая с МиГ-25, это происшествие не нанесло большого ущерба безопасности СССР. Самолет был возвращен, а летчик получил политическое убежище в США.

Следует отметить, что захват носителей секретной информации не всегда приводит к ее дешифрованию. В качестве примера приведем следующий эпизод. 2 марта 2003 г. **итальянская полиция**, во время спецоперации против террористической группировки **«Красные бригады»**, захватила несколько компьютеров, однако ознакомиться с содержащейся в них информацией не удалось, так как она была зашифрована с помощью известной криптосистемы PGP (Pretty Good Privacy), ключи же были вовремя уничтожены террористами. Итальянцам не помогло даже обращение за помощью к ФБР США, специалисты этого ведомства также не смогли вскрыть шифр. Интересно отметить, что создатель PGP **Фил Циммерман** отказался сотрудничать со следствием, заявив, что право людей на частную жизнь выше интересов государства.

Этим эпизодом мы заканчиваем свой цикл очерков о специальных методах в криптографической деятельности. Авторы в своих очерках сделали первые шаги в попытке методичного изложения вопросов проникновения в криптографические секреты противника на примерах исторических фактов прошлого.

В мире произошло существенное ослабление контроля над криптографией. Развитие электронной торговли, признания права людей на защиту неприкосновенности их частной жизни, стремление повысить безопасность в Интернете – все это стало причиной широкого распространения криптографических методов защиты. Страны, которые развивают элек-

тронную торговлю, убедились, что шифрование можно эффективно использовать при заключении сделок.

На сегодняшний день приходится констатировать неутешительный факт наличия отставания России в области развития технологий защиты информации. И это действительно отставание в развитии, но не в технологиях. Закрытая криптография традиционно высоко развитая в СССР, заложила прочные основы развития открытой криптографии в современной России. Между тем технологии защиты информации являются привлекательными с точки зрения инвестиций как российских, так и зарубежных компаний, что подчеркивается все возрастающим спросом на специалистов в этой области.

Сегодня для России является важным не только преодоление технологического разрыва в области телекоммуникаций с ведущими мировыми державами, но и сохранение за собой приоритетов в тех областях, развитие которых либо не уступает Западу, либо даже превосходит его.

Необходимость изучения агентурно-оперативных методов работы спецслужб диктуется тем, что нередко затраты, связанные с оперативно-агентурным проникновением в криптографические тайны противника, оказываются значительно меньше затрат на криптографическую разработку методов дешифрования, создания соответствующей техники и др. Кража, подкуп, взлом оказываются «более рентабельными», поэтому на взгляд авторов рассмотрение исторических фактов использования агентурно-оперативных методов доступа к тайнам противника или конкурента обращает внимание специалистов по защите информации и на этот вид информационной угрозы.

Список рекомендуемой литературы

1. Абрамов В.. Евреи в КГБ. Палачи и жертвы. – М., Яуза - Эксмо, 2005.
2. Агеева И.А. Канада и начало холодной войны: дело Гузенко в советско-канадских отношениях: http://www.usinfo.ru/c2.files/holodnajavojna10.htm

3. Агабеков Г. ЧК за работой / Предисловие А.В. Шаврова. Комментарии А.В. Шаврова, И.М. Смирновой. – М.: Ассоциация «Книга. Просвещение. Милосердие», 1992.
4. Блейк Джордж. Прозрачные стены. – М.: Молодая гвардия, 2006.
5. Быстролётов Д.А. Пир бессмертных. – М.: Граница, 1993.
6. Быстролётов Д.А. Путешествие на край ночи. – М.: Современник, 1996.
7. Габис С.А. Тайна «Магдебурга». Морской исторический сборник. Вып. 2. – СПб, 1991, С. 37-57.
8. Глинка Я.В., Одиннадцать лет в Государственной Думе. 1906–1917. Дневник и воспоминания. – М., 2001.
9. Гоголь В. Бомба для Сталина. – М.: 1996.
10. Гордиевский О., Эндрю К. КГБ. История внешнеполитических операций от Ленина до Горбачева. – М.:1992.
11. Даллес А. Искусство разведки. – М., 1992.
12. Дамаскин И.А. Сто великих разведчиков. – М., 2002.
13. Двинин В. Операция «Карфаген» или Тайны сейфовой комнаты. «Российская газета» – Неделя №4009 от 3 марта 2006 г.
14. Думова Н.Г. Кадетская контрреволюция и ее разгром (октябрь 1917-1920). – М.: 1982.
15. Ежов М.Ю. Один из мифов о крейсере «Магдебург» // Вопросы истории, №2, 2007.
16. Жиль Перро. Красная капелла. – М.: ЭКСМО-Пресс Яуза, 2004.
17. Залесский К.А. Империя Сталина. Биографический энциклопедический словарь. – М.: Вече, 2000.
18. Кан Д. Взломщики кодов / Пер. с англ. – М.: ЗАО Изд-во Центрполиграф, 2000.
19. Ким Филби. Моя тайная война. – М.: Военное издательство, 1989.
20. Колесников М.С. Таким был Рихард Зорге. Военное издательство МО СССР. – М.: 1965.
21. Кукридж Е.Х. Тайны английской секретной службы. – М., 1959.

22. Мерзляков В.М. Русская контрразведка: на заре века тотального шпионажа // В сб. «Легион «Белой смерти»». — М., 2002, С. 3-25.
23. Млечин Л., Чернова Т. Москва не платит пенсий своим агентам // Новое время. – 1991. – № 48. – С. 39.
24. Норманн П., Томас А. Энциклопедия шпионажа. – М.: Крон-Пресс, 1998.
25. Очерки истории внешней разведки. Т. 1 / под. ред. Е.М. Примакова. – М.,1999.
26. Павлов В.Г. «Сезам откройся!» Тайные разведывательные операции: Из воспоминаний ветерана внешней разведки. – М.: 1999.
27. Павлов В.Г. ТФП. Тайное физическое проникновение на вражеский объект. Серия: Высшая школа КГБ. Профессиональные секреты – М.: АЛГОРИТМ, 2010.
28. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа / Пер. с англ. В.Смирнова. – М.: КРОН-ПРЕСС, 1999.
29. Ронге М. Разведка и контрразведка. – Киев, 1993.
30. Спиридонович А.И. Записки жандарма. – М., 1991.
31. Феклистов А. За океаном и на острове. – М.: ДЭМ, 1994.
32. Филатов В. «Власовщина РОА: белые пятна». – М.: ЭКСМО АЛГОРИТМ, 2005.
33. Чернин О.В дни мировой войны. Воспоминания бывшего австрийского министра иностранных дел / Перевод с немецкого М. Константиновой, под ред. М. Павловича. – М. – Пг.: Гиз, 1923.
34. Черняк Е.Б. Пять столетий тайной войны. Из истории секретной дипломатии и разведки (монография). «Международные отношения». – М., 1991.
35. Шварев Н. Разведчики-нелегалы СССР и России. Кн. 1, – М.: Родина, 2006.
36. Шелков В. А. Кит Мэлтон и его музей «шпионской техники»: http://st.ess.ru/publications/articles/melton.