Министерство иностранных дел РФ
Московский государственный институт международных отношений (университет)
Европейский учебный институт

Т.Д. ТУЛЕШОВ, В.Н. СПЕКТОР

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК СПОСОБ ЗАЩИТЫ ГЕОПОЛИТИЧЕСКИХ ИНТЕРЕСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКВА
2015

УДК 004.6
ББК 30
Т 82

Т.Д. ТУЛЕШОВ
Директор Центрально-Азиатского направления
Центра анализа террористических угроз,
эксперт-политолог

В.Н. СПЕКТОР
Главный научный сотрудник Института биохимической физики РАН,
доктор физико-математических наук, профессор

НАУЧНЫЕ РЕЦЕНЗЕНТЫ:

О.Н. Барабанов – заведующий кафедрой политики и функционирования ЕС и Совета Европы МГИМО – Университета МИД России, доктор политических наук, профессор

В.Н. Лихачев – Чрезвычайный и Полномочный посол РФ, доктор юридических наук, профессор

А.А. Новиков-Ланской – заведующий кафедрой политической и деловой журналистики РАНХИГС при Президенте РФ, кандидат филологических наук

Т.Д. ТУЛЕШОВ, В.Н. СПЕКТОР. Современные информационные технологии как способ защиты геополитических интересов Российской Федерации. – Москва: Издание Европейского учебного института при МГИМО (У) МИД РФ, 2015. – 464 с., илл.

Данная книга является обобщением результатов исследований, проведенных в области современных информационных технологий. Обеспечение безопасности в мировом информационном пространстве становится одной из важнейших задач современности. Авторы раскрывают потенциалы современных информационных технологий, их понимание и практическое применение, что необходимо для защиты геополитических интересов и безопасности Российской Федерации.

ISBN 9785427000991

Если крикнет рать святая:
«Кинь ты Русь, живи в раю!»
Я скажу: «Не надо рая,
Дайте родину мою».
С. Есенин «Гой ты, Русь, моя родная»
(1914).

ГЛАВА 1

ВВЕДЕНИЕ

Что такое информация.

Сравним с эпиграфом наставление отца-основателя США Бенджамина Франклина:

Те, кто готов променять свободу на временную безопасность,
не заслуживают ни безопасности, ни свободы.

Это тоже информация – русский народ никогда не менял свободу на безопасность, русский народ всегда шёл на битву за свою свободу, какие бы опасности его ни поджидали.

Понятие информации рассматривалось ещё античными философами. В течение, по крайней мере, двух последних веков в науке идёт вполне содержательный спор о том, что же такое информация.

Википедия даёт её формальное и довольно противоречивое определение: «Информация (от ***лат.*** *informatio – формирование как выявление своей сущности, разъяснение, изложение, осведомление*) – значимые сведения о чём-либо, когда форма их представления также является информацией, то есть имеет форматирующую функцию в соответствии с собственной природой».

В бытовом или прикладном понимании всё представляется предельно простым – информация есть сумма собранных или полученных данных об интересующих объектах и передача собранных или систематизированных сведений от одних субъектов другим субъектам. Одно из первых определений бытовой информации было дано русским – философом и лингвистом проф. С.И. Ожёговым: «В бытовом смысле информация – сведения об окружающем мире и протекающих в нём процессах, воспринимаемые человеком или специальным устройством».[1] Было бы, конечно, точнее сказать: воспринимаемые человеком непосредственно или посредством специального устройства.

1 *Ожёгов С.И. – Словарь русского языка. Москва. 1990*

Источник: www.calend.ru

Сергей Иванович Ожёгов
(1900—1964)

Источник: www.physchem.chimfak.rsu.ru

Нильс Хенрик Давид Бор
(1885 – 1962)

Источник: ru.wikipedia.org

Вернер Гейзенберг
(1901 – 1976)

Однако не всё так просто – было замечено, что во многих случаях, особенно в микромире и в социуме, сам факт наблюдения (сбора информации, например, в ходе избирательных кампаний) изменяет свойства наблюдаемого объекта, и фиксируемая информация оказывается в лучшем случае неполной, чаще неточной или даже ложной. При этом необходимо понимать, что ложная информация не обязательно является дезинформацией, довольно часто она оказывается ошибочной. В физике микромира этот феномен обсуждается в рамках принципа дополнительности (*Нильс Бор, 1927)* и соотношений неопределённости (*Вернер Гейзенберг, 1927*).

В социуме, где по очевидным причинам воздействие этих принципов должно быть существенно более явным, законы ненамеренного искажения информации в связи с фактом наблюдения, если, конечно, не считать намерением сам факт наблюдения, изучены гораздо хуже.

В настоящее время не существует единого определения информации и как научного понятия, и как термина.

В современной науке рассматриваются два вида информации *(Википедия)*:

Объективная (*первичная*) информация – «свойство материальных объектов и явлений (*процессов*) порождать многообразие состояний, которые посредством взаимодействий (фундаментальные взаимодействия) передаются другим объектам и запечатлеваются в их структуре» [4]. Это утверждение, не слишком точное даже для своего времени, не отражает того факта, что ни передача информации обо всех свойствах материальных объектов, ни, тем более, их фиксация в структуре других объектов не может быть полной, следовательно, исчерпывающе объективной.

Субъективная (*семантическая, смысловая, вторичная*) информация по Амосову – смысловое содержание объективной информации об объектах и процессах материального мира, сформированное сознанием челове-

ка с помощью смысловых образов (слов, образов и ощущений) и зафиксированное на каком-либо материальном носителе.

Развитие материи в процессе её движения направлено в сторону усложнения структуры материальных объектов. Одна из самых сложных структур – человеческий мозг. На сегодняшний день человеческий мозг, единственная из известных структур, обладающая характеристиками, которые человек называет сознанием. Мыслящие существа считают, что информация обязательно имеет некий смысл, и не ограничивают ее восприятие только в виде принимаемых сигналов. Создавая в сознании модель окружающего мира, как совокупность, состоящую из множества составляющих его моделей объектов и процессов, человек использует не информацию, а именно смысловые понятия. Чаще всего ошибочная информация возникает как функция неверной или искажённой модели окружающего мира у субъекта, воспринимающего и передающего полученную информацию.

Источник: ru.wikipedia.org

Виктор Михайлович Глушков (1903-1982) академик

Источник: www.peoples.ru

Николай Михайлович Амосов (1913-2002) член-корреспондент АН СССР

Смысл – сущность любого феномена, которая не совпадает с ним самим и связывает его с более широким контекстом реальности. Смысл – это понятие, описывающее глобальное содержание некоторого высказывания *(БСЭ, статья «Смысл»)*. Само слово прямо указывает, что смысловое содержание информации могут формировать только мыслящие приёмники информации. В человеческом обществе решающее значение приобретает не сама информация, а её смысловое содержание.

Смысл феномена оправдывает его существование, определяя его место в некоей системе, вводит соотношение «часть – целое», создавая необходимость его существования в качестве элемента системы. Мнимое или реальное предназначение каких либо вещей, слов, понятий или действий, которые закладывает в них общность или отдельно взятая личность, также называют смыслом. Бессмысленность – есть противоположность смысла, когда в действии, вещах словах, понятиях нет целевого предназначения. Под смыслом может подразумеваться и самостоятельное достижение целей, и имеющее конечный результат чье либо или какое либо действие.. В церковнославян-

Источник: en.wikipedia.org

Готфрид Вильгельм фон Лейбниц (1646-1716)

Источник: wtexts.ru

Фердинанд де Соссюр (1851-1913)

ском переводе Библии смыслом (*лат. prūdentia*) именует то, что в синодальном тексте обозначено разумом *(Иез. 28:4)*.

Способность мозга создавать смысловые понятия и связи между ними является основой сознания. Сознание можно рассматривать как саморазвивающуюся смысловую модель окружающего мира. Понятно, что в пределе количество моделей окружающего мира совпадает с числом носителей сознания, а предел саморазвитие каждой модели определяется качеством сознания каждого его носителя.

Смысловое содержание информации является предметом исследования семантики как одного из крупных научных направлений семиотики – комплекса научных теорий изучающих свойства знаковых систем.

Знаковой системой считается система конкретных или абстрактных объектов (знаков, слов), с каждым из которых определённым образом сопоставлено некоторое значение. В теории доказано, что таких сопоставлений может быть два. Первый вид соответствия определяет непосредственно материальный объект, который обозначает это слово и называется денотат (или, в некоторых работах, – номинат). Второй вид соответствия определяет смысл знака (слова) и называется концепт. При этом исследуются такие свойства сопоставлений как «смысл», «истинность», «определимость», «следование», «интерпретация» и другие. Для исследований используется аппарат математической логики и математической лингвистики.

Идеи семантики, намеченные ещё Г.В. Лейбницем и Ф. де Соссюром в XIX веке, сформулировали и развили Ч. Пирс (1839-1914), Ч. Моррис (р. 1901), Р. Карнап (1891-1970) и другие.

Фундаментом для создания устройств (программ) машинного перевода с одного естественного языка на другой также является семантический анализ. Создание аппарата семантического анализа можно считать главным теоретическим успехом. Смысл текста на естественном языке он дает возможность представить в виде записи на некотором формализованном семантическом (смысловом) языке. Фундаментом для создания устройств (программ) машинного перевода с одного естественного языка на другой также является семантический анализ.

Сама по себе фиксация информации на материальном носителе, хотя и считается максимально приближенной к объективной (аудиовизуально зафиксированные показания свидетеля, аэрофотосъёмка и тому подобное), на самом деле она таковой не становится, а является лишь средством обеспечения её воспроизводимости без темпоральных искажений, связанных со свойством мозга осуществлять селекцию информационных сигналов в рамках смысловой модели, присущей каждому конкретному индивиду.

Источник: ru.wikipedia.org

Чарльз Пирс

Таким образом, можно утверждать, что существовавшие ранее и бушующие в настоящее время информационные войны на самом деле являются более или менее острым столкновением смысловых моделей, принятых или навязанных противостоящим социумам, что, например, подтверждается антагонистической интерпретацией информации о событиях в Сирии в частности и, в общем, в отношении событий «Арабской весны».

Источник: is-practice.16mb.com

Рудольф Карнап

Согласно концепции К. Шеннона, «информация – это снятая неопределенность, то есть сведения, которые должны снять в той или иной степени существующую у потребителя до их получения неопределенность, расширить его понимание объекта полезными сведениями».[2] Точнее было сказать: информация – это снимаемая неопределённость.

Необходимо отметить тот факт, что Шеннон в своей ставшей классической работе «Бандвагон/The Bandwagon» и в других публикациях предупреждал об опасности переоценки теории информации: «За последние несколько лет теория информации превратилась в своего рода бандвагон от науки» …

Источник: www.pandia.ru

Клод Элвуд Шеннон
(1916-2001)
профессор

«… значение теории информации было, возможно, преувеличено и раздуто до пределов, превышающих её реальные достижения. Учёные различных

2 Shannon C. – The Bandwagon, Trans. IRE, 1956, IT-2, № 1, p. 3; Шеннон К. – Работы по теории информации и кибернетике (пер. с английского, под ред. Р. Л. Добрушина и О. В. Лупанова) – Изд. иностранной литературы, М,, 1963, с. с. 667-668.

Источник: ru.wikipedia.org

Леон Бриллюэн
(1889-1969)
профессор

специальностей … используют идеи теории информации при решении своих частных задач. Так, теория информации нашла применение в биологии, психологии, лингвистике, теоретической физике, экономике, теории организации производства и во многих других областях науки и техники. Короче говоря, сейчас теория информации, как модный опьяняющий напиток, кружит голову всем вокруг» …

«… Очень редко удаётся открыть одновременно несколько тайн природы одним и тем же ключом. Здание нашего, несколько искусственно созданного благополучия, слишком легко может рухнуть, как только в один прекрасный день окажется, что при помощи нескольких магических слов, таких, как информация, энтропия, избыточность…, нельзя решить всех нерешённых проблем» …

«… основные положения теории информации касаются очень специфического направления исследования, направления, которое совершенно не обязательно должно оказаться плодотворным в психологии, экономике и в других социальных науках» …

«… основу теории информации составляет одна из ветвей математики, т. е. строго дедуктивная система. Поэтому глубокое понимание математической стороны теории информации и её практических приложений к вопросам общей теории связи, является обязательным условием использования теории информации в других областях науки» … «… поиск путей применения теории информации в других областях не сводится к тривиальному переносу терминов из одной области науки в другую. Этот поиск осуществляется в длительном процессе выдвижения новых гипотез и их экспериментальной проверки».

В науке случается, что постановка вопроса подчас оказывается важнее самых крупных открытий, полученных в поисках ответа. Так случилось, что известный физик- структурщик Бриллюэн сформулировал ряд вопросов, оказавшихся важными для теории информации: «Новая территория была завоевана для науки с появлением в недавнее время теории информации. Это открытие создало новую область, немедленно привлекшую разведчиков и исследователей. Как это случилось? Как далеко это идёт? И где оно может продолжать распространяться? Означает ли это вторжение науки на территорию, принадлежащую по традиции философии, или это есть открытие новой страны, своего рода «ничейной земли», которая ускользала от прежних исследований?» [3]

3 *Бриллюэн Л. – Наука и теория информации, М., 1960; Научная неопределенность и информация, М., 1966*

Смысловая множественность понятия «информация»

Многогранность понятия информации выражается и в необходимости привлечения возможностей большого количества других научных дисциплин для возможно более полного раскрытия сущности отдельных аспектов этого понятия.

Так, предметом информатики являются данные информационных сообщений, методы их создания/генерации/получения, хранения, обработки и передачи.

Системология исследует преобразования информации: запись как формирование структуры материи и модуляции потоков энергии при взаимодействии инструмента с носителем, хранения как обеспечения стабильности структуры (квазистатика) и модуляции (квазидинамика) и чтения (изучения) как взаимодействия зонда (инструмента, преобразователя, детектора) с субстратом. Системология рассматривает информацию через связь с другими основаниями:

$$I = S/F\ [M \underline{\vee} R \underline{\vee} T],$$

где: I – информация; S – системность мироздания; F – функциональная связь; M – материя; $\underline{\vee}$ – знак объединения универсума; R – пространство и T – время.

Объекты, существующие в материальном мире, непрерывно изменяясь, обмениваются энергией с окружающей средой. Изменение состояния объекта обязательно изменяет состояния некоторых других объектов окружающей среды. Это процесс можно рассматривать, как передачу неких сигналов от объекта к объекту. Само же измененное состояние объекта во время передачи ему сигнала, называется регистрацией сигнала.

Единичный сигнал или их множественность, расположенных в последовательности, создают сообщение, которое может восприниматься получателем в самом различном виде или объёме.

Для физики «информация» является термином, который по качественным характеристикам объединяет такие понятия как «сигнал» и «сообщение». Если последние могут быть исчислены количественно, то сигналы и сообщения могут быть единицами измерения объёма информации.

Одно и то же сообщение (сигнал) разными системами интерпретируется по-своему. Например, последовательно длинный и два коротких звуковых сигнала в терминологии азбуки Морзе – это буква Д (или D), а в терминологии БИОС от фирмы AWARD – неисправность видеокарты.

Правовое определение понятия «информация» в России дано в федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, инфор-

мационных технологиях и о защите информации» *(Статья 2)*: «информация – сведения (сообщения, данные) независимо от формы их представления».

Федеральный закон № 149-ФЗ определяет и закрепляет права на защиту информации и информационную безопасность граждан и организаций в ЭВМ и в информационных системах, а также вопросы информационной безопасности граждан, организаций, общества и государства[4].

В теории управления (кибернетике), предметом исследования которой являются основные законы управления, то есть развития систем управления, информацией называются сообщения, получаемые системой из внешнего мира при адаптивном управлении (приспособлении, самосохранении системы управления).

Кибернетика определяя объективную информацию, характеризует ее как присущее материальным объектам и явлениям объективное свойство порождать разнообразие состояний, передающихся от одного объекта или процесса другому, посредством фундаментальных взаимодействий и запечатленных в его структуре. Материальную систему кибернетика рассматривает как множественность объектов, которые даже при нахождении в различных состояниях, оказывают влияние на состояние других объектов системы и испытывают на себе их влияние. В природе разнообразные состояния системы являют собой информацию, множество состояний представляют собой первичный код, или код источника. И в этом случае, источником информации является каждая материальная система.

Субъективную (семантическую) информацию кибернетика определяет как смысл или содержание сообщения. Информация – это характеристика объекта.

В математической теории понятие «информация» связано с исключительно абстрактными объектами – случайными величинами, в то время как в современной теории информации это понятие рассматривается значительно шире – как свойство универсума.

Несомненна связь между двумя одинаковыми терминами. Автор теории информации Клод Шеннон использовал именно математический аппарат случайных чисел. Сам же он вкладывал в термин «информация» нечто большее, фундаментальное (нередуцируемое). В теории информации интуитивно предполагается, что информация имеет содержание. Количество информации доступно измерению, а сама информация может уменьшить существующую неопределённость и информационную энтропию.

---

4 Королев А. Н., Плешакова О. В. – Об информации, информационных технологиях и о защите информации. Постатейный комментарий к Федеральному закону. – М.: Юстицинформ, 2007, 128 с. (Библиотека журнала «Право и экономика». Комментарий специалиста). ISBN 5-7205-0791-4

Классификация «информации»

Информацию можно разделить на виды по разным критериям, например:

по истинности

- истинная;
- ложная;
- дезинформация.

по способу восприятия

- Визуальная – воспринимаемая органами зрения.
- Аудиальная – воспринимаемая органами слуха.
- Тактильная – воспринимаемая тактильными рецепторами.
- Обонятельная – воспринимаемая обонятельными рецепторами.
- Вкусовая – воспринимаемая вкусовыми рецепторами.

по форме представления

- Текстовая – передаваемая в виде символов, предназначенных обозначать лексемы языка.
- Числовая – в виде цифр и знаков, обозначающих математические действия.
- Графическая – в виде изображений предметов, графиков.
- Звуковая – устная или в виде записи передача лексем языка аудиальным путём.

по назначению

- Массовая – содержит тривиальные сведения и оперирует набором понятий, воспринимаемых большей частью социума.
- Специальная – содержит специфический набор понятий, при использовании происходит передача сведений, которые могут быть не понятны основной массе социума, но необходимы и понятны в рамках узкой социальной группы, где используется данная информация.
- Служебная (государственная и корпоративная) – содержит набор внутренних сведений (распорядительных и исполнительных документов, инструкций, деловой переписки и анкет сотрудников) государственных ведомств и учреждений и корпораций, без дополнительных разрешений доступная только сотрудникам этих ведомств, учреждений и корпораций.
- Секретная – передаваемая узкому кругу лиц и по закрытым (защищённым) каналам.
- Личная (приватная) – набор сведений о какой-либо личности, определяющий социальное положение и типы социальных взаимодействий внутри популяции. Здесь необходимо заметить, что по наследству от СССР Российской Федерации достался правовой нигилизм

в отношении личной информации. В связи с этим данное определение предпочтительно формулировать в следующем виде:

- Личная (приватная) – набор законодательно защищенных сведений о какой-либо личности, определяющий социальное положение и типы её социальных взаимодействий внутри популяции. В публичный домен из личной информации могут входить лишь сведения (данные), лично представленные субъектом информационного сообщения.

по значению

- Актуальная – информация ценная в данный момент времени.
- Достоверная – информация, полученная без искажений.
- Понятная – информация, выраженная на языке, понятном тому, кому она предназначена.
- Полная (достижимо полная') – информация, достаточная для принятия правильного решения или понимания.
- Полезная – полезность информации определяется субъектом, получившим информацию в зависимости от объёма возможностей её использования.

Традиционализм субъективного в философии постоянно доминировал в ранних определениях информации, как категории; понятия; свойства материального мира. Информация существует вне нашего сознания, и может иметь отражение в нашем восприятии только как результат взаимодействия: отражения, чтения, получения в виде сигнала, стимула. «Информация стоит в ряду: материя, пространство, время, системность, функция и другие, составляющие основополагающие понятия формализованного отражения объективной реальности в её распространении и изменчивости, разнообразии и проявленности»[5]. Вопреки устоявшемуся представлению об информации как свойстве материи, информация скорее свойство универсума.

С материальной точки зрения информация – это отражение порядка следования объектов материального мира (универсума). Например, порядок следования генов в ДНК является наследственной информацией. Для осуществления информационного обмена требуется наличие необходимых и достаточных условий. Существует несколько подходов к определению необходимых условий, и лишь одно признано как необходимое и достаточное: Наличие субъекта, способного распознавать информацию. Это человек и человеческое общество, сообщества животных, роботов и т. д.

Различные объекты, взятые по одному разу, образуют базис информации. Информационное сообщение строится выбором из базиса копий объек-

---

5 *Википедия*

тов и расположением этих объектов в пространстве в определённом порядке. Длина информационного сообщения определяется как количество копий объектов базиса и всегда выражается целым числом. Необходимо различать длину информационного сообщения, которое всегда измеряется целым числом, и количество знаний, содержащихся в информационном сообщении.

Источник: habrahabr.ru

Норберт Винер (1894-1964) кавалер Золотой Медали Учёного (США)

Последовательность целых чисел, которые записаны в вектор – так выглядит информация с математической точки зрения. При этом числа – это порядковый номер объекта в информационном базисе. Вектор не зависит от физической природы объектов базиса и называется инвариантом информации. Одно и то же информационное сообщение можно выразить с помощью различных символов или их комбинаций. Но сколь бы разнообразными не были символы в информации, изменится не вектор или инвариант, а лишь базис.

Весьма показательно забавное высказывание об информации основоположника современной кибернетики и теории искусственного интеллекта Норберта Винера: «Информация – это не материя и не энергия, информация – это информация». Но основное определение информации, которое он дал в нескольких своих книгах, более вразумительно: *«информация – это обозначение содержания, полученного нами из внешнего мира в процессе приспосабливания к нему нас и наших чувств».*[6]

Большой философский интерес представляет классическое утверждение Винера: «Понятие количества информации совершенно естественно связывается с классическим понятием статистической механики – понятием энтропии. Как количество информации в системе есть мера организованности системы, точно также энтропия системы есть мера дезорганизованности системы».

Утверждение о том, что эта «формулировка Винера даёт прямое указание на объективность информации»[7], то есть на её существование в природе независимо от сознания (восприятия) человека, хотя и правильное само по себе, не отражает латентность этой «объективной» информации. Её актуализация, то есть вывод на оператора, делает информацию инструментом сознания. Такое утверждение, с нашей точки зрения снимает затянувшуюся

---

6 Н. Винер – Кибернетика, или управление и связь в животном и машине. Советское радио. М., 2 изд., 1968; Наука. М., 1983

7 Википедия

Источник: www.chronos.msu.ru

Седов Евгений Александрович (1929-1993) профессор

коллизию соотношения энтропии как меры беспорядка и информации как меры/отражения структурной упорядоченности. Информация как отражение структурной упорядоченности материального мира сама по себе не может противостоять энтропии, являющейся энергетическим свойством, характеризующим процессы разупорядочения материального мира (универсума).

Тот факт, что традиционная теория информации оказалась не самодостаточной, нашёл отражение в дискуссиях ведущих учёных.

Например, академик А.Н. Колмогоров убедительно оспаривает вторичность теории информации по отношению к теории вероятности. Он в частности пишет: «Не видно, почему теория информации должна столь существенно основываться на теории вероятностей, как это представляется по большинству руководств… эта зависимость от заранее созданной теории вероятностей в действительности не является неизбежной.

Теория информации должна предшествовать теории вероятностей, а не опираться на неё. Основы теории информации имеют по самому существу этой дисциплины финитный комбинаторный характер[8]».

Далее он утверждает: «Информация по своей природе – не специально вероятностное понятие. Исходное представление об информации как о числе двоичных знаков, необходимых для того, чтобы выделить определённый объект из конечного множества объектов, ничего общего с теорией вероятностей не содержит. Лишь в более высоких разделах теории информации сейчас доминируют вероятностные методы. Возможно, однако, что соотношения между теорией информации и теорией вероятностей радикально изменятся. <… > Отношения эти могут быть обратными современным, и не теория вероятностей будет основой высших разделов теории информации, а в основе теории вероятностей будут лежать понятия теории информации[9].

В своей работе[10] проф. Е.А. Седов даёт своё видение соотношения информации и энтропии: «Теория информации в том виде, в каком она существует сегодня, – это лишь первый шаг к решению многих научных задач.

---

8 Колмогоров А.Н. – Комбинаторные основания теории информации и исчисления вероятностей. УМН, 1983, т. 38, вып. 4

9 Колмогоров А.Н. – Проблемы теории вероятностей и математической статистики. Вестник Академии наук СССР, 1965, №5

10 Седов Е.А. – Одна формула и весь мир (книга об энтропии). М., 1982

…Современная наука изучает различные уровни материального мира… И на всех уровнях она обнаруживает нескончаемую диалектическую борьбу энтропии и информации – двух противоположных начал, отражающих вечное стремление к увеличению хаоса и противодействующую ему тенденцию к образованию упорядоченных структур».

Проф. И. Б. Новик, с одной стороны, отмечает, что «Отсутствие в современной теории информации законов сохранения можно рассматривать как свидетельство незавершённости этой теории…. Решение вопроса относительно обобщения законов сохранения на область информации, на наш взгляд, существенно продвинет разработку содержательной теории информации, даст опорный стержень для, так сказать, «физики отражения»».

Нам представляется, что информацию можно трактовать как форму отражения…. По нашему мнению, в информации выражается упорядоченность отражения…. Если для материи справедливы законы сохранения, то можно полагать, что некоторые аналоги этих законов применимы и к атрибуту отражения…. При рассмотрении только одной формы отражения (информации) без учета её перехода в другую форму закон сохранения в данной области не удаётся установить[11].

С другой стороны, он предсказывает, что «…и в области теории информации мы столкнёмся со специфическими статистическими законами, характеризующими «дуализм» отражения (информация и шум), подобно тому, как специфичность статистики в квантовой механике связана с «дуализмом» микрообъектов (обладание свойствами частицы и волны)[12].

Однако, по этому поводу проф. А. Д. Урсул замечает: «Доведенная до крайности концепция выбора, неопределённости может привести к тому, что объективный характер самой информации окажется под сомнением, и будет признаваться «творение» информации субъектом или вообще воспринимающей системой. В силу этих соображений наше общее понимание информации должно быть освобождено от её зависимости от воспринимающей системы (хотя в ряде случаев эта зависимость действительно существует) в такой же степени, как и от трактовки информации в духе чисто вероятностных представлений»[13].

Далее он подчёркивает необходимость придерживаться концепции информации как отражения – «Понятия информации, которые изолируются от связи с категорией отражения, на наш взгляд, не будут далее развиваться, они образуют тупиковые линии развития…. Категория отражения выступа-

11 Новик И. Б. – Негэнтропия и количество информации. Вопросы философии, 1962, № 6

12 Новик И. Б. – Кибернетика. Философские и социологические проблемы. М., 1963

13 Урсул А. Д. – Природа информации. М., 1968

Источник: lib.znate.ru

Урсул Аркадий Дмитриевич профессор

Источник: lib3.podelise.ru

Вяткин Виктор Борисович Кандидат технических наук, старший научный сотрудник Центральной научной библиотеки Уральского отделения Российской Академии наук

ет в качестве важнейшего методологического ориентира, помогающего обнаружить верные пути в «хаосе» омонимии понятия информации»[14].

Кардинальное развитие теории информации связано с работами В.Б. Вяткина, сформулировавшего в рамках синергетического подхода законы сохранения информации[15].

На качественном уровне синергетический подход Вяткина связан с рядом начальных утверждений.

Вероятностная и синергетическая теории информации, имея предметом своего познания различные виды информации (вероятностный, связанный с управлением и синергетический, существующий независимо от управления), в то же самое время непосредственно взаимосвязаны между собой отношением взаимного проникновения друг в друга.

Комбинаторное количество информации имеет двойственную природу, и в зависимости от того, с какой стороны его рассматривать, может относиться, как к синергетическому, так и к вероятностному виду информации.

Закон сохранения информации.

Суммарное количество синергетической и вероятностной информации, характеризующей структуру дискретной системы и её взаимоотношения с окружающей средой, при фиксированном числе элементов системы, является постоянной величиной.

Для раскрытия закона сохранения В. Вяткин использовал универсальное уравнение. Большинство приведенных высказываний было сделано до появления <=»«а=»»> синергетической теории информации, по отношению к которой они имеют превентивный характер. Предметом познания данной теории являются информационно-количественные аспекты отражения дискретных систем через свои части (подсистемы). Ключевое положение при этом занимает универсальное информационное уравнение, первона-

14 *Проблема информации в современной науке. М., 1975*

15 *Вяткин В.Б. – Введение в синергетическую теорию информации. Информационные технологии, 2010, №12*

чально полученное как соотношение между отражаемой (I_0), отраженной (I_Σ) и неотраженной (S) информациями:

$$I_0 = I_\Sigma + S$$

Отражённая I_Σ и неотражённая S информации именуются как аддитивная негэнтропия и энтропия отражения и характеризуют структуру отражаемой дискретной системы со стороны упорядоченности и хаотичности, соответственно.

Универсальность уравнения заключается в многозначности его интерпретации, которая зависит от того, с какой стороны это уравнение рассматривается. В настоящее время (2009) можно указать пять таких интерпретаций:

1) Информационный закон отражения, согласно которому информация, отражаемая системой через совокупность своих частей, разделяется на отражённую и неотражённую части, равные, соответственно, аддитивной негэнтропии и энтропии отражения.

2) Закон сохранения суммы хаоса и порядка, в соответствии с которым, чтобы мы ни делали с системой без изменения общего количества элементов, на сколько бы частей ни разбивали её по значениям какого-либо признака и в каком бы соотношении по числу элементов ни находились между собой части, сумма хаоса и порядка в структуре системы всегда будет оставаться неизменной.

3) Закон сохранения информации на межвидовом информационном уровне, говорящий о том, что при любых структурных преобразованиях системы суммарное количество её синергетической и вероятностной информации сохраняет свою постоянную величину.

4) Уравнение выражает непосредственную взаимосвязь комбинаторного (I0), синергетического (I_Σ) и вероятностного (S) подходов к определению количества информации, в своей совокупности образующих единую количественную основу общей теории информации.

5) В термодинамическом отношении универсальное информационное уравнение асимптотически эквивалентно уравнению перехода системы идеальных газов из структурно-упорядоченного состояния в состояние термодинамического равновесия, составленному с помощью энтропии Больцмана.

В целом, универсальное информационное уравнение (1) свидетельствует о том, что в формате <=»«а=»»> синергетической теории информации возникает новая научная теория. «Дальнейшее развитие этой теории и внедрение её в практику научных и прикладных исследований будет иметь значение не только для общей теории информации, но и для тех предметных областей, где объекты познания представимы в виде дискретных систем с конечным множеством элементов».

В пользу этого говорит тот факт, что на синергетическую теорию информации уже делаются ссылки в публикациях различных авторов [16]по тематике таких предметных областей, как поисковая геология, нефтегазовый промысел, физика атома, экономика, философия, структурная лингвистика, социальная политика, военное дело. Кроме того, уже есть прецеденты её включения в образовательный процесс.

Начиная с 70 годов прошлого века, активно внедряется новая классификация исторического процесса развития человечества. И «первая волна» (сельскохозяйственная), начавшись около 10 тысяч лет назад, и «вторая волна» (промышленная), начавшись около 300 лет назад, принесли кардинальные изменения для человеческой цивилизации. Сейчас человечество находится на стадии «третьей волны» (технологической), которая также принесет свои составляющие – экономику и политические институты, СМИ и свою структуру семьи, равно как и свой собственный период болезненного и хаотичного становления и, конечно же, свои способы и методы характера ведения войны.

В соответствии с этой временной классификацией академик В. М. Глушков ввёл понятие трёх барьеров в освоении и оперировании информацией.

Первый информационный барьер был связан с изобретением письменности, которая дала возможность сохранять и передавать знания. До этого мозг человека был единственным хранилищем информации. Первый информационный барьер был преодолён приблизительно в V тысячелетии до н. э.

Второй информационный барьер был связан с изобретением книгопечатания, что резко увеличило число носителей информации. Этот барьер был преодолён приблизительно в XV веке. Позже появились новые методы распространения и хранения информации – телеграф, телефон, фотография, телевидение, кино, магнитные записи. Но обработку информации по-прежнему выполнял исключительно мозг человека.

Третий информационный барьер был связан с созданием ЭВМ, которые позволили резко увеличить скорость обработки информации. Этот барьер был преодолён в середине XX века, когда появились первые компьютеры. К этому моменту объёмы информации стали такими большими, что способностей человеческого мозга для её обработки стало не хватать.

«Мыслитель» Родена являет образ человека, потерявшегося в потоках информации.

Осознание этих процессов привело к возникновению термина информационная война и к целой системе определений этого термина.

---

16 Например, Чернавский Д. С. – Синергетика и информация (динамическая теория информации) – М., Едиториал УРСС, 2004, 288 с. ISBN 5-354-00241-9

О термине «информационная война».

Источник: ru.wikipedia.org

Огюст Роден (1840-1917)

Попытка дать такое определение с предупреждением о возможной неэнциклопедичности сделана в Википедии, *Интернет*. Оно, в лучшем случае, относится к традиционной или к современной форме информационной войны и вполне может запутать неискушённого читателя введением альтернативных терминов.

Информационная война *(англ. Information war)* – термин, имеющий два значения:

1) Воздействие на гражданское население и /или военнослужащих другого государства распространением определённой информации. Термин «информационно-психологическая война» был заимствован в русский язык из словаря военных кругов США. Перевод этого термина (*«information and psychological warfare»*) с английского языка может звучать и как «информационное противоборство», и как «информационная, психологическая война», в зависимости от контекста конкретного официального документа или научной публикации[17].

Источник: alldayl2.com

Скульптура Родена «Мыслитель»

В этом смысле также используется термин психологическая война – психологическое воздействие на гражданское население и (или) военнослужащих другого государства с целью достижения политических или чисто военных целей[18].

2) Целенаправленные действия, предпринятые для достижения информационного превосходства нанесением ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем.

Одно из первых документированных проявлений информационной войны было зафиксировано во время Крымской войны (1853—1856), когда сразу после Синопского сражения английские газеты в отчётах о сражении писали, что русские достреливали плававших в море раненых турок[19].

---

17 Манойло А. В. – Информационно-психологическая война: факторы, определяющие формат современного вооружённого конфликта

18 Крысько В. Г. – Словарь-справочник по социальной психологии

19 The Crimean War 1854/56 and Australian Involvement

В этой же статье Википедии делается попытка определить основные черты современной информационной войны.

Основные черты информационной войны.

- В информационной войне не задействуются психоактивные вещества, прямой шантаж и запугивание (это характерно для терроризма), подкуп, физическое воздействие и т. п. Хотя указанные воздействия могут применяться параллельно с информационной войной, они не являются обязательным элементом.

Очевидно, что «психоактивные» (лучше психотропные) вещества и физическое воздействие не могут передаваться по системам компьютерной связи, что же касается прямого шантажа, запугивания и подкупа, то почему бы и нет. Можно согласиться, что последние средства воздействия, может быть за исключением подкупа, характерны для терроризма, но информационная война в противоположность идеологической борьбе чаще всего есть разновидность ***государственного терроризма.***

- Объектом является как массовое, так и индивидуальное сознание. Индивидуального воздействия «удостоиваются» лица, от решения которых зависит принятие решений по интересующим противоборствующую сторону вопросам (президент, премьер-министр, глава МИД, дипломатические представители, главы воинских формирований и т. п.). Можно сказать, что методы информационной войны воздействуют на массовое сознание аналогично тому, как методы психотерапии воздействуют на сознание индивидуальное.
- Информационное воздействие может осуществляться как на фоне информационного шума, так и в условиях информационного вакуума.
- Навязывание чуждых целей – это то, что делает информационную войну войной и отличает её от обычной рекламы. Однако «навязывание чуждых целей» является предметом рекламной деятельности, что делает рекламу одним из средств достижения экономических целей в ходе информационной войны, как это имеет место в современной российской экономике и торговле.

Это проявилось и в пролиферации негативных сведений о состоянии российской экономики на этапе длившегося более 17 лет рассмотрения вопроса о вхождении России в ВТО (коррупция, рэкет, организованная преступность, продажность и зависимость от власти судебной и правоохранительной системы, двусмысленная законодательная база, слабость и криминализованность банковской системы и другие), что, кстати, характерно для всех переходных экономик и для многих экономик стран устоявшегося капитализма.

Это была явная информационная война, направленная на принуждение России к согласию на принятие невыгодных ей условий присоединения

к ВТО, и нельзя думать, что эта война прекратилась с вхождением России в ВТО. Вместо ставшей очевидно абсурдной поправки Нанна-Лугара Конгресс США протаскивает «Акт Магницкого» и вынуждает Евросоюз поддержать его. Обсуждение этого Акта в Сенате США российский министр иностранных дел совершенно справедливо охарактеризовал как «театр абсурда».

Такие действия многими специалистами определяются уже не просто как информационная война, а как кибертерроризм[20], часто становящийся разновидностью государственного терроризма.

- Средствами ведения традиционной и современной информационной войны являются любые средства передачи информации – от СМИ до почты и сплетен, целенаправленно распространяемых в атакуемом социуме агентурой (в том числе и завербованной) противника.
- Информационное воздействие содержит искажение фактов (дезинформацию) или навязывает подвергающимся ему эмоциональное восприятие, выгодное воздействующей стороне.

Методы ведения традиционной и современной информационной войны отражены в статье крайне скупо: «Как правило, методами информационной войны является выброс дезинформации или представление информации в выгодном для себя свете. Данные методы позволяют изменять оценку происходящего населением территории противника, развивать пораженческое настроение, и, в перспективе, обеспечить переход на сторону ведущего информационное воздействие» с приведенными в статье Википедии нелепыми примерами деятельности Стеньки Разина с его «прелестными письмами» и Йозефа Геббельса за интенсивное использование им СМИ для изменения общественного сознания.

Авторы статьи (*Википедия*) считают Холодную войну 1946-1991 годов классическим примером традиционной информационной войны, уточняя, что её основой был идеологический аспект. Идеологическая борьба в её острой фазе ведётся преимущественно на философском фронте методами консциентальной войны, физические средства ведения которой находятся в начальной стадии разработки. Безусловно, семантические методы её осуществления лежат в области информационного противоборства.

Часть исследователей считает, что распад СССР был обусловлен не только амбициями республиканских элит и экономическими причинами, но и применением странами Запада информационных методов, которые способствовали началу внутриполитических процессов (возможно, что и вызва-

---

20 Шкляр Я.Е. – Кибертерроризм и информационные войны как средство достижения экономических и геополитических интересов. Центр прогнозирования конфликтов (Методические материалы). Терроризм, часть1, 2006, с. с. 71-78

ли их), закончившихся перестройкой и распадом СССР[21]. Эмоционально хочется согласиться с Сергеем Кара – Мурзой, но зато, как у него всегда всё просто получается – злые «дяди» из-за «бугра» напакостили нам, тщеславные «дяди» из союзных республик предали нас, наши старые, глупые «дедушки» из Политбюро растерялись, натворили глупостей, и СССР распался. Здесь всё не так просто[22], но, конечно, глупо было бы отрицать, что в ходе реально существовавшего информационного противоборства после 1985 года выспятком по копчику КПСС получила от зарубежных злых «дядей». Просто «щательней» нужно быть, излагать в реальной перспективе и не «гавкать на забор» – иначе беда – «искажение прошлого – прямой путь к поражениям в настоящем и в будущем» (А. П. Чехов).

«Википеды» утверждают, что «КГБ СССР осуществлял так называемые «активные мероприятия» по воздействию на зарубежное общественное мнение, а также на действия отдельных лиц, государственных и общественных организаций». До 1985 года при активном участии КГБ СССР и других ведомств информационную войну достаточно успешно (преимущество или паритет) вёл ЦК КПСС (группа Печенева). Потом, если ответно-встречные информационные удары и осуществлялись, то шли мимо «копчика» «злых дядей» – КГБ СССР не ЦК КПСС и не ТАСС – другие функции: подносить информационные патроны и стрелять, если скажут, куда или в кого.

Примером деструктивной роли аппарата Политбюро ЦК КПСС в это время может служить обсуждение содержательной части Программы конверсии оборонного потенциала в Госплане СССР. На последнем этапе этого обсуждения возникла коллизия точек зрения относительно включения в Программу результатов НИР по Стелтс. Достаточно компетентный генерал, представлявший точку зрения КГБ СССР, категорически возражал против включения в Программу этих материалов по двум причинным. Во-первых, Программа конверсии предусматривала только промышленные образцы (в крайнем случае, образцы, полученные в условиях опытно-промышленного производства) [23]. Во-вторых, эти результаты имели отношение к исследованиям, направленным на достижение стратегического превосходства. Представитель аппарата Генерального секретаря ЦК КПСС (заметим, не Оборонного отдела, с которым Программа была согласована заранее) настаивал

---

21 Кара-Мурза С. Г. – Манипуляция сознанием

22 Спектор В. Н. – Письмо Председателю Президиума Верховного Совета СССР А. А. Громыко «Замечания к Закону «О государственном предприятии» от 30 июня 1987 года». М., июль 1987 г., 23 с.; Спектор В. Н. – О геополитических последствиях распада СССР и внутриполитической обстановке в России. Приглашённое выступление на семинаре Политического комитета НАТО. Брюссель. 1992; Спектор В. Н. – Меморандум об очередном витке предкризисной стагнации российской государственности, его исторических корнях и возможных управляющих мерах по обеспечению позитивной эволюции. В кн.: Труды МАН ПНБ, М., 2008, т. 2, вып. 1, с. 4

23 Спектор В. Н. – Интервью ЦТ СССР по проблемам конверсии. 1988

на включение этих материалов, ссылаясь на требование Генсека «включить что-нибудь серьёзное». В ответ на аргументированные возражения представителя КГБ СССР он заявил «Ваше дело собачье: сторожить, что вам приказано и не гавкать». Один из авторов, возглавлявших группу экспертов АН СССР, призвал представителя ЦК КПСС, во-первых, вести себя пристойно, во-вторых, придерживаться согласованной с Оборонным отделом ЦК позиции по содержанию.

Программы и, в-третьих, покинуть помещение до тех пор, пока его компетенция не будет подтверждена дополнительно.

НИР по СТЕЛТС в результате не были включены в Программу, а этот представитель ЦК больше в Госплане не появлялся, и работа велась с Оборонным отделом ЦК КПСС в установленном порядке.

В дополнение интересно заметить, что уже значительно позже (1992) в ходе визита российской делегации на межакадемических российско-американских переговорах по технологиям двойного назначения в корпорацию «Вестингауз», когда в беседе с вице-президентом этой корпорации был затронут вопрос о соотношении технологий двойного назначения и конверсии, он пожаловался, что у корпорации возникли сложности в связи с резким снижением объёма оборонной продукции с 98 до 96%. Услышав, что в России в ходе конверсии объём оборонной продукции понизился до 14%, он заявил: «Это не конверсия, а развал отрасли».

Приведенные факты свидетельствуют о сдаче стратегических позиций Горбачёвым, а затем и Ельциным, попавшим в зависимость от вражеской логики, навязанной им в ходе информационной войны.

Несколько убедительней примеры, даваемые Википедией, по методам и случаям ведения современной информационной войны.

«Примером информационной войны также считаются и «информационно-психологические операции», которые проводит Министерство обороны США в наше время, к примеру, в Ираке: «Минобороны США заплатит частным подрядчикам в Ираке до 300 миллионов долларов за производство политических материалов, новостей, развлекательных программ и социальной рекламы для иракских СМИ, чтобы привлечь местное население к поддержке США», – пишет в 03 октября 2008 газета The Washington Post[24].

Ярким примером информационной войны является конфликт Израиля и Палестины, который является глобальным, поскольку затрагивает интересы более десятка стран. Противоборствующие стороны используют в своих интересах разнообразные информационные ресурсы: печатную прессу, телевидение, радио, интернет. Активно в информационной борьбе используются не любитель-

24 Trend News/Вести. Ru: США будут финансировать проамериканские материалы в иракских СМИ

ские хакерские атаки: так, израильская организация JIDF (ЖИДэФ) – «Еврейские силы интернет-обороны» – заблокировала действие интернет-сообщества «Израиль не страна!», размещенное в социальной сети Facebook и насчитывающее более 45 тысяч пользователей, а группа израильских хакеров «Gilad Team», взломавших более 15 сайтов, разместила на их страницах израильский флаг и слоган «Взломано». В свою очередь, пропалестинские хакеры во время операции «Литой свинец» взломали несколько тысяч израильских сайтов, как сообщало информационное агентство Ynet, более 750 израильских сайтов были взломаны за первые сутки военного столкновения.

Ещё более ожесточённая палестино-израильская информационная война развернулась вокруг проблемы изменения статуса Палестины с организации-наблюдателя на государство-наблюдатель в ООН. В этом информационном сражении Израиль и его американские агенты потерпели разгромное поражение, набрав всего 9 голосов членов Генеральной ассамблеи ООН в поддержку их дискриминационной позиции, причём из них 4 голоса принадлежали Карибским островным государствам с марионеточными режимами.

Нужно заметить, что наиболее значимый, консциентальный ресурс был не в полной мере задействован в этом информационном сражении. Раввинаты при поддержке США и СССР добились решения свежесозданной ООН об учреждении светского государства Израиль на части территории Палестины (заметим не на своих территориях и не на территориях европейских государств, поддержавших это решение). Это решение о создании светского еврейского государства на части этой территории одновременно с созданием арабского светского государства Палестина обосновывалось чисто религиозной концепцией о «Земле обетованной», применимость которой для решения проблем, возникающих в многоконфессиональном сообществе наций, представляется сомнительной даже многим американцам[25].

Во время Вьетнамской войны правительство Северного Вьетнама проводило меры, направленные на сокрытие потерь от американских бомбардировок. Как отмечал Виктор Теплов[26], специалист из научно-технической группы при военном атташе СССР в ДРВ: «Вьетнамцы прикладывали много усилий, чтобы внушить населению и американцам, что бомбардировки не достигают целей. <…> В их официальных сообщениях тщательно перечислялись потери от очередного американского налёта: один буйвол, три свиньи, семь кур, человеческих жертв – нет. Причём, количество животных в этих сводках тоже строго лимитировалось».

Во время военной агрессии НАТО в Югославии в 1999 году югославские СМИ незадолго до прекращения бомбардировок сообщали о том, что ПВО

25 *Manning Jerry – Wars are human inventions*

26 *Коммерсантъ, 7 марта 2000*

страны уничтожила более 160 натовских самолётов и вертолётов[27]. Сразу после прекращения бомбардировок начальник югославского генштаба Драголюб Ойданич объявил о 68 сбитых самолётах и вертолётах[28], а год спустя эта цифра была уменьшена до 37 самолётов и вертолётов».

В контексте изучения новых форм, методов и приёмов информационных войн представляет интерес развитие обстановки, связанной с урегулированием ситуации вокруг ядерной программы Ирана. Анализ развития событий показывает, что сценарии информационно-психологических операций по дискредитации политической власти отдельных неугодных стран, отработанные США и их союзниками в ходе предыдущих вооружённых конфликтов, а также «Арабской весны» имеют общие черты и осуществляются с использованием классических схем, что не срабатывает в случае Ирана.

Довольно неплохо проиллюстрирована мировая информационная война вокруг Грузино-Осетино-Абхазско-Российского столкновения (08.08.08). Среди общеизвестных примеров дезинформации, прямой лжи многих глав государств и правительств интересно отметить два факта.

Во-первых, по параметрам лживости, глупой и очевидной лживости, М. Саакашвили превзошёл всех. Так, он заявил: «До сегодняшнего дня многие европейцы не понимают, как могли вообще грузины даже подумать о том, что за независимость стоит бороться против 3 тысяч танков, 20 самолетов, 80 тысяч вошедших иноземцев (*интересное определение для сограждан по СССР, с которыми прожили более 70 лет)*, но если бы в нас не было боевого гена, если бы у нас не было боевых способностей, тогда мы и не существовали бы»[29], что находилось в смешном контрасте с его испугом от звука пролетавшего вдали от поля боя самолёта и с паническим драпом грузинских войск, без боя оставлявших территории и военную технику.

Во-вторых, безусловный интерес представляет описание технологии формирования фигуры жертвы как одного из приёмов ведения информационной войны[30]. В этой работе, посвящённой «конструированию «жертвы» как способа создания управляемой конфликтной ситуации», доктор социологических наук Г.И. Козырев пишет, что западные политики и подконтрольные им СМИ пытались представить Грузию жертвой агрессии, подвергшейся нападению со стороны России.

Но эти события были лишь кульминацией длительного и сложного процесса конструирования из Грузии жертвы, осуществлявшегося США

---

27 Ильин В. – Воздушная война на Балканах. Авиамастер. 2001, № 1, с. 6

28 Божьева О. – Уроки Балканской войны. Независимое военное обозрение, 22 декабря 2000

29 Саакашвили. М- Вероятность возобновления войны снизилась». Информационно аналитический портал «Грузия online», 11.03.2009 г.

30 Козырев Г.И. – Конструирование «жертвы» как способ создания управляемой конфликтной ситуации. Социологические исследования. 2009, № 4, с. с. 63-73

и их союзниками. Козырев делает сравнение с произошедшей ранее подобной операцией по конструированию жертвы из косовских албанцев, которая была проведена в Сербском крае Косово[31]. Здесь нужно заметить, что самый масштабный и долговременно дестабилизирующий эксперимент НАТО по формированию образа жертвы из созданной ей же в виртуальном пространстве нации «мусульман», был осуществлён в Боснии[32], [33].

Целенаправленное конструирование из Грузии страны-жертвы, пишет Г. Козырев, по сути, началось с приходом к власти президента М. Саакашвили. Периодически инициируемые грузинской стороной провокации в отношении российских миротворцев интерпретировались западными СМИ как посягательство большой и кровожадной России на «маленькую, но гордую, демократическую» Грузию. То есть, шла подготовка мирового общественного мнения к тому, что Россия является потенциальным агрессором, а Грузия – жертвой.

Неплохой рецепт для Грузии следует из приведенной Википедией исторической справки по Древнему Египту: «Древний Египет часто вёл войны и проигрывал их, однако не переставал существовать как государство. Это указывает на то, что жрецами был выработан некий принцип на случай проигрыша в войне, который можно условно назвать «принципом культурного сотрудничества» со странами-победительницами». Кстати, историческая ретроспектива позволяет сделать вывод о том, что, несмотря на «боевой ген», Грузия довольно часто пользовалась этим рецептом в своих отношениях и с Персией, и с Блистательной Портой.

Саморазвитие понятия информационной войны.

Рассмотрим простейшую схему, представляющую классификацию информационных систем.

Идея приведенной диаграммы[34] состоит в том, чтобы показать ступени развития информационных систем. Любопытно, что та ниша, которую в сво-

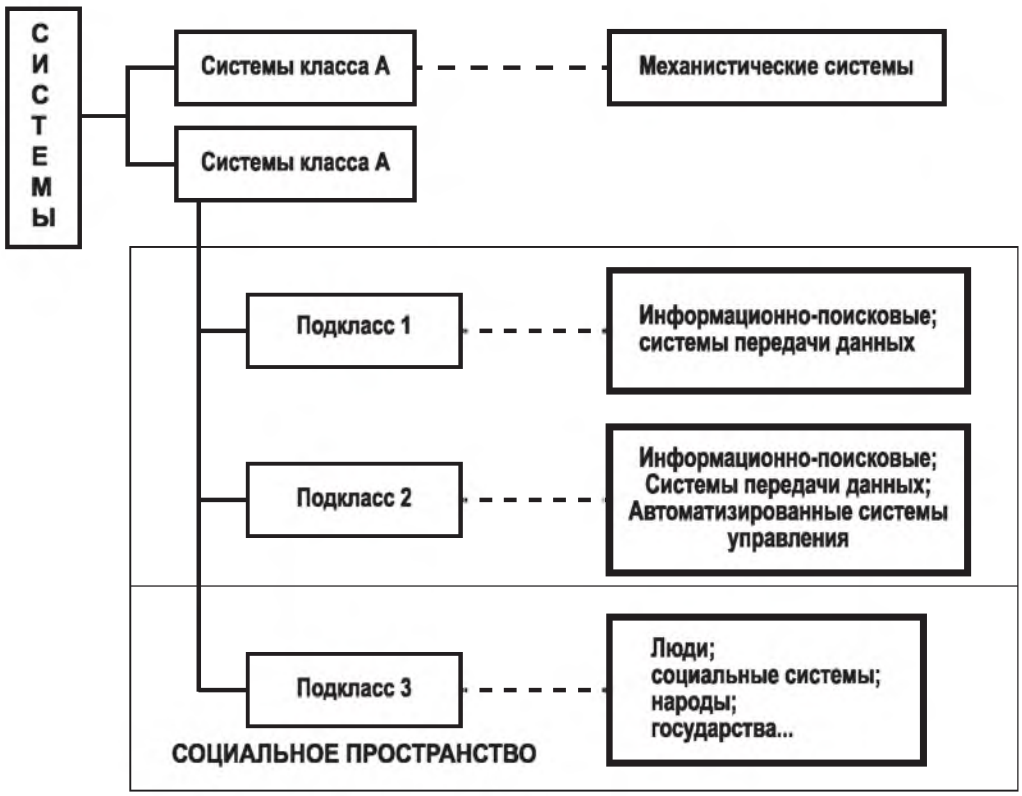
---

31 Спектор В.Н. – Разжигание этно-конфессионального конфликта в Косово и роль в этом внешних сил: США, Турции и Албании. Формирование в Косово криминального анклава под защитой сил КФОР (обзорный доклад на Секции 2). Международная конференция «Моноцентровная модель глобализации и её деструктивная роль на Балканах и во всём мире». М., 2008; Пахомов Л.Г., Спектор В.Н. – Экологическая катастрофа в Европе уже началась. Независимая газета. 23 июня 1999 г.; Спектор В.Н. – Заявление МАН ПНБ по гуманитарной ситуации и последним событиям в Косово. В кн.: Труды МАН ПНБ, М., 2008, т. 2, вып. 5, с. 286

32 Killing Eternity: Spiritual Genocide in the Territory of the Former SFRY/Library of the Publishing House NIP Press – East Sarajevo Documentation and Publication Centre

33 Спектор В.Н. – Роль внешнего фактора в инициировании гражданской войны и последующего распада Югославии (обзорный доклад на Секции 1). Международная конференция «Моноцентровая модель глобализации и её деструктивная роль на Балканах и во всём мире». М., 2008

34 Расторгуев С.П. Информационная война. – М: Радио и связь, 1999. – 416 С. ...



Источник: evartist.narod.ru

Классификация информационных систем

ей эволюции перескочила Природа – подкласс В2, заполнена с помощью человека, как говорится: «Свято место пусто не бывает».

По С. П. Расторгуеву, информационная война между двумя информационными системами – это открытые и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определённого выигрыша в материальной сфере

Системы целенаправленного сбора информации и контроля объектов в режиме реального времени выводятся из строя созданием перегрузок, например: «Космическая техника, особенно базирующаяся на геостационарной орбите, совершенно не ремонтнопригодна, не может быть оперативно заменена и очень уязвима к воздействию современных средств радиоэлектронного подавления (РЭП). Дело в том, что приемные устройства связных и разведывательных спутников выполнены очень чувствительными (*детекторы «Магнум» засекают сигналы, начиная с* 10^{-14} *Вт*) и защищены только от помех или перегрузок, сравнимых по длительности с продолжительностью полезных сигналов. <…> Мегаваттное воздействие с поверхности Земли, произведенное самодельными средствами РЭП на нужной частоте,

неизбежно приведёт к потере приёмного устройства спутника, а, следовательно, к выводу из строя всего канала связи» [35]. Здесь, конечно, составители «Белой книги» изрядно заблудились, видимо, чтобы запугать мир возможностями террористов, – самодельных мегаваттных средств РЭП не бывает. Это, правда, не значит, что ЭМИ более низкой мощности, генерируемое на установках, размещаемых, например, в микроавтобусах, не могут разрушить компьютерную сеть банка или головного офиса крупной корпорации.

Управляющее информационное воздействие на человека (подкласс В2) наиболее эффективно осуществляется методами психолингвистического программирования (ПЛП), в обиходе известное как зомбирование. Его нельзя относить к гипнозу, хотя на начальных стадиях ПЛП техника гипноза упрощает лингвистическое вхождение в психологический контакт с субъектом программирования.

Простейший пример психолингвистического программирования был предложен В. А. Крыловым:

...И говорит так сладко, чуть дыша:
«Голубушка, как хороша!
Ну что за шейка, что за глазки!
Рассказывать, так, право, сказки!
Какие перушки! какой носок!
И, верно, ангельский быть должен голосок!
Спой, светик, не стыдись! Что, ежели, сестрица,
При красоте такой и петь ты мастерица,
Ведь ты б у нас была царь-птица!»
Вещуньина с похвал вскружилась голова,
От радости в зобу дыханье сперло,
И на приветливы Лисицыны слова
Ворона каркнула во все воронье горло:
Сыр выпал – с ним была плутовка такова

Более сложную информационную систему, такую как человек, может вывести из строя информационное воздействие, которое, прежде всего, активизирует группу действий, мыслей, желаний и поступков, направленных на саморазрушение системы.

«Системы класса В образуют два пространства, в которых осуществляется их функционирование: кибернетическое и социальное. Социальное пространство существует уже не одно тысячелетие, но масштабные информационные войны начались только на исходе второго тысячелетия. Почему? Потому, что для систем с изменяемой целью, победа в информационной

---

35 Белая книга Российских спецслужб. – «Обозреватель». М., 1996

войне является, в общем случае, алгоритмически неразрешимой проблемой. За время войны могут измениться цели у воюющей системы.

Поэтому говорить о решении ряда задач в этой области в общем виде не приходится. Что же касается кибернетического пространства, то его возникновение и ознаменовало собой начало «эпохи информационных войн». Именно для кибернетических систем наработаны соответствующие средства, именуемые «информационным оружием». И именно в кибернетическом пространстве, используя это оружие, можно добиваться определенных побед.

<…> если быть точным, то, говоря о современной информационной войне технических систем, следует употреблять термины кибернетическая война и кибернетическое оружие. Они более правильно отражают суть происходящего, это отметил ещё М. Делаграмматик, назвав свою статью «Последний солдат суперимперии, или кому нужна кибервойна». Проблема обучения информационной самообучающейся системы, построенной на принципах СР-сети, при решении любой задачи, даже при условии, что информационная ёмкость СР-сети (исходное количество элементов) достаточна для хранения поступающей на вход информации, является алгоритмически неразрешимой [36].

Принято считать, что проблема алгоритмически разрешима, если существует алгоритм, осуществляющий отображение множества частных случаев решения проблемы в множество {0,1} (да, нет). В том случае, когда алгоритма, реализующего это отображение, не существует, проблема считается алгоритмически неразрешимой. При этом интересно, что, как отмечают А. Ахо и Дж. Ульман[37], в практике «очень важную роль играет кодирование частных случаев проблемы. Обычно подразумевается некоторое «стандартное» кодирование (кодирование, для которого существует алгоритм, отображающий коды описаний алгоритмов в эквивалентные программы машин Тьюринга). Если используются нестандартные кодирования, то неразрешимые проблемы могут стать разрешимыми. Но в таких случаях не существует алгоритма, с помощью которого можно перейти от стандартного кодирования к нестандартному».

Действительно, как порой мы понимаем себе подобных? Не всегда возможно найти компромисс и из-за неадекватного представления интересов и устремлений «высоких» договаривающихся сторон. Наши возгласы уподобляются «вопиющему в пустыне». Войны, периодически охватывающие континенты, – прямое доказательство того, что проблема человеческого взаимопонимания относится к алгоритмически неразрешимым для человечества проблемам. При этом формируются общества, партии, союзы государств, в рамках которых проблема взаимопонимания как-то решается, возможно, на базе нестандартного «стандартного кодирования» для определенного сти-

---

36 Расторгуев С. П. Информационная война. – М: Радио и связь, 1999. – 416 С

37 Ахо А., Ульман Дж. – Теория синтаксического анализа, перевода и компиляции. Том 1. «Мир». М., 1978, с. 46

ля мышления и множества общих интересов. В то же время переход от одного типа «кодирования» мыслей и интересов к другому превращается в непроходимое болото, на преодоление которого можно положить всю жизнь и так и не добраться до противоположного берега. В научной литературе делаются попытки даже количественного измерения непонимания, в частности, Налимов пишет: «Непонимание всегда вызывает агрессию. Степень агрессивности, наверное, может быть мерой непонимания»[38]. Вся движущая эмоциональная сила европейской культуры – Христианство, отмечает Налимов, возникла из трагичности непонимания, обернувшегося распятием.

И в этом ракурсе время, отпущенное на решение той или иной задачи, становится одним из наиболее важных факторов, позволяющих перебираться с кочки на кочку в болоте неразрешимых проблем. Действительно, не всегда с выбранного наблюдательного поста хорошо видно, будет ли решение конкретного частного случая отображено в «Да» или «Нет» и будет ли оно вообще куда-то отображено – вполне возможно, что процесс «уйдет в бесконечность». Для решения таких проблем человечество выработало свой двойной стандарт: один – для вечных проблем с вечной душой, второй – для конечного земного существования.

А так как выбор субъективен и порой случаен – одно и то же иногда «Да», а иногда «Нет», то именно отсюда, из ограниченности во времени и идут разногласие и непонимание; «да-да, нет-нет, всё остальное от лукавого» (*Еклезиаст)*. Это «всё остальное» воспринимается «от лукавого» в том смысле, что наша конечная жизнь никогда не позволит нам перевести его в разряд познанного.

Поэтому, утверждая любой тривиальный факт, надо всегда помнить, что истинность во многом определяется сегодняшним временем. В зависимости от времени переписывается не только такая константа, как фактическая история человечества, но и математические теории, и даже старые избитые истины»[39].

Изучая тактику и стратегию ведения информационных войн, необходимо дополнить ряд базовых понятий, но при этом изменить систему кодирования. На данный момент, если перенести результаты исследований на любую популяцию животных либо Человечество в целом, напрашивается вывод -невозможно категорично утверждать, какое воздействие окажет полученное знание на информационную систему, какое знание останется, а какое забудется в процессе целенаправленного обучения. В этом смысле интересна английская поговорка, описывающая парадокс сознания: «The

---

38 Налимов В. В. – Спонтанность сознания: Вероятностная теория смыслов и смысловая архитектоника личности. «Прометей». М., МГПИ им. Ленина, 1989

39 Расторгуев С. П. Информационная война. – М: Радио и связь, 1999.

more we study – the more we know; the more we know – the more we forget; the more we forget – the less we know, that is why: the more we study – the less we know»/«Чем больше мы учимся, тем меньше мы знаем; чем больше мы знаем, тем больше мы забываем; чем больше мы забываем, тем меньше мы знаем – следовательно: чем больше мы учимся, тем меньше мы знаем».

Источник: dimlevich.com

Николай Романович Димлевич

Всё это означает, что наша классическая логика, базирующаяся на принципах машины Тьюринга, не позволяет со 100% гарантией не только предсказать ожидаемые события, но и с достаточной точностью управлять движением человечества или народа. Для решения этой задачи нужна другая логика, может быть, логика магии или религии, но не логика классической математики»[40]. Понятийный аппарат, который используется при изучении и определении информационных войн и их последствий, на данный момент не устоялся и полностью не сформирован. А при применении другой классификации возможно в будущем будет изменяться. На это может повлиять появление перспективного информационного оружия геоцентрического ТВД. Вероятно, необходимо будет принятие новых законодательных актов. Не исключено, что все это вкупе потребует и новых подходов в политике и новой редакции многих международных законов и договоров.

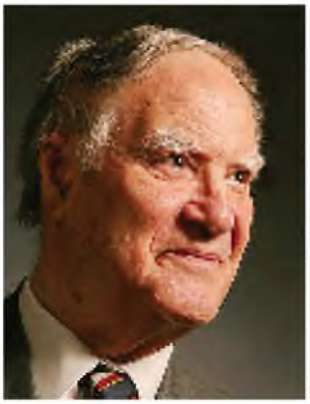
Сознание, вооружённое инструментом информации, является единственным источником управления материальными процессами и противостояния увеличению энтропии. Хотя усилиями некоторых операторов, выдающих информацию в виде намеренно неполной информации или целенаправленной дезинформации, происходит управляемое увеличение социальной энтропии – хаотизация глобального социума.

Дезинформацией (также дезинформированием) называется один из способов манипулирования информацией, как то – введение кого-либо в заблуждение предоставлением неполной информации или полной, но уже ненужной информации, искажения контекста, искажения части информации.

Главной целью направленного воздействия является стремление заставить оппонента изменить собственную точку зрения и поступить в соответствии с желанием манипулятора. При этом объект, против которого направлена дезинформация, может отказаться от принятия решения, невыгодного манипулятору или принять решение нужное манипулятору. Но, конечная цель – это предпринятое действие.

---

40 Гриняев Сергей (ЦСОиП) – Война в концептуальном пространстве. Открытый исследовательский и дискуссионный центр «Глобальная авантюра». Серия: «Глобальные проблемы», 15 марта 2012



Источник: vestnik.ulsu.ru

Сергей Петрович Капица

Источник: nptm.ru

Олег Николаевич Пивоваров

Источник: pushkin.ru

Александр Сергеевич Пушкин

Инициатором и финансистом злонамеренного манипулирования социально-политической информации является единый центр, природа и конечные цели которого определены в работах специалиста по сетевым информационным войнам Н. Р. Димлевича [41,42] и в работах В. Н. Спектора [43].

Хаотизация любой структуры – физической, биологической или социальной – является имманентным свойством её перехода из одного состояния в другое (например, аллотропные переходы в твёрдом теле). В работах О. Н. Пивоварова[44] показано, что важнейшим свойством любого биологического объекта является продуцирование и резервирование энергии, избыточной по отношению к обеспечению жизнедеятельности, на всех уровнях – от клеточного до уровня организма как целого. Эта избыточная энергия, в том числе может использоваться для актуализации информации как «содержания, полученного нами из внешнего мира в процессе приспосабливания к нему нас и наших чувств»[45].

Любой дефект на любом уровне биологической структуры, возникающий в результате травмы, заболевания или под воздействием неблагоприятных внешних факторов, включая нарушение когерентности подансамблей

41 Николай Романович Димлевич, заместитель главного редактора межрегиональной общественно-политической газеты «Северный Кавказ».

42 Например, «Вопрос об ударе по Ирану будет решать могущественное еврейское лобби США...» – Интервью АМИ «Новости-Азербайджан» с российским политологом Николаем Димлевичем и «Грузия, Запад и Россия в информационном противоборстве». 19.12.08. (www.fondsk.ru). Выступление на конференции «Международное радиовещание в современном мире» (Москва, 10 декабря 2008 г.). «Фонд стратегической культуры» и других

43 «Ортодоксальный иудаизм и проблемы глобальной стабильности»; «Политический, религиозный и этнический экстремизм, организованная преступность и терроризм как элементы единой системы дестабилизации планетарного социума» – Труды МАН ПНБ, т. т. 2 и 3 и других

44 Пивоваров О. Н., Пивоваров И. О., Кудрина Л. И. – Природа живых систем. НИА-Природа, 2002

45 Н. Винер – Кибернетика, или управление и связь в животном и машине. Советское радио. М., 2 изд.,1968; Наука. М., 1983

системы, является зародышем развития процесса хаотизации (возрастания энтропии системы), и только получение достоверной информации о характере дефекта (корректная диагностика) позволяет осознанно принимать меры по компенсации дефекта и пресечению процесса хаотизации.

На этом примере необходимо отметить, что в подавляющем большинстве случаев корректная диагностика немыслима в результате прямого, даже динамического получения информации о сложном биологическом объекте. Корректная диагностика всегда в большей или меньшей мере есть результат оценки получаемой информации по признакам релевантности сравнением с данными, полученными на других объектах с такими же (подобными) дефектами. Значимость такого подхода к оценке информации, впервые образно сформулированного А. С. Пушкиным, нашла отражение в эпиграфе к телевизионной передаче проф. С. П. Капицы:

О сколько нам открытий чудных
Готовит просвещенья дух
И опыт – сын ошибок трудных,
И гений – парадоксов друг.

На концептуальном уровне только такой подход применим к оценке информации о любой сложной системе (мировой социум) и протекающих в ней процессах (глобализация как дерево разнородных, в том числе конфликтующих тенденций, включая неизбежную хаотизацию[46]) – метод МАН ПНБ.

Мы утверждаем, что приведенное в Википедии утверждение о том, что «анализом информации занимается, прежде всего, наука логика» не соответствует современным реалиям. Аналитика как оценка достоверности, релевантности и значимости информации использует логику лишь как один, хотя и важный инструмент из множества других инструментов. Более важными инструментами являются определение встраиваемости полученной информации в общее информационное поле, то есть её принадлежность к определённому множеству информационных сообщений, и определение её релевантности исследуемым трендам. Большим подспорьем в реализации этого метода является встречный анализ участниками Академии – специалистами разных, подчас противоборствующих школ. Совпадение результатов является важным свидетельством корректности анализа[47].

---

46 Спектор В. Н. – Системный кризис в зеркале национальной безопасности. Труды МАН ПНБ, т. 1, М., 1999; первая редакция опубликована в Трудах Всероссийской конференции «Россия: государство и общество на пороге XXI века». М., 1997

47 Spector V. N., Walters M. B. – In: Joint Declaration on Dual Use Technologies of the delegations of the US National Academy of Sciences and Russian Academy of Sciences. NSF-NAN. Washington, D. C., USA, 1994; Спектор В. Н. и Уолтерс М. Б. – Бинокулярный взгляд на проблемы, связанные с технологиями двойного назначения. Труды МАН ПНБ, т. 1, М., 1999

Таблица. Страны, вызывающие беспокойство по поводу возможного распространения вооружений

Для США	*Для России*	*Для обеих стран*
Аргентина	*Афганистан*	
Боливия	*Азербайджан*	
Бразилия	*Латвия*	
Бирма	*Литва*	
Китай	*Китай*	*Китай*
Колумбия	*Ср. Азиатские республики*	
Куба	*Молдавия*	
Иран	*Иран*	*Иран*
Ирак	*Эстония*	
Индия	*Япония*	
Пакистан	*Пакистан*	*Пакистан*
Ливия	*Северный Кавказ*	
Никарагуа	*Польша*	
Югославия (сербы)	*Югославия (албанцы)*	*Югославия*
Чили	*Румыния*	
	Украина	

Оценки, приведенные в этой таблице, явились плодом совместного анализа и углубленного обсуждения по состоянию на 1993 год. Единственным неурегулированным разногласием стала Югославия. Авторам не удалось даже согласиться на исключение Югославии из рассматривавшегося списка.

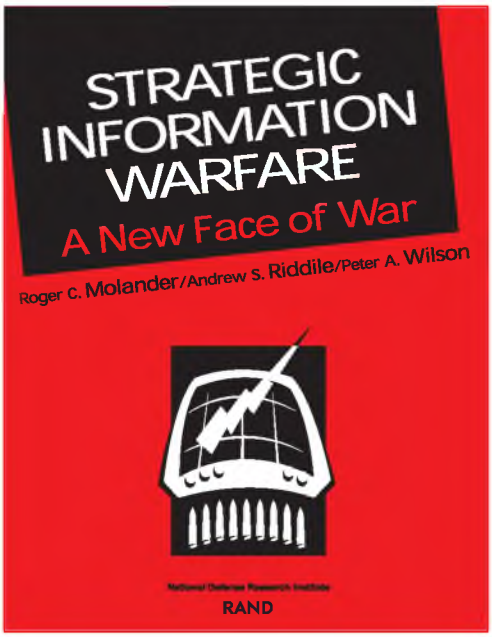
Несколько иной подход, основанный на сравнении предсказанных результатов с информацией, фиксируемой в динамическом режиме и подразумевающий предикативный волюнтаризм, выбирается «базовым вектором»[48] метода трендов, разработанного и практикуемого корпорацией РЭНД (США, 1948 – настоящее время)[49],[50].

---

48 Шеннон К. – Работы по теории информации и кибернетике (пер. с английского, под ред. Р. Л. Добрушина и О. В. Лупанова) – Изд. иностранной литературы, М,, 1963

49 Sperandeo Victor (Rand Management Corporation) – Trader Vic II – Principles of Professional Speculation

50 Molander Roger C., Riddile Andrew S., Wilson Peter A. – Strategic Information Warfare: a New Face of War. National Defense Research Institute/Report MR-661-OSD prepared for the Office of the Secretary of Defense/RAND. USA, 1996



Обложка отчёта MR-661-OSD выполнена Питером Сарьяно.

Титульный лист отчёта РЭНД корпорации MR-661-OSD

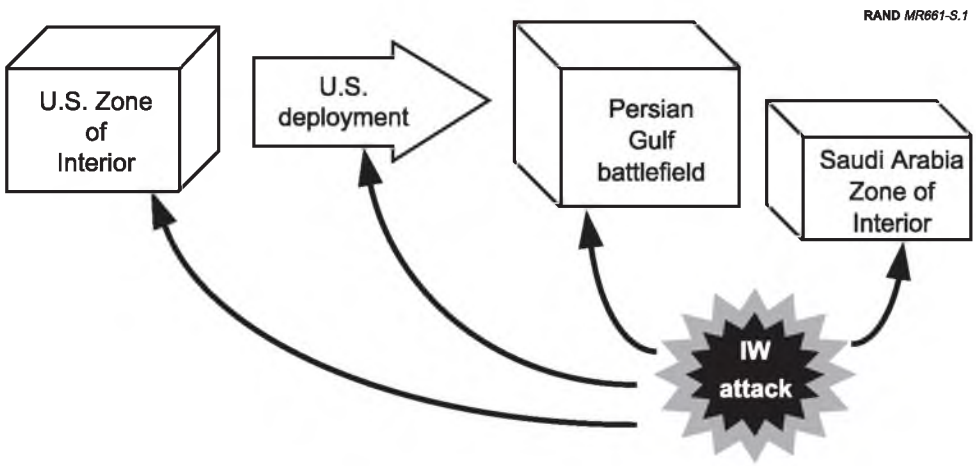


Figure S.1—The Changing Face of War: Four Strategic IW Theaters of Operation

Чёрная звезда – атака средствами информационной войны; *левый куб – зона внутренней территории США; стрелка – базы США; средний куб – ТВД Персидского залива;*
правый куб – зона внутренней территории Саудовской Аравии.

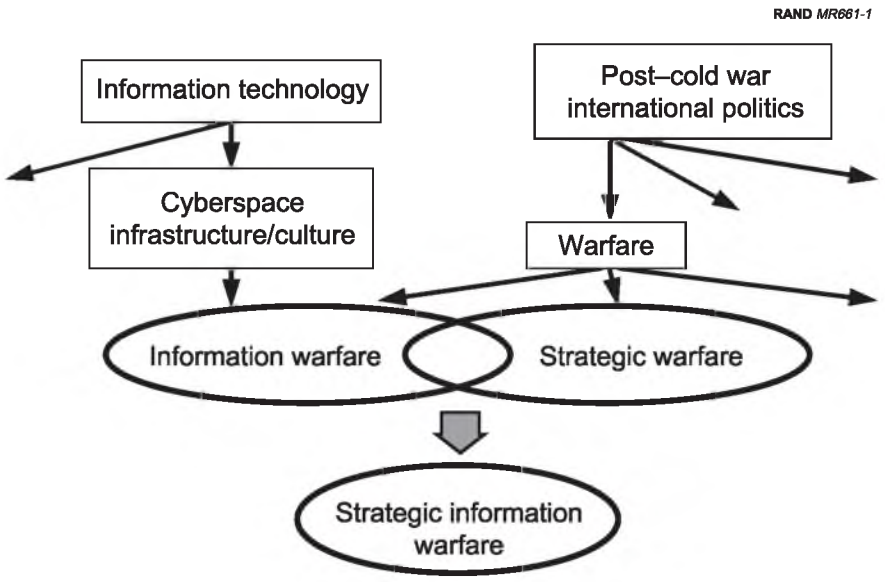


Figure 1—Strategic Information Warfare

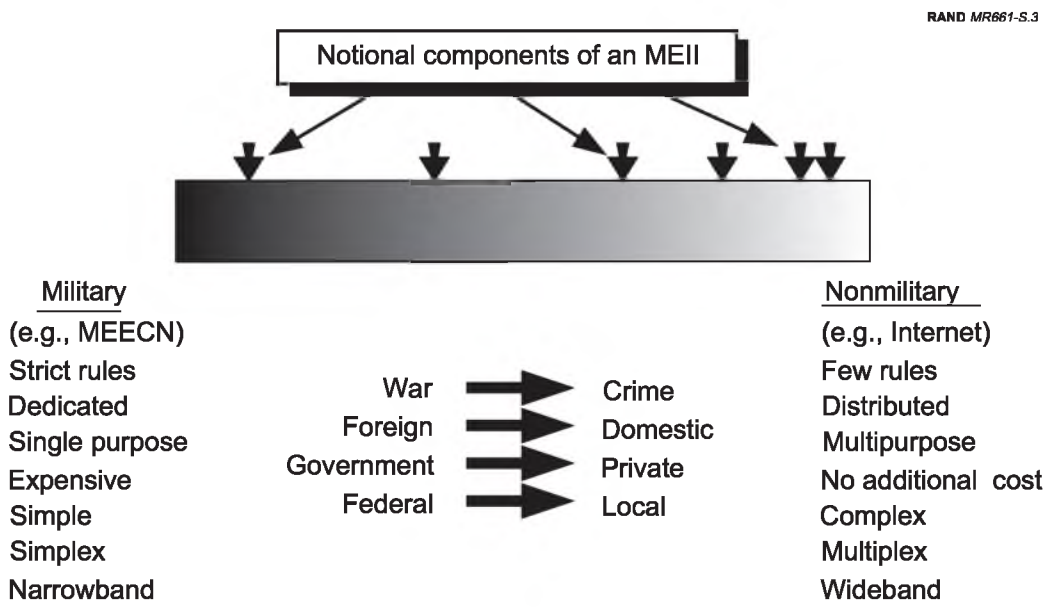
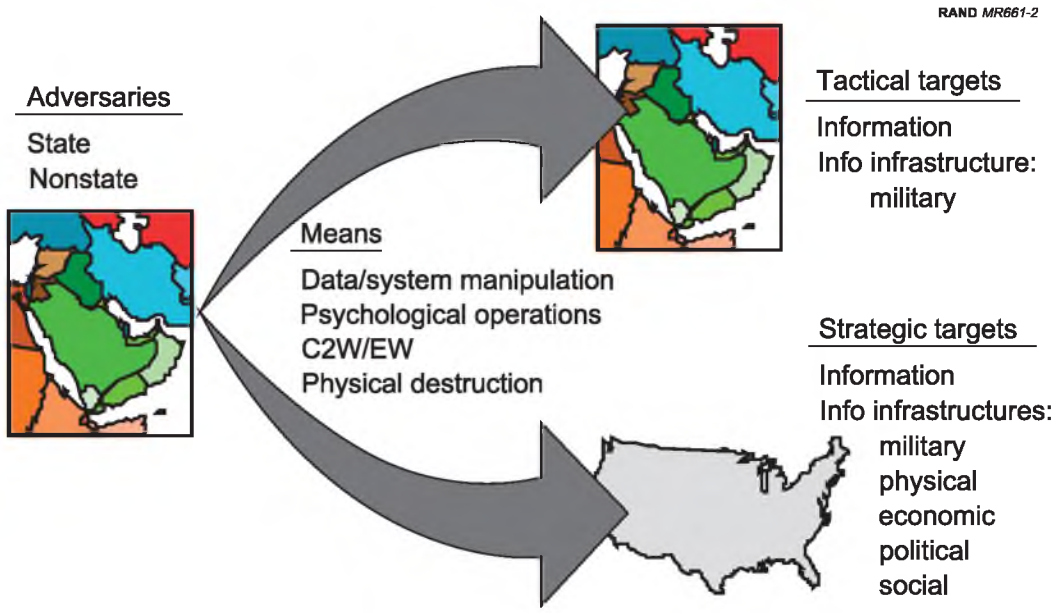


Figure S.3—A Spectrum of National Security Preparedness

Спектр мер готовности структур обеспечения Национальной безопасности.



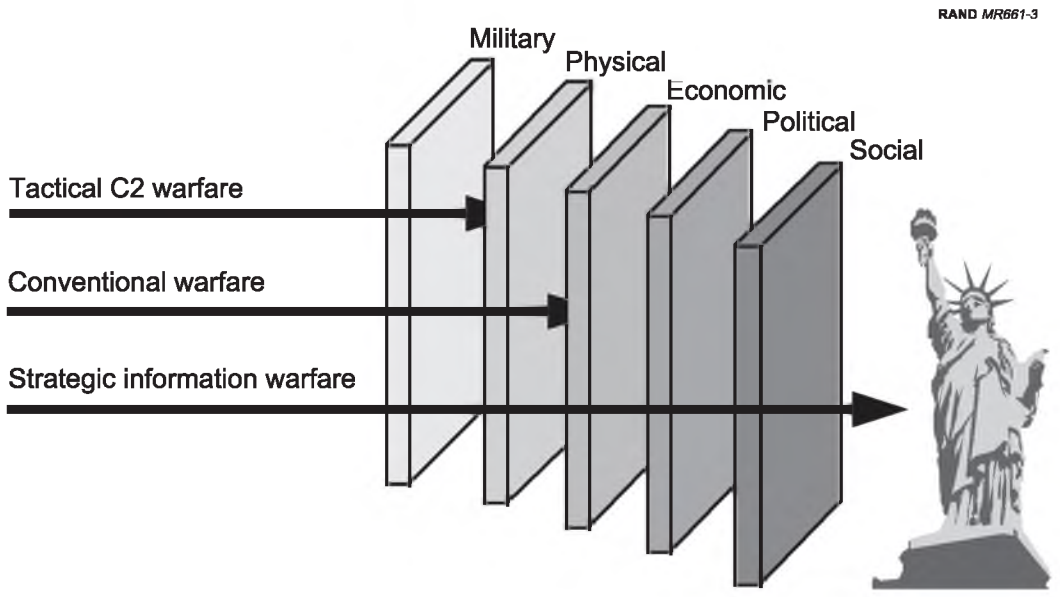


Figure 3—The Loss of Sanctuary

Evaluation of Scenarios for Exercise

Factors	Saudi Arabia	China
1. What's at stake in the crisis	Oil	Rapidly evolving global competitor
2. Avoiding a strong nuclear shadow	Strength of nuclear shadow a variable	Inescapable large nuclear shadow
3. Exercise development risk (within time available)	Start from tested structure and context (from counterproliferation studies)	New context and untested structure
4. Participant "adaption" to scenario	Persian Gulf conflict familiar; time frame more immediate	Strategic context unfamiliar; time frame longer; better for 2nd exercise
5. Avoiding provoking strategic offensive IW	Not necessarily tempting	More tempting
6. Preparation for addressing pressing "Next Steps in IW" issues	Covers more issues	Covers fewer issues

Оценка сценариев тестирования

RAND *MR661-11*

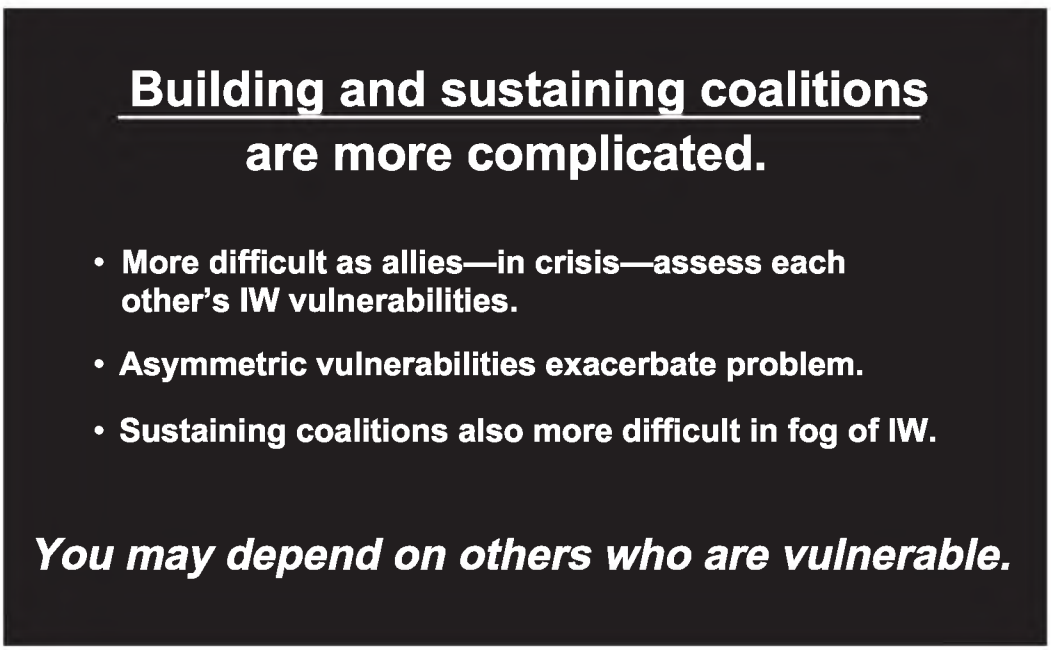


Figure 11—Building and Sustaining Coalitions Summary

(Создание и поддержание коалиций становится более сложным)

STEP TWO: The Day After...

Draft Memo for the President

The White House

24 May 2000

MEMORANDUM FOR: The President

FROM: The National Security Advisor

SUBJECT: The Crisis in Saudi Arabia and Related Information Warfare Issues

As requested this memorandum lays out the key issues for consideration at the 8:00 pm NSC Meeting on the crisis in Saudi Arabia.

OBJECTIVES

We would appear to have the following explicit near-term objectives in this context:

- To take whatever measures are necessary to forestall the collapse of the legitimate government of Saudi Arabia (including reassuring the Saudis that disruptive IW actions will not significantly affect our ability to meet our security commitments in the Gulf).

- To demonstrate clearly to the global community that the use of emerging strategic IW techniques does not constitute a legitimate means of effecting political change in any nation.

- To reassure the American and allied publics that threats to the security of their National Information Infrastructures and transportation systems can be effectively contained.

MILITARY AND STRATEGY ISSUES

A fundamental decision at this point in the crisis is whether we should seek to de-escalate this conflict (taking advantage of the Russian offer to work this problem in the UN Security Council) or continue to move forces into the region and take other actions on a timetable which recognizes the challenge of overcoming continuing Iranian, CIRD, and possibly domestic IW efforts.

(Форма меморандума Президенту США о ситуации на второй день после информационной атаки/the Day After approach).

Источник: old.redstar.ru

Олег Константинович Рогозин

Выше приводятся наиболее интересные примеры, иллюстрирующие результаты тестирования этой методики, выполненного в формате «день после» для анализа прогнозируемой ситуации на следующий день после атаки информационным оружием, как традиционным и современным, так и стратегическим перспективным информационным оружием в киберпространстве.

Интересно, что для такого тестирования выбран широкий театр военных действий: США – Персидский залив – Саудовская Аравия.

Это лишь один пример прикладных исследований стратегии и тактики ведения информационной войны, выполняемых корпорацией РЭНД в интересах вооружённых сил США.

Творчески переработанная теория трендов была применена доктором технических наук, генерал-лейтенантом авиации, проф. Рогозиным О.К.[51] (докторская диссертация) при планировании разработок (на 10-15 лет) систем новой техники, в первую очередь авиационных комплексов. Его метод основан на обработке и учёте информации об ожидаемых возможностях отечественной науки и промышленности (производственных трендах) на ближайшую и среднесрочную перспективу в рамках общей целевой функции получения изделий новой техники с опережающими мировой уровень тактико-техническими характеристиками. Это позволило, во-первых, достичь значительной экономии и, во-вторых, минимизировать эффект заложенного на этапе принятия решения о начале работ устаревания разработок на момент их приёмки и постановки на вооружение. Правда, его самый передовой метод проекции трендов на конкретные плоскости развития науки и технологий компрометировался объективно неоправданными трудностями внедрения соответствующих результатов завершённых разработок в промышленное производство.

Так, например, результаты работ по Стелс технологиям[52] в связи со срывом Н.И. Рыжковым (*«плачущим большевиком» – Интернет*) утверждения государственных программ работ по проблеме СТЕЛТС и стратегической авиации. Результаты этих работ не были внедрены, и не включены в технические отчёты и сохранились только в памяти разработчиков – ***непроявленная информация***.

---

51 Рогозин Олег Константинович, профессор, заместитель начальника Службы начальника вооружений МО СССР, д. т. н., г. н. с. ИХФ АН СССР

52 Михайлов В.М , Спектор В.Н. – Комплекс материалов и технологий для выравнивания поверхностной проводимости в изделиях новой техники. ИХФ АН СССР – ОКБ Сухого. М., 1986; Прохоров А.М. с сотрудниками – Генерация устойчивой гасимой плазмы в заантенных пространствах авиационных комплексов. ИОФ АН СССР – ОКБ Сухого. М., 1986; Спектор В.Н., Симонов М.П., Пахомов Л.Г. – Материалы и техника снижения ЭПР за счёт рупорных элементов авиационных комплексов. ИХФ АН СССР – ОКБ Сухого – ГГУ. М. – Горький. 1988

Одновременно невостребованными оказались и фундаментальные работы, связанные с открытием ферромагнетизма органических материалов и направленные на получение принципиально новых решений в области стелтс-технологий[53].

Несмотря на свёртывание этих работ и на неудавшуюся попытку команды М. С. Горбачёва по рассекречиванию работ включением в Государственную программу конверсии оборонного потенциала в области новых материалов и технологий (Госплан СССР, 1989), мировой уровень разработок в этом направлении пока остаётся ниже полученных более 20 лет тому назад результатов в интересах ОКБ Сухого. Это лишь один из многих примеров такого нерачительного отношения к науке, к учёным и к возникающей важной информации, бытовавшего в СССР, унаследованного и предельно возросшего в Российской Федерации.

Совершенно иная парадигма лежит в основе информационного противоборства в сфере международных отношений, имея, конечно, в виду не только и не столько официальную дипломатию, сколько и скорее создание желаемого образа государства в самых широких кругах мирового социума. Эта задача всегда решается предоставлением мировому сообществу тщательно подготовленной (совсем не обязательно полной и далеко не всегда правдивой – в советское время бытовала шутка, что в газету «Правда» не брали журналистов, которые даже в детстве или по ошибке говорили правду) информации о социальной обстановке в стране, об отношении национального социума к текущим мировым и историческим событиям и о видении руководством государства и народом ближайших, средне- и долгосрочных перспектив и конечной цели развития государства как составной части мирового сообщества наций.

Подготовка такой информации связана с рядом условий и ограничений. Прежде всего, она должна быть максимально приближена к внешней канве отражаемого события – «зеркало» не должно быть ощутимо кривым. Однако при подготовке информации к публичному представлению возможна и применяется техника изъятия мелких, как бы несущественных деталей

---

53 Овчинников А. А., Спектор В. Н. и другие – Полимерный ферромагнетик. Письма в ЖЭТФ (СССР), 1986, том. 43, вып. 6, с. 309; Ovchinnikov A. A., Spector V. N. et al – Organic Polymer Ferromagnet. Nature (L), 1987, vol. 326, p. 370; Овчинников А. А., Спектор В. Н. и другие – Пирополимерный органический ферромагнетик. Доклады АН СССР, 1988, т. 302, №4, с. 885; Ovchinnikov A. A. and Spector V. N. – Organic ferromagnetics. Synthetic Metals, 1988, m. 27, p. B615; Ovchinnikov A. A., Spector V. N. – Chemistry and Physics of Organic Polymer Ferromagnets. Frontiers of Macromolecular Science. IUPAC. Blackwell Sci. Publ., 1989, p. 445; Ovchinnikov A. A. – Magnetic phase of carbon. Nobel Simposium (NS 81): Conjugated Polymers and Related Materials, 1991, Part 6: Related concepts and materials, p. 453; Ovchinnikov A. A., Spector V. N. – Polymer Ferromagnet – an entry in Polymeric Materials Encyclopedia: F-G, vol. 4, p, 2320 ((72 p.)/Ed. J. C. Salamone. 1996. CRC Press, Inc., Boca Raton FL, ©Taylor&Francis Group, NY, USA; Овчинников А. А., Спектор В. Н., Боженко К. В. – Кластерный механизм возникновения отрицательного обменного взаимодействия в продуктах неполного сгорания углеводородов. Известия Академии наук (Россия). Сер.: физическая. 1997, т. 61, №5, с. 867

Источник: www.nd.m-necropol.ru

Михаил Петрович Симонов

Источник: isaran.ru

Александр Анатольевич Овчинников

Источник: pushkin.ru

Валерий Наумович Спектор

и дисторсии по перспективе картины. Такая техника должна реализовываться на основе воззрений Грегори Бейсона о том, что элементарная единица информации это «небезразличное различие» (the difference that makes a difference) или действенное различие для какой-то большей воспринимающей системы. Те различия, которые не воспринимаются, он называет «потенциальными», а воспринимаемые – «действенными». К этим определениям необходимо добавить, как было показано, «непроявленную информацию». Таким образом, любая информация состоит из небезразличных различий, а любое восприятие информации с необходимостью является получением сведений о различии.

При этом необходимо учитывать и тот факт, что в зависимости от исторической ретроспективы существует и дисторсия восприятия. Дисторсия восприятия, как национальным социумом, так и всем многообразием иностранных социумов и мировым сообществом в целом в значительной мере определяется существующей информационной средой, формируемой в первую очередь средствами массовой информации на основе действующих идеологем.

Задачи информационной борьбы в СССР достаточно эффективно решались всей системой государственных структур, координировавшихся Группой консультантов ЦК КПСС, формально в составе Отдела идеологии ЦК КПСС, но на деле подчинявшейся непосредственно Генеральному секретарю ЦК КПСС и пользовавшейся информационной поддержкой со стороны КГБ СССР, ГРУ ГШ ВС СССР, МИД СССР, МВД СССР, АН СССР и других ведомств. Помимо оперативного получения достижимо полной информации, в том числе по специальной доставке из агентурных источников, группа Печенева располагала впечатляющим бюджетом. Это позволяло содержать собственные средства распространения обработанной информации в значимых

Источник: www.pomnimas.ru

Грегори Бейсон (1904-1980)

д-р Меррилл Бовен Уолтерс (США)

Печенев Вадим Алексеевич

политических кругах и за рубежом, в первую очередь, но не исключительно в государствах СЭВ/ОВД, а также арендовать место и время в западных печатных и электронных СМИ. При своевременном получении информации о готовившемся «сливе» неблагоприятной информации о Советском Союзе последнее позволяло группе Печенева наносить упреждающий информационный удар, делавший либо бессмысленной, либо неэффективной медийную провокацию.

При осуществлении М.С. Горбачёвым политики разрядки эта группа была ***де факто*** распущена. СССР начал терпеть ощутимые поражения в информационном противостоянии, что в немалой степени способствовало развалу Советского Союза.

Методика Печенева после 1996 года без бюджетной поддержки использовалась авторами от имени международной некоммерческой общественной организации МАН ПНБ (Москва, учредители: бывший директор Международного штаба ядерного планирования НАТО д-р Меррилл Б. Уолтерс, США; бывший руководитель группы экспертов АН СССР в Госплане СССР, проф. Валерий Н. Спектор, РФ; бывший член ЦК КПСС, д-р Игорь А. Ильин, РФ; начальник отдела ОКБ МИГ, инж. Михаил А. Прудцев, РФ).

При получении информации, всесторонний анализ которой указывал на потенциально опасные, дестабилизирующие геополитические последствия, информационно-аналитические материалы рассылались в СБ ООН, Штаб-квартиру НАТО, ЦРУ США, ФСБ РФ и в Федеральное собрание России, а в необходимых случаях в службы безопасности Армении, Сербии, Республики Сербской (Босния), Арцаха (Нагорно-Карабахской республики) и Киргизии через участников Академии.

В ряде случаев само наличие таких материалов в конкурирующих службах обеспечивало отказ от проведения провокационных или дестабилизирующих

Источник: ru.wikipedia.org

Михаил Сергеевич Горбачёв

акций в «горячих» точках в связи с очевидными потерями в общественном мнении (в практике информационного противоборства – репутационные потери).

Наиболее свежим примером такой акции стала рассылка аналитически-информационного материала (*январь-февраль 2011*) о согласованной руководителями Армении, Азербайджана и России по инициативе Хилари Клинтон операции по ограниченному вторжению в апреле 2011 года азербайджанских войск на территорию Арцаха (Нагорно-Карабахской республики). Действительной конечной целью этой акции было размещение «миротворческих» контингентов НАТО/США в Нагорном Карабахе как элемента подготовки военной акции против Ирана. Информационное противостояние сыграло свою роль – вторжение не состоялось, хотя до сих пор, как убедился на месте один из авторов, сохраняется высокая интенсивность столкновений на линии разделения.

Государственные структуры Российской Федерации, ответственные за работу по информационной борьбе, не сумели в полной мере освоить технологию информационного противостояния, применявшуюся группой Печенева. Главной причиной невозможности работы по технологиям ЦК КПСС является отсутствие идеологической основы у российских структур, ответственных за ведение пропагандистской борьбы.

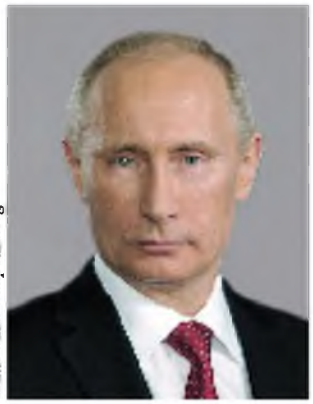
Как будет показано в следующих разделах настоящей работы, такие структуры, в том числе оперирующие на зарубежном информационном поле (*DigitalMetro. US; Daily Media; Око Планеты: Аналика-Информация*), вместо внятных идеологем и объявленной внятной и последовательной политики в области национальной безопасности и национальных интересов страны, пользуются ссылками на политическую фигуру В. В. Путина.

Приведём выдержки такого творчества, ориентированные на российские пропагандистские структуры, ряда авторов[54]. Эти публикации являются русским и английским вариантом одного текста, в котором приводятся суждения о позициях Путина на российской и международной сцене.

«Популярность Путина основывается на многочисленных факторах. Он ярый националист (что за бред! – он национальный лидер – *прим. авторов*), который неутомимо работает над улучшением уровня жизни простых (что такое непростые – это те, что воруют или те, что и не россияне вовсе? –

54 Sergiy Pozniy – За что Комитет по международным отношениям ненавидит Путина..»CounterPunch», США, 23.01.08 [http://www.counterpunch.com] и Майк Уитни – За что Journal Мердока любит Каспарова. «CounterPunch»: STRATEGiUM: ВЕССНА, США, 15 декабря 2007 года

прим. авторов) россиян и восстановлением былой славы страны. Он поднял более 20 миллионов русских из беспросветной нищеты, улучшил образование, медицинскую помощь и пенсионную систему …, национализировал имеющие государственное значение отрасли промышленности, уменьшил безработицу, увеличил уровень производства и экспорт, придал жизнеспособность российскому рынку, … улучшил общее качество жизни, снизил коррупцию в государстве и создал резервный фонд в размере $ 450 миллиардов.



Источник: wikipedia.org

Владимир Владимирович Путин

Россия больше не является легкой добычей …. Путин с этим покончил. Он восстановил контроль над … ресурсами страны, и он использует их для улучшения уровня жизни … народа. В этом состоит существенное отличие от 1990-х, когда … Ельцин, следуя вашингтонским неолиберальным эдиктам и продавая (скорее, раздавая[55]) жемчужины российской короны олигархам-стервятникам, завёл Россию в болото экономической катастрофы. Путин навёл в российском доме порядок; … усилил военно-экономические альянсы в регионе и устранил корпоративных гангстеров, которые по дешёвке растаскивали российские ценности. … Россия больше не продается.

Россия вновь стала одной из главных мировых держав … Её звезда постепенно поднимается, в то время как звезда Америки клонится к закату. … Путин определил курс социальных перемен, который входит в явное противоречие с основными посылами неолиберализма, являющимися основополагающими принципами международной политики США. Он не принадлежит к корпоративно-банковскому братству, которое свято верит в то, что все богатства мира должны принадлежать ему, невзирая на причинённые … страдания и разрушения. Интересы Путина подчинены России: российское благосостояние, российский суверенитет и место России в мире. Он не глобалист.

Вот почему … Россия как возрождающаяся [империя] видится как потенциальный конкурент империалистическим амбициям США…

В ранние годы президентства Путина, верилось, что он согласится с требованиями Запада и признает подчинённое положение в системе, центром которой является связка США-ЕС-Израиль. Но этого не произошло. Путин упрямо защищал независимость России и препятствовал интеграции в доминировавшую систему.

---

55 Спектор В. Н. и Воевода Ю. Е. – Подайте вору, Христа ради. Труды МАН ПНБ. М., 1999, т. 1, с. 75

Наиболее влиятельный среди вашингтонских аналитических центров – The Council on Foreign Relations, CFR (Комитет по Международным Отношениям) – определил проблему достаточно рано и решил, что российская политика США должна быть полностью переработана.

Джон Эдвардс (John Edwards) и Джэк Кемп (Jack Kemp) были назначены лидерами группы CFR …. Так зародилась идея о том, что Путин «отступает от демократии». В их статье «Неправильное направление России» («Russia's Wrong Direction») Эдвардс и Кемп утверждают, что «стратегическое партнёрство» с Россией более невозможно.

<…> на Путина кричат (неудачное, а, главное, неверное утверждение – прим. авторов) за «отход от демократии», в то время, когда вассал Америки Михаил Саакашвили своевольно объявляет чрезвычайное положение и посылает своих размахивающих дубинками робокопов избивать протестующих до потери сознания перед отправкой в грузинский ГУЛАГ.

Настоящим преступлением (по мнению западных СМИ – прим. авторов) Путина является его служение национальным интересам России, а не интересам глобального Капитала. Он также отвергает вашингтонскую модель однополярного мира. Как заявил он сам в Мюнхене: «Модель однополярного мира означает мир, у которого один хозяин, один суверен, один центр власти, один центр силы, один центр принятия решений. В итоге это несёт опасность не только всем, находящимся внутри системы, но и самому суверену, который разрушает себя изнутри. Что более важно, эта модель порочна по своей сути и не может являться моральным фундаментом современной цивилизации».

И далее: «Мы наблюдаем всё большее и большее неприятие базовых принципов международного права… Мы являемся свидетелями почти неограниченного гипертрофированного применения силы – военной силы – в международных отношениях, силы, которая толкает мир в пропасть перманентных конфликтов. Я убеждён, что настал решающий момент, когда нам необходимо серьёзно задуматься по поводу глобальной безопасности» (В. В. Путин, мюнхенская речь)».

Все эти пассажи, являются скорее агитацией, а не развернутой программой пропаганды, что в условиях информационной войны недостаточно. Это, скорее, пусть и заслуженное, восхваление тактических мер

Совершенно неприемлема ситуация, когда Российская Федерация является соучредителем международной медийной организации, но практически не участвует в определении редакционной политики. В результате освещение российской жизни и политической позиции Российской Федерации по важнейшим политическим и геополитическим вопросам, например, на телевизионном канале «Евроньюс» слишком часто имеет негативную окраску

или вообще замалчивается. Было бы смешно, если бы не было так грустно, что до самого последнего времени давно покойный, жестикулирующий Каддафи следовал сразу же за жестикулирующим подобным же образом Медведевым.

Источник: ru.wikipedia.org

Джон Едвардс

Отражение событий в Косово и в ходе грузино-югоосетинского конфликта 08.08.08, в Ливии и в Сирии было и остаётся направленным на дискредитацию России. Более того, новостные передачи по внутриполитическим событиям в России, как правило, дают одностороннюю трактовку взаимоотношения власти и так называемой «оппозиции». За российские деньги Россию же и малюют чёрным при странном непротивлении российской редакции «Евроньюс».

Источник: gate.sinovision.net

Джек Кемп

Такая методика информационного противостояния, даже в случае самого эффективного исполнения, сводится к апостериорной реакции на информационную провокацию, слив дезинформации, сетевые акции и т. п. Однако беда заключается ещё и в том, что эффективность исполнения даже задач апостериорного противодействия оказывается по-прежнему запоздалой, некачественной и малоэффективной[56].

Такая методика информационного противостояния не соответствует реалиям необходимости готовности к информационной войне, уже в широких масштабах ведущейся США в странах Магриба и Ближнего Востока, со многими странами Евросоюза и с Евросоюзом как с крупной межгосударственной организацией, обладающей собственной резервной валютой. Эта информационная война как продолжение «холодной войны» с СССР на новом идеологическом и техническом уровне серьёзно затронула интересы Российской Федерации.

Следующее определение вышло из стен кабинета Директора информационных войск Министерства обороны США: «Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в обеспечении национальной военной стратегии путём воздействия на информацию и информационные системы противника с одновременным укреплением и защитой нашей собственной информации и информацион-

56 Illine I.A. and Spector V.N. – Think tanks and civil society in Russia. World Bank Conference. Barcelona, Catalonia, Spain

ных систем. Информационная война представляет собой всеобъемлющую, целостную стратегию, призванную отдать должное значимости и ценности информации в вопросах командования, управления и выполнения приказов вооружёнными силами и в реализации национальной политики. Информационная война нацелена на все возможности и факторы уязвимости, неизбежно возникающие при возрастающей зависимости от информации, а также на использование информации во всевозможных конфликтах.

Объектом внимания становятся информационные системы (включая соответствующие линии передач, обрабатывающие центры и человеческий фактор этих систем), а также информационные технологии, используемые в системах вооружений. Информационная война имеет наступательные и оборонительные составляющие, но начинается с целевого проектирования и разработки своей «Архитектуры командования, управления, коммуникаций, компьютеров и разведки», обеспечивающей лицам, принимающим решения, ощутимое информационное превосходство во всевозможных конфликтах»[57].

И. И. Завадский справедливо утверждает, что «информационная война – всеобъемлющая, целостная стратегия, обусловленная всё возрастающей значимостью и ценностью информации в вопросах командования, управления и политики»[58].

Следует отличать информационную войну от компьютерной преступности. Любое компьютерное преступление представляет собой факт нарушения закона. Но нарушение может быть не преднамеренным, а может быть и осознанным, заранее подготовленным; может быть единичным и обособленным, а может являться отдельно взятой частью глобального плана кибер проникновения. При этом, случайным или обособленным ведение информационной войны никогда не бывает (хотя, с позиций стороны агрессора, такие действия нарушением закона могут даже и не являться). Вместе с тем, как и всякая война подразумевает применение оружия, так и информационная, предполагает для ведения боевых действий использовать информацию в качестве оружия. А сфера согласованного применения этого вида оружия может быть чрезвычайно разнообразной – как в экономической, политической или социальной сферах так и в реальном театре военных действий». Важно подчеркнуть, что нарушение международных соглашений, подписанных и ратифицированных страной, автоматически становится нарушением национального закона, и это в полной мере относится к исследованиям и разработкам методов и средств ведения информационной войны, предусмотренным военным руководством США.

---

57 http://www.5ka.ru/16/2772/1.html

58 Завадский И. И. Информационная война – что это такое? // Конфидент. Защита информации – 1996.

Реальности сегодняшнего дня заставляют всерьез задуматься над поставленным И. И. Завадским вопросом о безопасности информационных систем. Опасность для последних заключается не столько в предпринимаемых действиях недовольных сотрудников или доморощенных юнцов-хакеров. Уже одно появление и применение термина значит переход на качественно иной уровень, когда существует потенциальная опасность противостояния угрозам внутренних и внешних враждебных сил.

Муамар Каддафи
(из заставок Евроньюс)

Обратимся к источникам в США.

Ставшее достоянием общественности «Пособие Института компьютерной безопасности по компьютерной преступности и информационной войне: существующие и потенциальные угрозы» дало повод к бурному обсуждению в среде не только независимых экспертов по информационной безопасности, научных и академических кругов, но также органов национальной безопасности, военных ведомств и правоохранительных органов. Комитет Сената США по правительственным делам не ограничился констатацией факта появления «Пособия..», а организовал слушания по компьютерной безопасности. Перед специально созданной в Министерстве юстиции «Группой обеспечения кибербезопасности» (Cyber SecurityAssurance Group), была поставлена задача содействовать защите компьютеров от проникновений в информационном пространстве, не оставлять без внимания ни одной чрезвычайной ситуации, и проводить расследования всех диверсии кибертеррористов. В течение года специалисты созданной группы должны были выработать программу действенных мер по достижению безопасности киберпространства.

Мартин Либики (старший научный сотрудник Рэнд Корпорейшен) из Университета национальной обороны высказался так: «Попытки в полной мере осознать все грани понятия информационной войны напоминают усилия слепых, пытающихся понять природу слона: тот, кто ощупывает его ногу, называет её деревом; тот, кто ощупывает хвост, называет его канатом и так далее. Можно ли так получить верное представление? Возможно, слона-то и нет, а есть только деревья и канаты. Одни готовы подвести под это понятие слишком много, другие трактуют какой-то один аспект информационной войны как понятие в целом…»[59].

59 Libicki M. C. The mesh and the net: Speculation on armed conflict in a time of free silicon. Washington: National defense university, 1994

Это мнение свидетельствует о том, что окончательная формулировка пока не выкристаллизовалась, но процесс идёт. Необходимо добавить, что мнение научного сотрудника не вполне соответствует политике Рэнд Корпорейшен, серьёзно и большими силами включившуюся в разработку и тестирование методов ведения информационной войны, о чём, в частности свидетельствует пространный отчёт MR-661-OSD по контракту DASW01-95-C-0059, выполнявшемуся по гранту Федерального правительства и поддерживавшегося Офисом Секретаря по обороне, Объединённым штабом и оборонными ведомствами США[60].

В разработках боевые действия в информационной войне не ограничиваются привычными рамками полей сражений, а разворачиваются на обширном театре, который включает и домашний компьютер рядового пользователя и секретные кабинеты военного ведомства, аэрокосмические станции и лаборатории университета.

Информационные войны и новая историческая реальность – «планируемая история».

Рассматривая новую историческую реальность, известный русский общественный деятель А. А. Зиновьев в своей книге «Русский эксперимент (в разделе «Планируемая история») так описывает воздействие информационного противостояния на развитие исторических событий: «Теперь история не происходит по своему капризу, стихийно. Она теперь делается сознательно, можно сказать – по заказу сильных мира сего».

Причины, по которым это стало возможным, Зиновьев видит в следующем:

1) прогресс средств сбора, обработки и передачи информации;

2) прогресс средств коммуникаций;

3) прогресс средств манипулирования людьми, надзора за ними, пресечения массовых движений;

4) влияние массовой культуры на стандартизацию образа жизни людей.

Всё сказанное привело к тому, что «Степень непредвиденности и неожиданности исторических событий резко сократилась сравнительно с резко возросшей степенью предсказуемости и запланированности.

Холодная война Запада, возглавляемого США, против коммунистического Востока, возглавляемого Советским Союзом, была с самого начала грандиозной запланированной операцией, по затратам, размаху и результатам самой грандиозной человеческой операцией глобального масштаба. В ней было много незапланированного, непредвиденного, неподконтрольно-

60 *Molander R. C. et al, RAND. 1996*

го, что неизбежно даже в мелких операциях. Но в целом, в главном, в определяющих ход процесса решениях она была именно такой»[61].

Об этом же говорил и У. Колби – бывший директор ЦРУ США, разработавший и проводивший в своё время операцию по свержению правительства С. Альенде в Чили. В своём интервью он назвал эту операцию «лабораторным экспериментом по использованию финансовых средств для дискредитации и смещения иностранного правительства». Использованные финансовые средства определили, кто и что должен говорить, а тем самым определили содержание и направление информационных потоков. Говорят, что по коридорам Пентагона гуляет такая шутка: «Информационная война – что это такое?» – «О, это компьютерная безопасность плюс деньги». Можно сказать ещё, что информационная война – это компьютерная безопасность плюс взвешенное отношение к принимаемым решениям.

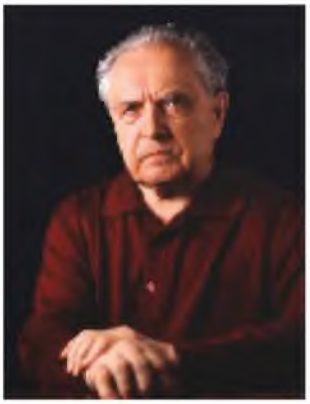
Проф. Гельман[62] полагает, что с позиции проведения масштабной информационно-психологической войны «создание панарабского телеканала «Аль-Джазира» следует считать блестящим стратегическим и тактическим ходом эмира Хамада бин Халифа ат-Тани». Показательно, что в 1995 году, то есть за год до выхода первой передачи на этом канале, специалист по информационным войнам Мартин Либики из Национального института обороны США предсказывал резкое возрастание роли международных телевизионных каналов в инициировании, реже в сдерживании военных конфликтов.

В «Аль-Джазире», подобран высокопрофессиональный состав, который не только выполняет свою прямую задачу – информировать, но и умело подает дезинформацию, грамотно проводя пропаганду, формируя и манипулируя мнением зрителей и читателей. Широко декларируемые журналистским сообществом принципы объективности, всесторонности здесь не могут воплощаться в жизнь по определению. Телеканал вещает на английском и арабском языках, но проводимая этим средством массовой информации политика подконтрольна и определяется семьей эмира Катара. Именно канал «Аль- Джазира» сыграл большую роль в милитаризации сферы электронных СМИ, и еще большую, в организации потока арабских революций. Нередко можно услышать и прочитать о том, что «Аль-Джазира» события в Сирии трактует односторонне. Материалы подбираются так, чтобы легитимное правление президента Башара Асада выставить в неприглядном свете, а значит, и осудить, а оппозиционеров показать борцами за права граждан, свободу и независимость. Подобного стиля «Аль-Джазира» придерживается не только в отношении Сирии,

---

61 Зиновьев А.А. «Русский эксперимент»,. 1995., Издательство: L'Age d'Homme – Наш дом

62 проф. Гельман Захар (Израиль) – Эмират, «Аль-Джазира» и верные полки солдат: Катар стремится к доминированию в арабском мире. Независимая газета: Независимое военное обозрение. 30 марта 2012 г. [http://nvo.ng.ru/forces/2012-03-30/1_katar. html] (раздел «Аль-Джазира» – оружие массового разложения)



Источник: ru.wikipedia.org

Александр Александрович Зино́вьев

Источник: ru.wikipedia.org

Уильям Иган Колби (1920 – 1996)

Источник: vovizit2008.narod.ru

проф. Гельман Захар

но и в публикации материалов обо всем арабском мире. Нередко журналисты телеканала получали предупреждения из соседних государств Кувейта и Объединенных Арабских Эмиратов (ОАЭ), а некоторые и вовсе были лишены аккредитации, за то, что материалы из этих стран, передаваемые по катарскому телевидению, инициировали такое поведение людей, когда в вооруженное столкновение могли перерасти вполне мирные акции протеста.

Руководители арабских государств достаточно быстро оценили роль «Аль – Джазиры» в нагнетании напряженности, тем паче, что тенденциозно подобранные материалы однозначно говорили о симпатиях к радикальным и экстремистским группировкам. А затем предсказуемо пришли к выводу о необходимости появления альтернативы. 3 марта 2003 года из Дубая началось вещание «Аль-Арабия», ещё одного панарабского телеканала, который был создан благодаря совместным усилиям ливанского миллиардера и значимого политического деятеля Рафика Харири (убитого в 2005 году в ходе теракта), Кувейта и ОАЭ. Но новорожденному СМИ пришлось не просто, так как информационная ниша была уже занята и «Аль Арабия» пришлось потратить много сил, чтобы выстоять в конкурентной борьбе и отвоевать свое информационное поле у соперников.

Можно смело допустить, что вещающие на большое количество стран телеканалы, играют существенную роль в сетецентрических (инструментальная разновидность геоцентрических) конфликтах и войнах, когда в силу системного информационного превосходства будет достигаться победа одной из сторон. На сегодняшний день оба арабских телеканала активно распространяют свое вещание на все большую аудиторию, завоевывая информационное пространство. А телевизионные профессионалы и те, кто стоит за ними и руководит ими, определяя направления информационных ударов, искусно разжигают огонь людского недовольства, усиливая стремление к радикализму, превращая в кровавые конфликты мирные демонстрации.

Источник: lenta.ru

Хамад бин Халиф ат-Тани

Источник: inosmi.ru

Вада (Вадах) Ханфар

Источник: mishmar.info

Рафик Бахаеддин Харири

1.1 РЕВОЛЮЦИЯ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ.

Отмеченные в общей части Введения особенности восприятия и оперирования информаций в последней четверти XX века претерпели кардинальные, революционные изменения. Бурный прогресс в области компьютерных технологий и в совершенствовании систем передачи информации привёл к резкому увеличению общего объёма доступной информации (информационный взрыв), к увеличению потока новой информации, к радикальному возрастанию скорости передачи информации и к уменьшению скорости доступа к ней.

Информационный взрыв

– постоянное увеличение скорости и объёмов публикаций (объёма информации) в масштабах планеты.

М. Н. Эпштейн совершенно справедливо утверждает, что «Информационный взрыв таит в себе не меньшую опасность, чем демографический. По Мальтусу, человечество как производитель отстаёт от себя же, как потребителя, то есть речь идёт о соотношении совокупной биологической массы и совокупного экономического продукта человечества. Но в состязании с самим собой у человечества всё же гораздо лучшие шансы, чем у индивида в состязании со всем человечеством. Как выясняется к началу третьего тысячелетия, основные ресурсы общества – не промышленные или сельскохозяйственные, но информационные. Если материальное производство человечества отстаёт от его же материальных потребностей, то ещё более отстаёт информационное потребление индивида от информационного производства человечества. Это кризис не перенаселённости, а недопонимания, кризис родовой идентичности. Человечество может себя прокормить, но может ли оно себя понять, охва-

тить разумом индивида то, что создано видовым разумом? Хватит ли человеку биологически отмеренного срока жизни, чтобы стать человеком?»[63] (это кому как – Гастелло, например, для этого хватило и двадцати с небольшим лет)».

Хотя это психоделическое и эсхатологическое произведение целиком построено на ложных философских посылах и на психологии духовной «расчленёнки», одно из его положений имеет конкретное значение, конечно, не в приложении к человеку, не задействованному в манипуляциях информационной войны, а применимо именно к оператору систем информационного оружия. Оно состоит в том, что, если такой оператор вычисляется оппонирующей стороной и становится виртуальной мишенью противника, то превышение темпа его загрузки предположительно значимой, но разнородной информацией с темпом выше определённого уровня неизбежно приведёт к срыву его способности контролировать боевую информационную машину.

Революция в современных информационных технологиях имеет три основных особенности, главным образом связанные с темпоральными (временными) факторами.

Во-первых, независимо от пространственного фактора передача информации происходит быстрее ($\tau_1 \leq 1$ мс), чем осознание оператором самого факта её получения (у военного лётчика-испытателя $\tau_2 \geq 200$ мс), тем более, осознание значимости её содержания.

Во-вторых, дополнительным фактором временного отставания осознания значимости получаемой информации является оценка её конгруэнтности (пополнения знаний) или инконгруэнтности (новых знания) референтной системе архивных данных, а также проверка её релевантности задачам, назначенным конкретному оператору. Этот фактор имеет жизненно важное значение при обработке внешнеполитической и военно-политической информации. Это, в первую очередь относится к Интернету как к сетевому информационному ресурсу, где объективная и /или значимая информация щедро разбавляется откровенной дезинформацией, провокационными и подрывными (особенно в области культуры и социальных процессов) информационными сообщениями, такими, например, как упоминавшаяся статья постмодернистского культуртрегера.

И, наконец, в третьих, большое значение имеет экстенсивный фактор, когда сечение потока получаемой в единицу времени релевантной информации (прочая может отсеиваться техническими средствами) превышает возможности обзора оператором. В таком случае возникает необходимость введения в технологию обработки информации медленного процесса ранжировки поступающей информации по её значимости для сужения поля обзора по закладываемым в компьютер смысловым и семантическим критериям.

---

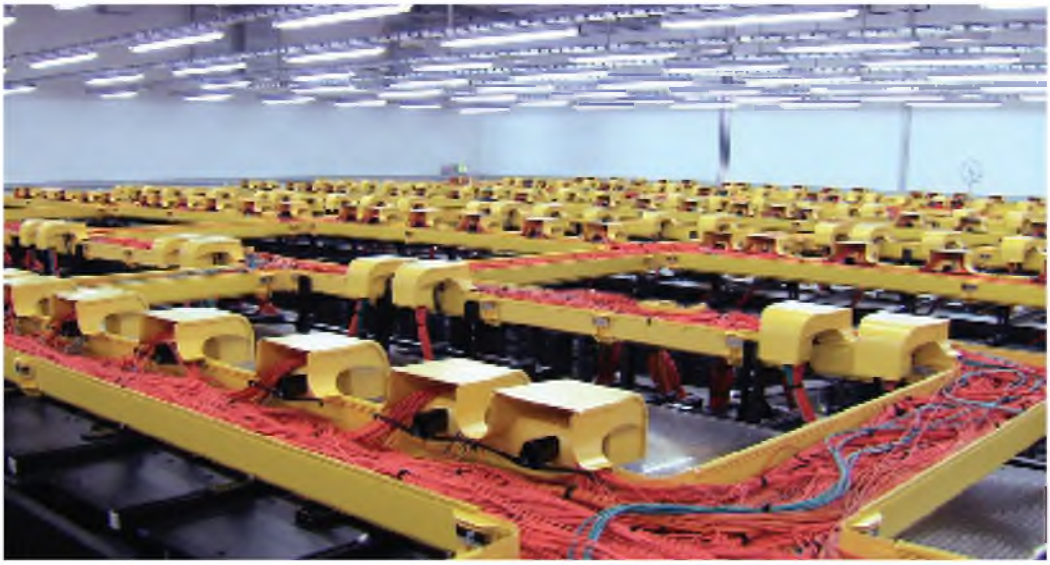
63 Эпштейн М.Н. – Информационный взрыв и травма постмодерна. Русский журнал, 29.10.1998, Эморийский университет, Атланта, США

Источник: www.ozon.ru

Михаил Наумович Эпштейн

В принципе, технические возможности современной вычислительной техники (например, европейский супер-МУК – с быстродействием $4{,}9 \cdot 10^{15}$ бит·с$^{-1}$, размещение которого потребовало строительства специального здания) позволяют справляться со всеми отмеченными видами темпоральных факторов. Однако в обозримом будущем трудно надеяться на получение необходимого и достаточного программного обеспечения для решения всего спектра проблем, возникающих в связи с этими факторами, и если мы не можем полностью доверять оператору, то мы точно не можем позволить себе доверять искусственному интеллекту самообучающегося компьютера. Хотя в понимании кибернетики человек-оператор является неформализуемым фактором, что снижает надёжность информационно-вычислительной структуры и повышает риск системного отказа, участие оператора является на настоящем этапе развития компьютерных комплексов единственной гарантией обеспечения их работоспособности в случае информационной атаки или возникновения иного спровоцированного извне неформализуемого фактора, то есть фактором снижения уязвимости элемента информационной системы в условиях информационной войны.

Совершенно ясно, что в настоящее время, в условиях темпоральной информационной революции, на первый план выходит не скорость передачи информации в глобальном информационном поле, так как она уже на поряд-



Европейский суперкомпьютер супер-МУК

ки опережает скорость осознания её получения, а скорость её обработки и предоставления лицам, принимающим решения, в достоверном, надёжном и удобном для понимания виде.

Палеативное решение возникающих проблем технологически и логистически может быть достигнуто выполнением ряда мероприятий, в первую очередь следующими из них:

– переходом от эстафетной к веерной передаче стратегической информации, при этом стратегический характер определяется по заданным критериям (источник информации, ключевые семантические паттерны и другие) специальными программными блоками;

– созданием системы независимого он-лайн и регистрируемого (для последующего анализа характера и причин допущенной ошибки) контроля неформализуемого фактора (оператора);

– разработкой системы мгновенного (параллельного) доступа к релевантным архивным данным;

– созданием на базе современного самообучающегося суперкомпьютера, предпочтительно национального производства (важность этого фактора будет оценена в последующих разделах работы), ситуативного центра оценки и распределения релевантной информации по иерархическим структурам государственного управления.

Выбор этих мероприятий, безусловно, не является ни единственным, ни наилучшим – он является на данный момент оптимальным по параметру доступности и оперативной выполнимости адаптирующих мероприятий.

Скорость передачи информации.

Скорость передачи информации – скорость передачи данных, выраженная в количестве бит, символов или блоков, передаваемых за единицу времени. Теоретическая верхняя граница скорости передачи информации определяется теоремой Шеннона-Хартли.

Рассматривая все возможные многоуровневые и многофазные методы шифрования, теорема Шеннона-Хартли утверждает, что ёмкость канала C, означающая теоретическую верхнюю границу скорости передачи информации, которые можно передать с данной средней мощностью сигнала **S** через один аналоговый канал связи, подверженный аддитивному белому гауссовскому шуму мощности **N** равна:

$$C = B \log_2 \left(1 + \frac{S}{N} \right),$$

где: **C**— ёмкость канала в битах в секунду; **B** – полоса пропускания канала в герцах; **S** – полная мощность сигнала над полосой пропускания; **N** – полная шумовая мощность над полосой пропускания; **S/N** – отношение сигнала к шуму – (SNR) сигнала к гауссовскому шуму, выраженное как отношение мощностей.

Методы повышения скорости передачи информации.

Одним из способов повышения скорости передачи информации является применение адаптивных антенных решёток со слабо коррелированными антенными элементами. Системы связи, которые используют такие антенны, получили название MIMO системы (Multiple Input Multiple Output)[64].

Другим способом повышения скорости передачи информации является метод конволюции – деконволюции сообщений по согласованному алгоритму. Любой человек, даже не подозревая об этом, знаком с понятием алгоритма.

Первые в истории человечества правила решения арифметических задач, названные тогда алгорифмами, были разработаны известным учёным древности Аль-Хорезми в IX веке нашей эры. В честь его работ формализованные правила для достижения какой-либо цели называют алгоритмами.

Чтобы обработать информацию необходимо найти способы построения и оценки вычислительных и управляющих алгоритмов (по- возможности, универсальных). Все это является предметом изучения теории алгоритмов. В ней же возникло и понятие автомата. Если есть универсальные алгоритмы для решения вычислительных задач, то логично предположить, что существуют, (хотя бы абстрактно) некие механизмы или устройства, для решения таких алгоритмов. Одним из таких устройств может являться абстрактная машина Тюринга, которая считается неформально определённым автоматом и рассматривается в теории алгоритмов. А предметом теории автоматов является теоретическое обоснование построения таких устройств. Понятийный и теоретический аппарат теории вероятностей, теории графов, комбинаторного анализа, алгебры, математической логики, широко используется в теории автоматов.

Теория автоматов вместе с теорией алгоритмов являются основной теоретической базой для создания электронных вычислительных машин и автоматизированных управляющих систем.

---

64 Флаксман А. Г. – Адаптивная пространственная обработка в многоканальных информационных системах. Диссертация на соискание учёной степени доктора физико-математических наук. М.: РГБ, 2005 (Из фондов Российской Государственной библиотеки), стр. 5

Источник: www.biometrica.tomsk.ru

Андрей Николаевич Колмогоров 1903-1987

Современное научное понятие алгоритмов как способов обработки информации введено в работах Э. Поста и А. Тьюринга в 20-х годах XX века (Машина Тьюринга). Большой вклад в развитие теории алгоритмов внесли русские ученые А. Марков (нормальный алгоритм Маркова) и А. Колмогоров[65].

Однако эта техника требует значительных затрат времени на шифровку и дешифровку передаваемых сообщений. Эта техника хорошо освоена в технологии компьютерного архивирования, но в технологии передачи информации она преимущественно применяется для сокрытия контента с использованием техники спутникового транзита разведслужбами и их агентами.

Впервые в СССР факт передачи за рубеж секретных научно-технических данных из АН СССР таким методом был отмечен после ликвидации в конце 80-х годов XX века Специального управления Президиума АН СССР (КГБ СССР) по инициативе Главного учёного секретаря Президиума АН СССР/РАН академика И.М. Макарова (бывший заместитель заведующего отделом науки и учебных заведений ЦК КПСС, бывший заместитель министра высшего и среднего специального образования СССР по вопросам науки – его секретарь за коррупцию был привлечён к уголовной ответственности).

1.2. ПЕРЕОПРЕДЕЛЕНИЕ ПОНЯТИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Сложившаяся система понятий, терминов и определений нуждается в приведении в соответствие с реалиями XXI века с учётом достижений математики, физики, кибернетики, вычислительной техники и космонавтики, а также развития средств связи.

Попытаемся в первую очередь дать рабочие определения терминов и понятий, релевантных рассматриваемой теме информационного противо-

65 Проф. Андрей Николаевич Колмогоров (урождённый Катаев, 1903-1987), Герой Социалистического Труда СССР, академик. Президент Московского математического общества. Иностранный член Национальной академии наук США, Лондонского королевского общества), член Германской академии естествоиспытателей «Леопольдина», Французской (Парижской) академии наук, почётный член Американской академии искусств и наук, иностранный член Венгерской академии наук, Польской академии наук, Нидерландской королевской академии наук; Академии наук ГДР, Академии наук Финляндии, почетный член Румынской академии; член Лондонского математического общества, Индийского математического общества, иностранный член Американского философского общества; почётный доктор Парижского университета (Сорбонны), Стокгольмского университета, Индийского статистического института в Калькутте. Кавалер Венгерского Ордена Знамени; Золотой медали им. Гельмгольца АН ГДР; Золотой медали Американского метеорологического общества. Лауреат Сталинской премии; премии им. Чебышева АН СССР; премии Бальцана; Ленинской премии; премии им. Лобачевского и премии Вольфа.


Источник: www.liveinternet.ru

Мухаммед аль Хорезми


Источник: www.securitylab.ru

Алан Тьюринг


Источник: info61.blogspot.com

Эмиль Леон Пост

борства/информационной войны, и связанных с этим проблем современной геополитики, новой стратегии ведения войны и новых видов оружия, входящих в реальность современной войны на геоцентрическом театре военных действий, базирующихся на информационных (как метод) и кибернетических (как средство) технологиях.

Будем понимать, что **информационное противоборство** – это состояние противостоящих субъектов геополитики, не связанное с тотальным применением силы для достижения победы в открытом вооружённом столкновении.

Информационное противостояние характеризуется накоплением и совершенствованием информационных и кибернетических технологий и соответствующим развитием методов и средств ведения информационной борьбы. Информационное противостояние следует рассматривать как гонку вооружений, направленную на достижение потенциального преимущества в вооружениях и методах ведения боевых действий на геоцентрическом ТВД.

Информационная война. Ранее мы уже приводили ряд частных определений понятия. Однако их множественность и, во многих случаях, противоречивость обусловлена тем, что до сих пор не сформулировано понимание того, что традиционная информационная война, современная информационная война и перспективная информационная война различаются по своим стратегическим целям, а, следовательно, по своим методам и средствам их ведения, по выбору и набору целей и по масштабам развёртывания.

Для начала остановимся на наиболее фундаментальных понятиях, составляющих основу информационных и связанных с ними технологий.

Теорема Котельникова (*в англоязычной литературе – теорема Найквиста – Шеннона или теорема отсчётов*) гласит, что, если аналоговый сигнал ***X (t)*** имеет финитный (ограниченный по ширине) спектр, то он может быть восстановлен однозначно и без потерь по своим дискретным отсчётам, взятым с частотой, строго большей удвоенной верхней частоты ***fc***:

Широкополосный роутер MC-419 MIMO

$$f>2\,fc$$

Такая трактовка рассматривает идеальный случай, когда сигнал начался бесконечно давно и никогда не закончится, а также не имеет точек разрыва во временно́й характеристике. Именно это подразумевает понятие «спектр, ограниченный частотой ***fc***».

Разумеется, реальные сигналы (например, звук на цифровом носителе) не обладают такими свойствами, так как они конечны по времени и, обычно, имеют разрывы во временной характеристике. Соответственно, их спектр бесконечен. В таком случае полное восстановление сигнала невозможно и из теоремы Котельникова вытекают два следствия:

- Любой аналоговый сигнал может быть восстановлен с какой угодно точностью по своим дискретным отсчётам, взятым с частотой ***f>2fc***, где ***fc*** – максимальная частота, которой ограничен спектр реального сигнала.
- Если максимальная частота в сигнале превышает половину частоты дискретизации, то способа восстановить сигнал из дискретного в аналоговый без искажений не существует.

Говоря шире, теорема Котельникова утверждает, что непрерывный сигнал ***x (t)*** можно представить в виде интерполяционного ряда

Широкополосная адаптивная антенная решётка.

$$x(t)=\sum_{k=-\infty}^{\infty} x(k\Delta)\,\mathrm{sinc}\left[\frac{\pi}{\Delta}(t-k\Delta)\right]$$

где ***sinc (x) = sin (x)/x*** – функция sinc. Интервал дискретизации удовлетворяет ограничениям ***0<Δ≤1/(2 fc).*** Мгновенные значения данного ряда есть дискретные отсчёты сигнала ***x (kΔ)***.

Хотя в западной литературе теорема часто называется теоремой Найквиста со ссылкой на работу 1928 года[66], в этой работе речь идёт лишь о требуемой полосе линии связи для передачи импульсного сигнала (частота следования должна быть меньше удвоенной полосы). Таким образом, в контексте теоремы отсчётов справедливо говорить лишь о частоте Найквиста. Примерно в это же время Карл Купфмюллер получил тот же результат[67]. О возможности полной реконструкции исходного сигнала по дискретным отсчётам в этих работах речь не идёт.

Теорема была предложена и доказана В. А. Котельниковым в 1933 году в работе[68], в которой, в частности, была сформулирована одна из теорем следующим образом[69]:«Любую функцию ***f (t)***, состоящую из частот от 0 до ***fc***, можно непрерывно передавать с любой точностью при помощи чисел, следующих друг за другом через ***1/(2 fc)*** секунд».

Независимо от Котельникова эту теорему в 1949 году доказал Клод Шеннон[70], поэтому в западной литературе эту теорему часто называют теоремой Шеннона.

В 1999 году Международный научный фонд Эдуарда Рейна (Германия) признал приоритет В. А. Котельникова, наградив его премией в номинации «за фундаментальные исследования» за впервые математически точно сформулированную и доказанную в аспекте коммуникационных технологий теорему отсчётов Исторические изыскания показывают, однако, что теорема отсчётов, как в части утверждения возможности реконструкции аналогового сигнала по дискретным отсчётам, так и в части способа реконструкции, рассматривалась в математическом плане многими учеными и ранее. В частности, её первая часть была сформулирована ещё в 1897 году Борелем.

---

66 Nyquist H. – Certain topics in telegraph transmission theory. Trans. AIEE, vol. 47, pp. 617-644, 1928

67 Küpfmüller K. – Über die Dynamik der selbsttätigen Verstärkungsregler. Elektrische Nachrichtentechnik, vol. 5, no. 11, pp. 459-467, 1928. (German); K. Küpfmüller, On the dynamics of automatic gain controllers, Elektrische Nachrichtentechnik, vol. 5, no. 11, pp. 459-467. (English translation)

68 Котельников В. А. – О пропускной способности «эфира» и проволоки в электросвязи. Успехи физических наук, 2006, № 7, с. с. 762-770

69 Спектры и анализ/А. А. Харкевич. 4-е изд. Москва, СССР. ЛКИ, 2007, с. 89

70 Shannon C. E. – Communication in the presence of noise. Proc. Institute of Radio Engineers. Vol. 37,. № 1, p. p. 10-21, Jan. 1949

Источник: www.edenhell.net

Гарри Теодор Найквист, (1889-1976)

Карл Купфмюллер, (1897-1977)

Впоследствии было предложено большое число различных способов аппроксимации сигналов с ограниченным спектром, обобщающих теорему отсчётов[71].

Так, вместо кардинального ряда по функциям **sinc**, являющимся характеристическими функциями прямоугольных импульсов, можно использовать ряды по конечно- или бесконечнократным свёрткам функций **sinc**. Например, справедливо следующее обобщение ряда Котельникова непрерывной функции ***x (t)*** с финитным спектром **(supp x= [-f_c, f_c])** на основе преобразований Фурье атомарных функций[72] и [73]:

$$x(t)=\sum_{k=-\infty}^{\infty} x(k\Delta)\prod_{n=1}^{M}\operatorname{sinc}\left[\frac{\pi}{a^{n-1}\Delta}(t-k\Delta)\right],$$

где параметры ***a, M*** удовлетворяют неравенству ***aM-1 (a-2) +1>0***, а интервал дискретизации

$$0<\Delta\le\frac{1}{2\int_c}1+\frac{a^{M-1}+1}{a^{M-1}(a-1)},$$

Необходимо отметить, что некоторые следствия теоремы Котельникова легли в основу разработки материалов технологии СТЕЛТС[74].

---

71 Meijering Erik – A Chronology of Interpolation From Ancient Astronomy to Modern Signal and Image Processing. Proc. IEEE, 90, 2002. DOI: 10.1109/5.993400; [Джерри А.Дж. – Теорема отсчётов Шеннона, её различные обобщения и приложения. Обзор. ТИИЭР, т. 65, №11, 1977, с. с. 53-89

72 Хургин Я.И., Яковлев В.П. – Прогресс в Советском Союзе в области теории финитных функций и её применений в физике и технике. ТИИЭР, 1977, т. 65, №7, с. с. 16-45

73 Басараб М.А., Зелкин Е.Г., Кравченко В.Ф., Яковлев В.П. – Цифровая обработка сигналов на основе теоремы Уиттекера-Котельникова-Шеннона. Радиотехника. М., 2004

74 Спектор В.Н. и другие – Авторское свидетельство СССР №295665 от 01.06.89 с приоритетом от 01.08.88; Спектор В.Н. и другие – Авторское свидетельство СССР №301885, зарегистрировано 2 октября 1989 г. с приоритетом от 29 июля 1988 г. по заявке №3205820; Бибиков С.Б., Горшенев В.Н., Спектор В.Н. – Радиопоглощающие материалы и покрытия. Деп. ВИНИТИ 11.07.96 №2329-В96, 32 с.; Овчинников А.А., Спектор В.Н., Божеико К.В. – Кластерный механизм возникновения отрицательного обменного взаимодействия в продуктах неполного сгорания углеводородов. Известия Академии наук (Россия). Сер.: физическая. 1997, т. 61, №5, с. 867; Bibickov S.B., Ghorshenyov V.N., Spector V.N. – Simulation, synthesis and investigation of microwave absorbing composite materials. Synth. Metals, 1997, vol. 86, p. 2255

С точки зрения информационной безопасности это материалы, позволяющие физическим объектам максимально затруднить получение информации об их присутствии в реальном пространстве и свойствах (подавление отражения или искажённое, ложное отражение).

Выстроенная система понятий, терминов и определений, используемых в военной учебной и научной литературе и применяемых в уставах, нормативных материалах, инструкциях, приказах и в других документах органов управления Вооружёнными силами, крайне важна для обеспечения единообразия понимания сущности таких документов всеми участниками процесса строительства и функционирования вооружённых сил, как в мирное, так и в военное время.

Первой «ласточкой» на эту тему в открытой печати в 1992 году стала брошюра группы высших и старших офицеров[75] под редакцией бывшего заместителя начальника Службы начальника вооружений Министерства обороны СССР, доктора технических наук, генерал-лейтенанта, проф. О. К. Рогозина[76], [77].

Среди авторского коллектива профессор **Цымбал Виталий Иванович,** полковник запаса, доктор технических наук, вице-президент Российской Академии проблем военной экономики и финансов, академик Академии военных наук РФ. Основная научная деятельность: военная безопасность, военная экономика, перспективы развития вооружений и управление их развитием.

Еще одним соавтором являлся профессор **Тихомиров Юрий Павлович,** полковник запаса, доктор технических наук, профессор Военно-воздушной академии им. Н. Е. Жуковского.

Выход этой брошюры, отражавшей состояние военной науки в формате современных форм и методов вооружённой борьбы и сохранившей идеоло-

---

*75 *Проф. Данилевич Андриан Александрович (1921-2003), Почётный член Российской академии естественных наук, генерал-полковник, заместитель президента Ассоциации военных историков, ведущий научный сотрудник редакции «Великая Отечественная война 1941-1945 гг.» Института военной истории МО РФ, кандидат военных наук, академик РАЕН, профессор Академии военных наук РФ. Основная научная деятельность: стратегия, оперативное искусство, строительство ВС, управление ВС, военная политика, военная безопасность. Другие основные труды: Рогозин О. К., Данилевич А. А., Цымбал В. И., Рогозин Д. О., Терехов И. И , Рафаилов А. Г., Терехов Г. И., Шунин О. П. – Международная безопасность и обороноспособность государств. НПО «Конверс АВИА». М., 1998, 487 с.*

Дайнес В. О., Данилевич А. А., Пронько В. А. и др. – История военной стратегии России/Под редакцией В. А. Золотарева; Институт военной истории Министерства обороны РФ. М., 2000.

Данилевич А. А., Рогозин Д. О., Рогозин О. К, Савельев А. Н., Слуцкий Л. Э., Терехов И. И., Цымбал В. И. – Война и мир в терминах и определениях/Под общей редакцией Д. О. Рогозина. Издательский дом «ПоРог». М., 2004, 624 с.

76 Данилевич А. А., Рогозин О. К., Тихомиров Ю. П., Цымбал В. И. – Понятия, определения и термины по проблеме «Оборонная достаточность». РАН, НПО «Элорма», Российско-американский университет, Международный фонд конверсии. Изд. «Элорма». М., 1992, 86 с.

77 Проф. Рогозин Олег Константинович (1929-2010), генерал-лейтенант, доктор технических наук, вице-президент Академии проблем безопасности, обороны и правопорядка (Россия). Основная научная деятельность: теория вооружения, проблемы развития вооружений, военная безопасность.

Источник: www.iep.ru

Виталий Иванович Цымбал

гические установки и концепции Советской армии, вызвал большой интерес в военных кругах.

Работа получила положительные отзывы со стороны известных военных специалистов. Например, доктор технических наук, генерал-лейтенант С. Я. Карпов писал: «Значимость предлагаемого сборника как труда энциклопедического типа в современных условиях возрастает, так как адекватное понимание терминов и определений, установление единых категорий и понятий будет способствовать более эффективному решению военно-политических проблем и выработке приемлемых процедур согласования назревших вопросов современности».

Более сдержано высказался бывший начальник 4 отдела Госплана СССР, кандидат технических наук, генерал-майор Р. Ф. Степанов: «…нельзя не отметить определённый успех … авторов, сумевших в достаточно концентрированном виде показать результаты глубоких исследований в области научного анализа военных проблем современности, подтверждающих плодотворность самой идеи такого сборника».

Заметим, что в обоих отзывах упор делается на современность, хотя сама эта современность в перспективе страны радикально изменилась (1991) уже к моменту выхода брошюры. Более того, все формулировки привязаны к традиционным и современным вооружениям, к традиционным и современным методам и средствам ведения вооружённой борьбы, и эта установка авторов сохранилась и в более поздних расширенных публикациях авторов и возглавлявшихся ими коллективах.

При этом необходимо отметить, что сразу вслед за выходом этой брошюры, презентация которой прошла в ходе научно-практического семинара по теме «Военная доктрина и концепция военного строительства в России: опыт, теория и практика», состоявшегося 3 апреля 1997 года в Президент-отеле Москвы под руководством Юрия Батурина (Секретарь Совета Обороны при Президенте РФ) и президента Академии военных наук Махмута Гареева, в газете «Дуэль» появилась статья[78], в которой работа подвергается весьма жёсткой принципиальной критике. Оставим в покое идеологические разногласия авторов брошюры и автора статьи.

Приведём лишь конкретную критику по существу.

«… знакомство с этим – сразу заявлю – всего лишь наукообразным, творением оказалось небесполезным. Правда, в том отношении, что лишний раз

78 *Брезкун С. Т. (Арзамас-16) – Подлость генеральских звёзд. Газета «Дуэль» № 12 (34), 17 июня 1997 года*

пришлось убедиться, насколько язвы предательства разъели даже такую исконно патриотическую среду, как военная.

В набитом «определениями» труде есть, например, понятия «воздушно-космическое направление» и «воздушно-космическое нападение». Есть даже определения «боевой танк», «огнестрельное оружие» и т. п. Зато нет такого «несущественного», как «вероятный противник».

…Вначале, как известно, было Слово. Так что терминологические проблемы имеют порой далеко не академический, а животрепещущий, злободневнейший политический смысл. …

Источник: vsr.mil.by

Махмут Ахметович Гареев

Источник: potsreotizm.livejournal.com

Сергей Тарасович Брезкун

Не то, что классового, – даже просто антиимпериалистического оттенка избегают бывшие офицеры Советской Армии. В классификации войн перечислены самые мудрёные их типы, а вот места для «национально-освободительной» не нашлось! Зато вводится понятие «ограниченной ядерной войны» – в чём сразу чувствуется школа американских наставников.

Нет и понятия «психологическая война». И тоже понятно почему – в доме повешенного о верёвке не говорят.

…Только не мешает добавить в определение целей ещё и установление идеологического контроля, одной из иллюстраций которого оказывается деятельность РАУ-корпорации и её продажных активистов»[79].

Таким образом, можно утверждать, что главная ценность этих работ состоит в создании внутренне непротиворечивой системы понятий о традиционных и современных ТВД и соответствующих вооружениях, то есть появляется земля под ногами для дальнейших шагов в осознании того, что и традиционные, и современные ТВД, и соответствующие вооружения – это уже область истории, что они уже сейчас становятся частью более общего и более сложного целого, играющими, хотя и важную, но отнюдь не определяющую роль на геоцентрическом ТВД, что, к сожалению, не нашло никакого отражения в сборнике[80]. При этом необходимо учитывать мудрое утверждение о том, что история никого ничему не учит, но она не прощает и жестоко нака-

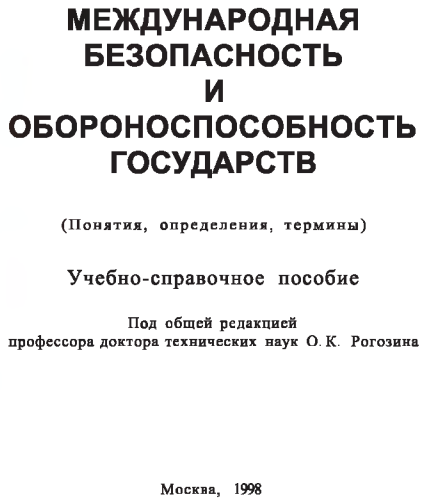
79 *Брезкун С. Т. (Арзамас-16) – Подлость генеральских звёзд. Газета «Дуэль» № 12 (34), 17 июня 1997 года,*

80 *Данилевич А. А. … – Понятия, определения и термины…*

зывает тех, кто забывает её уроки. Есть опасения, что авторы этого сборника забыли уроки жизни и распада великой Державы, которой они служили.

Особенностью сборника[81] и производных, расширенных публикаций с участием Д.О. Рогозина является то, что в их основе лежит концепция оборонной достаточности, разработанная генералом О.К. Рогозиным. Эта концепция в первоначальном виде, доложенном лично О.К. Рогозиным на Политбюро ЦК КПСС, безусловно, имела право на существование в условиях, сложившихся в СССР после 1985 года. Изначально концепция состояла в сокращении численности терявшей боеготовность и боеспособность советской армии, ставшей, кроме того, непосильным бременем для экономики страны, и в переходе к чисто оборонительной доктрине, работоспособность которой должна была подтверждаться наращиванием ядерного потенциала сдерживания и его эффективности.

Доклад не был одобрен ни Политбюро ЦК КПСС, ни руководством МО СССР, ни советским генералитетом, правда, по разным причинам. Горбачёвское политбюро, готовое стать крайкомом «мирового правительства», представляемого США, по Советскому Союзу, опасалось, что «старшие коллеги» не одобрят реальной угрозы ядерного возмездия.



81 *Данилевич А.А. ... – Понятия, определения и термины ...*

Руководство МО СССР, в целом не имело намерений смены мундиров, к тому же с понижением, если не зарплаты, то реального влияния. В оборонном ведомстве Советского Союза опасались любых реформ и перемен в ставшей весьма хрупкой структуре вооружённых сил страны (эти опасения были успешно унаследованы и МО РФ относительно любых реальных реформ вооружённых сил). Генералитету, понятно, кроме привычки к своему мундиру, не понравилось и предусматриваемое концепцией оборонной достаточности сокращение численности вооружённых сил, ergo сокращение числа генеральских должностей.

Ремир Фёдорович Степанов

Источник: elite-astronomy.narod.ru

Юрий Михайлович Батурин

Единственной влиятельной персоной, возлюбившей эту концепцию, оказалась д-р Маргарет Тэтчер[82], отправлявшая тогда должность премьер-министра Великобритании. Её опубликованная в британской открытой печати оборонная доктрина в значительной мере опиралась на дословный перевод концепции оборонной достаточности генерала О. Рогозина, пожалуй, единственного советского генерала удостоившегося чести украшать обложку журнала «Таймс». Не удивительно, что госпоже Тэтчер понравилась эта концепция – с появлением и развитием ракетно-ядерных вооружений, с родоначальниками которых (ФАУ-2) Великобритания «познакомилась» в конце Второй мировой войны, уязвимость сравнительно небольшого острова резко возросла, и стратегия «скорпиона» – угрозы ядерного возмездия «из могилы», кстати, тоже изобретённого в СССР, рассматривалась ею в качестве компенсации возросшей уязвимости страны.

Если восприятие Тэтчер рогозинской концепции не вызывает особого удивления, то сам факт получения ею копии доклада генерала Рогозина на Политбюро ЦК КПСС (материал «Особой папки») воистину удивителен. По утверждению О.К. Рогозина существовало всего два экземпляра этого доклада – один хранился в служебном сейфе генерала, по которому по просьбе Рогозина и производилось сопоставление с английским текстом, а второй – в Политбюро. Единственным реалистичным предположением о природе этого трансферта

---

82 ***Ма́ргарет Хи́льда Тэ́тчер,*** *баронесса Тэтчер урождённая Робертс; 13 октября 1925 (англ. Margaret Hilda Thatcher, Baroness Thatcher; премьер-министр Великобритании (Консервативная партия Великобритании). ru.wikipedia.org›wiki/Тэтчер, _Маргарет*

Источник: vpersone.ru

Алекса́ндр Никола́евич Я́ковлев

может служить прямая передача этого материала Тэтчер самим Горбачёвым или его коллегой по формированию упоминавшегося «крайкома мирового правительства» А. Н. Яковлевым[83].

На самом деле, то, что может быть хорошо для Великобритании, не обязательно было хорошо для СССР и приемлемо для Российской Федерации. Британия является ближайшим союзником США, входит в военно-политический блок НАТО, который не только не был распущен после роспуска ОВД, но и начал активное продвижении на восток, поближе, а местами и вплотную к границам Российской Федерации. России не на кого надеяться, кроме как на саму себя, на свои вооружённые силы, и с этой точки зрения многие определения из упомянутой брошюры, раскрывающие понимание авторами концепции оборонной достаточности представляются сомнительными.

Так, в основной статье 5.1 – Оборонная достаточность раздела 5 «Стратегическое противостояние государств и «оборонная достаточность» после неконкретной общей части следует перечисление «важнейших объективных признаков и критериев, выражающих оборонную достаточность государства». Рассмотрим их содержательную и смысловую часть:

«Миролюбивая внешняя политика, признающая роль военной силы лишь как средство для отражения любой агрессии». Признак невнятный по содержанию: не определено, что значит «любая» агрессия и против кого эта любая агрессия направлена. Смысл просто ошибочный – в случае агрессии против России роль военной силы не может рассматриваться лишь как средство её отражения (отразили, они перевели дух, перегруппировались и опять учинили агрессию); в случае агрессии роль военной силы состоит в нанесении поражения агрессору с целью обеспечения национальной безопасности от военных посягательств.

«Открытый оборонительный характер военной политики, военной доктрины, стратегических концепций вооружённых сил, не провоцирующих противостоящие государства к наращиванию вооружений». Стратегические концепции вооружённых сил по определению не могут иметь исключительно оборонительный характер, так как они предназначены для защиты геополитических интересов страны. Всё остальное – общие слова, декларации, не имеющие практического смысла. Однако в целом этот с позволения ска-

---

*83 **Алекса́ндр Никола́евич Я́ковлев** 2 декабря 1923-18 октября 2005 академик РАН, идеолог и «архитектор» перестройки член Политбюро ЦК КПСС, председатель РПСД.*

зать принцип закладывает основу пораженческой направленности и отказа вооружённых сил страны от защиты её геополитических интересов.

Этот принцип усугубляется в определении 5.11 – Меры по предупреждению войны: «…В стратегическом плане не допускать действий, которые могли бы быть квалифицированы в качестве военной угрозы, максимально ограничить военную деятельность у внешних границ, в прибрежных водах и в воздухе. <…> Не ставить военных задач, угрожающих безопасности других стран, и не проводить мероприятий по подготовке к их выполнению». Это уже не определение, а готовая инструкция по подготовке к капитуляции.


Источник: etymet.com

Ма́ргарет Хи́льда Тэ́тчер

«Излишне необременительный для экономики численный состав и оборонительная структура вооружённых сил, а также преимущественное развитие оборонительных видов вооружений, что в совокупности должно исключать возможность использования вооружённых сил для проведения широкомасштабных наступательных боевых действий».

Этот критерий является точной формулировкой стратегии поражения. Здесь всё очевидно – развитие преимущественно оборонительных видов вооружений обрекает армию на поражение даже без возможности нанесения эффективного ответного удара, поскольку этим же критерием исключается возможность проведения ответных широкомасштабных наступательных действий. Этот же тезис подтверждается в определении 5.20 – Применение вооружённых сил.

Остальные два положения, относящиеся к соблюдению ядерных квот и к участию в международных системах контроля состояния стратегической обстановки не имеют отношения ни к принципам, ни к критериям оборонной достаточности.

Рассмотрим ещё несколько релевантных определений из упомянутой брошюры.

Определение 3.11.1. **Стратегическая оборонная инициатива (СОИ)** США – программа НИОКР, основной целью которой является создание научно-технического «задела» для разработки широкомасштабной ПРО с элементами космического базирования и её поэтапного развёртывания.

Хотя это определение и не относится напрямую к осознанию собственно российских проблем модернизации структуры вооружённых сил и осовременивания их парадигмальной базы, оно уводит военное и политическое руководство страны от концентрации на решение задач приведения всей

военной, промышленной и социальной структуры страны в соответствие с весьма вероятными вооружёнными конфликтами близкого будущего.

СОИ, безусловно, включает и систему научно-исследовательских (в том числе фундаментальных), и опытно-конструкторских работ, которые, будучи необходимой и неотрывной частью практических мероприятий по переходу к перспективным методам и формам вооружённой борьбы, выставляются на всеобщее обозрение национальной и международной общественности и играют роль ширмы, за которой уже внедряются принципиально новые формы и методы вооружённой борьбы и осуществляется кибер-космическая интеграция всей структуры вооружённых сил.

Опытными образцами этих мероприятий являются дистанционные трёхмерные войны, например, в Ираке, СРЮ и Ливии. Примечательно, что самым первым экспериментом по тестированию многих элементов трёхмерных операций за счёт интегрирования морских и наземных операций британских вооружённых сил со средствами космической разведки и наведения США стал Мальвинский конфликт.

В быстротекущей войне между сражавшейся за восстановление своего суверенитета над Мальвинскими (Фолклендскими – английское название) островами Аргентиной и неформализованным англо-американским неоколониальным альянсом с «посильным» участием Франции, и при молчаливом нейтралитете мирового сообщества, у Аргентины не было шансов на военную победу.

«Оружие – общее название устройств и средств для уничтожения живой силы противника, его техники и сооружений. Подразделяется на оружие массового поражения и обычное; на огнестрельное, ракетное, минное, торпедное и холодное; на стационарное (на неподвижном и подвижном основании), самоходное, буксируемое, возимое и другое».

Это определение могло бы быть дано, за исключением ОМП, военными специалистами времён наполеоновских войн, а, может быть, и Крестовых походов. Как бы сказал Винер: «оружие – это оружие».

На самом деле, вместо весьма неопределённого термина «оружие», включающего, кроме приведенного в определении 3.19, и охотничье оружие, и личное оружие, и прочие средства убийства, это определение могло бы быть озаглавлено как Определение 3.19'. **«Оружие как средство вооружённой борьбы организованных сообществ** (государств {в том числе и непризнанных}, блоков государств, освободительных движений и тому подобных), предназначенное для достижения военной победы за счёт уничтожения/принуждения к капитуляции воинских контингентов противника, его военной инфраструктуры (промышленной, транспортной и иной), систем управления и связи, а также для достижения осознания населением государства-противника и его политическим руководством бессмысленности дальнейшего военного сопротивления.

Излишней представляется и бессистемная детализация видов оружия, при этом укрупнённое упоминание ОМП перед перечислением «пистолетов и ножичков» выглядит как арбуз на помидорной делянке. В связи с этим вторая часть Определения 3.19' могла бы быть записана в следующем виде:

Определение 3.19' (продолжение). Средства вооружённой борьбы подразделяются на традиционные вооружения (сухопутных войск – стрелково-пушечные вооружения, противовоздушные вооружения, ракетно-артиллерийские и танковые вооружения и другие; военно-морского флота – надводные и подводные комплексы и военно-воздушных сил – истребители, штурмовики, бомбардировщики, самолёты-разведчики и другие); современные вооружения (интегрированные через современные, включая космические системы связи, традиционные вооружения, прецизионные вооружения: артиллерия со снарядами с активной фазой полёта, в том числе с самонаводящимися боеприпасами, ракеты малой дальности (поля боя), ракеты средней и большей дальности; крылатые ракеты, запускаемые с корабельных и авиационных платформ, и межконтинентальные ракеты с традиционными боеголовками; оружие массового поражения – ядерное/термоядерное с современными средствами доставки, включая МИРВ, биологическое/бактериологическое и химическое, в том числе радиохимическое оружие, например, **U236** и **U232**) и опытные образцы новых перспективных типов вооружений, как правило, официально не декларируются как принятые на вооружение.

Источник: www.bufon.org

Памятник погибшим аргентинским воинам, *Буэнос-Айрес*

Это оружие новой геополитической данности – геоцентрического театра военных действий: информационное оружие; психотронное оружие; климатическое, включая экологическое, оружие; геотектоническое; пучковое; инфразвуковое; лазерное и ряд других вооружений на основе новых физических принципов.

Многие виды современного и перспективного оружия являются неконвенциональными, то есть запрещёнными международными соглашениями.

В связи с изложенным возникает необходимость корректировки определения ОМП и определений его видов, а также включения в понятийный обиход предваряющего определения геоцентрического ТВД и определений видов оружия геоцентрического ТВД: информационного оружия; психотронного оружия; климатического оружия, включая экологическое оружие; геотектонического; пучкового; инфразвукового и лазерного оружия, а также современного прецизионного оружия (оружия повышенной точности) и оружия с боеприпасами объёмного взрыва.» (см. рис 1 стр 74).

«Определение 3.19.1. (новое) – Оружие массового поражения (ОМП) – современное оружие, обладающее неизбирательными поражающими способностями на больших площадях с массовыми людскими (в первую очередь среди не комбатантов) потерями и поражением военных и гражданских объектов и инфраструктуры. К оружию массового поражения относят следующие типы вооружений:

ядерное/термоядерное/нейтронное оружие;

химическое/радиохимическое оружие, биологическое/бактериологическое/радиобиологическое оружие.

Источник: www.svoboda.org

Демонстрация аргентинских ветеранов военного конфликта 1982 года.

К ОМП следует отнести и оружие объёмного взрыва.

К перспективным видам ОМП геоцентрического ТВД относятся:

консциентальное (прошло предварительные научно исследовательские работы и лабораторные тесты);

информационное (прошло испытания в полном объёме, включая натурные);

психотронное, в том числе инфразвуковое оружие (прошло испытания в полном объёме, включая натурные);

кибернетическое оружие (в США, России, Великобритании, Германии, Китае и Индии принято на вооружение, ещё в 10-15 странах прошло испытания в полном объёме, включая натурные);

геотектоническое оружие (прошло испытания в полном объёме, включая натурные);

климатическое оружие, включая экологическое оружие на новых физических принципах (в США, России и Германии принято на вооружение, ещё в 3-5 странах прошло испытания в полном объёме, включая натурные);

пучковое, включая лазерное оружие (прошло испытания в полном объёме, включая натурные).

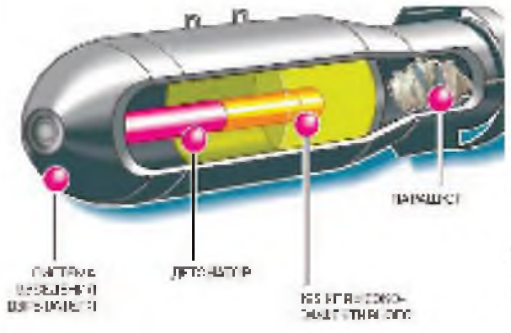
Попробуем дать необходимые определения отдельным блоком, включающим наше видение поправок в определения всех типов современного ОМП, а также определения перспективного оружия геоцентрического ТВД.

1.2.1 Геоцентрический театр военных действий (ГЦ ТВД)

1. Геоцентрический театр военных действий – стратегическое сферическое пространство вероятных военных действий, простирающееся от центра планеты[84] до геостационарных спутников Земли и включающее систему заряженных оболочек, начиная с верхних слоёв атмосферы, включая озонный слой, предохраняющий жизнь на поверхности планеты от губительного жёсткого излучения; до геостационарной орбиты (ионосфера; концентрические заряженные пояса Ван Аллена и слой Хэвисайда), и магнитосферу, индуцируемую вращением твёрдого ядра планеты, форма которой определяется взаимодействием магнитного поля Земли и излучением Солнца.

Геоцентрический театр военных действий, поглощая все современные домены операций вооружённых сил {наземные, флотские и аэрокосмиче-

84 В формулировке генерала Келера – автора термина и теоретика операций на геостационарном ТВД: от поверхности Земли до геостационарной орбиты (36000 км); наше уточнение связано с тем, что магнитосфера Земли определяется вращением ядра планеты, и действие тектонического оружия зависит как от взаимодействия магнитосферы с солнечным ветром, так и от вызываваемых действиями человека изменений в ионосфере и других заряженных поясах внешней оболочки Земли (Хэвисайда и Ван Аллена).



Источник: topwar.ru

Боеприпас объёмного взрыва.

ские (ближний космос)}, формирует принципиально новую стратегическую реальность, в которой как ближний, так и открытый космос становится не только местом размещения и действия вооружений на новых физических принципах, но и оружием. При этом переход к оружию геоцентрического ТВД несравнимо значимее, чем, скажем, переход от меча и лука к огнестрельному оружию и даже чем переход от традиционных вооружений к современным СМП.

Безусловно, следующим шагом в развитии форм и средств вооружённой борьбы станет расширение сферы использования космоса с переносом боевых действий на Луну, Марс и на точки гравитационного равновесия в системе Солнце – Земля – Луна (гелиоцентрический ТВД), если, конечно, человечество сумеет пережить конфликты на геоцентрическом ТВД. Новое оружие в будущем использует, например, лишь слегка затронутый в тектоническом оружии потенциал гравитации, а в качестве неисчерпаемого источника энергии – ещё непознанные свойства открытого космоса[85] – свойства «пустоты» как говорит Лесков.

---

85 Лесков Л. В. – Пять шагов за горизонт; Синергизм: философская парадигма XXI века. Изд. «Экономика». М., 2006, 637 с. [www.leskovlv.ru/list/listsinergizm. htm]

***Беспилотные вертолеты MQ-8 Fire Scout** с APKWS (Advanced Precision Kill Weapons System) – 70-миллиметровыми ракетами с лазерным наведением.*

Mirage 2000S (Strike) *– многоцелевой истребитель-бомбардировщик французской фирмы Dassault. Самолет предназначен для применения обычного высокоточного вооружения. Для наведения подвесного вооружения используется РЛС Thomson-CSF/ESD Antilope V. ЛА может нести до 6000 килограмм неядерных прецизионных вооружений с дальностью действия более 3000 км, подвешиваемых на 9 узлах подвески под крылом и под фюзеляжем.*

GBU-44/E Viper Strike *представляет собой планирующую бомбу, способную с высокой точностью поражать цели, используя GPS-навигацию и полуактивную лазерную систему наведения.*

1.2.2. Оружие геоцентрического ТВД

Оружие, обладающее разрушительными действиями планетарного масштаба, размещаемого, как на поверхности планеты, так в сферическом геоцентрическом пространстве, простирающемся на расстояние в 35-40 тысяч километров от поверхности Земли, причём ближний космос, включающий магнитосферу и заряженные слои внешних оболочек планеты, сам становится элементом этого оружия.

Специфическим видом оружия геоцентрического ТВД в обозримом будущем станет информационное оружие (Калита геоцентрического театра); консциентальное (смысловое) оружие; психотронное оружие, в том числе инфразвуковое оружие; кибернетическое оружие; климатическое оружие, включая экологическое оружие на новых физических принципах; тектоническое оружие и пучковое, включая лазерное оружие.

Кроме того, оружие геоцентрического ТВД интегрирует посредством информационного оружия в единую систему ведения боевых действий все системно адаптированные виды традиционного и современного оружия, в первую очередь ядерное/термоядерное оружие как средство накачки носителями заряда ионосферы и других заряженных слоёв внешних оболочек планеты.

1.2.3. Информационное оружие

Оружие массового поражения психологического действия, основанное на использовании средств массовой информации, в первую очередь электронных СМИ, и иных систем передачи данных для дезорганизации систем управления, деморализации вооружённых сил и населения противника, инициирования массовых беспорядков на этнической, религиозной и социальной почве. Кроме того, информационное оружие является основой и неотъемлемой частью всех видов оружия геоцентрического ТВД.

Атакующим информационным оружием называют (Д.С. Черешкин и др., 1996):

- компьютерные вирусы;
- логические бомбы (программные закладки);
- средства подавления информационного обмена в телекоммуникационных сетях,

фальсификация информации в каналах государственного и военного управления;

- средства нейтрализации тестовых программ;
- различного рода ошибки, сознательно вводимые в программное обеспечение объекта.

К сожалению, в сборнике[86], вышедшему позже работ Д. С. Черешина, определение информационного оружия 3.25 дано в виде: «перспективные комплексы специфических программно-информационных средств, создаваемых для поражения информационного ресурса противника.


Источник: centr.kravchenko.ru

Леонид Васильевич Лесков

«Логическая бомба» – программа, заложенная в ЭВМ, которая по определённому сигналу или в установленное время приходит в действие, искажая или уничтожая информацию.

««Компьютерные вирусы» – или вводимые дефекты в программное обеспечение ЭВМ противника, способные нарушить компьютерную сеть и вывести из строя оружие, управляемое с помощью ЭВМ». Это определение явно недостаточно даже при описании современного информационного оружия.

Последствия воздействия информационного оружия устранимы в тех случаях, пока психологические эффекты не перешли грань психиатрических синдромов. Здесь проф. Черешкин допускает методологическую ошибку, так как информационное оружие не оказывает прямого действия на психику человека, но является определяющим несущим элементом психотронного оружия, оказывающего деструктивное или деформирующее воздействие на психику человека.

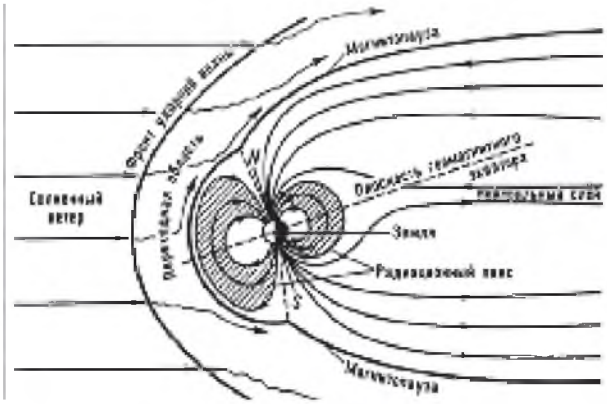
Кроме того, информационное оружие геоцентрического ТВД является средством скоростной и кодированной передачи данных в структуре управления боевыми действиями всех видов оружия и по всему объёму трёхмерного ТВД.

Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в обеспечении национальной военной стратегии воздействием на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем»[87].

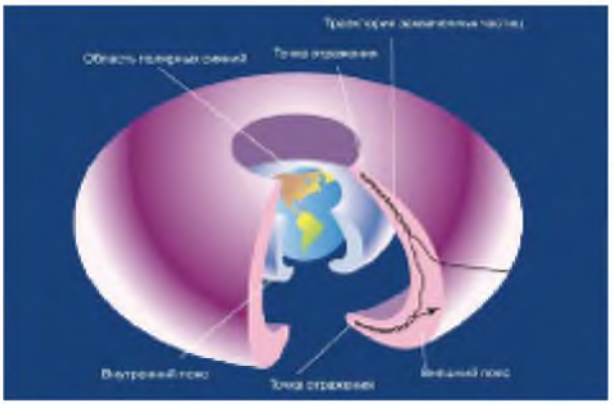
Угрозами информационных войн можно считать желание неких конкретных сил использовать в киберпространстве гигантские возможности компьютерной техники и компьютерных технологий для ведения бесконтактной войны. Отличительной особенностью таковых действий является минимальное количество жертв, которые будут следствием непосредственного воздействия информационного оружия. «Мы приближаемся к такой

86 *Данилевич А. А. ... – Понятия, определения и термины ...*

87 *Завадский И. И. – Информационная война – что это такое? Защита информации. «Конфидент», №4, 1996*



Схематическое представление строения магнитосферы



Источник: earth-chronicles.ru

Заряженные пояса Ван Аллена.

ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий, – сказал один из руководителей Пентагона. – Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума». Эта полу-идиллическая пентагоновская сентенция из арсенала «чёрной магии» не имеет ничего общего с мрачной реальностью: информационная война – дело кровавое. В ходе информационной войны, помимо подрыва взглядов, разрушается инфраструктура управления большинством систем жизнеобеспечения социума, а это уже ведёт к массовой гибели гражданского населения.

«Атаки типа «отказ в обслуживании» (DoS-атаки) породили стандартные заголовки со словом «кибервойна», но в действительности, с технической точки зрения, эти «атаки» могут быть противоположностью настоящей «кибервойны». Между тем, статья в ведущем израильском еженедельнике Ha'aretz об операциях Израиля против ядерной программы Ирана, прошедшая относительно незамеченной, может дать больше представления о том, что такое кибервойна на самом деле.

Не секрет, что некоторые страны, включая Соединённые Штаты, Китай, Россию и Израиль, ведут изучение возможностей кибервойны. Какими могут быть эти возможности, и как могла бы выглядеть кибервойна – всё это покрыто завесой секретности. DoS-атаки из газетных заголовков – это не она.

Эти атаки – не более чем отправка громадного количества запросов на серверы, в результате чего сайты не способны отвечать на легитимный трафик, и нарушается работа электронной почты. Компетентные профессионалы в сфере информационных технологий обычно могут сгладить послед-

ствия этих атак, и, даже если они успешны, то, с точки зрения национальной безопасности, их воздействие является маргинальным»[88].

«DoS-атаки совершаются при помощи бот-сетей, тысяч взломанных компьютеров, которым можно дать команду одновременно послать сообщения по электронной почте или зайти на тот или иной сайт. Бот-сети строятся при помощи вредоносных программ, которые атакуют отдельные компьютеры, – зачастую просто пользуясь тем, что установленное на них программное обеспечение не имеет актуальных обновлений систем безопасности. Компьютеры, подключенные к государственным ведомствам, взламывались и становились частями бот-сетей, но это не обязательно влечёт за собой чудовищные последствия в сфере безопасности. Реальная кибервойна может потребовать навыков, противоположных тем, что нужны для осуществления DoS-атак, о которых пишут в газетах.

По данным статьи в Ha'aretz, израильская разведка систематически работает над внедрением вредоносного программного обеспечения, которое может нарушить работу информационных систем иранской ядерной программы. Считается, что эти системы не подсоединены к Интернету, а вредоносное программное обеспечение установлено на оборудование, которое продается иранскому правительству.

Вот так может выглядеть кибервойна будущего. Современные общества представляют собой сложные сети, состоящие из людей, информационных систем и машин. Те державы, которые могут быстро идентифицировать и нейтрализовать критические узлы и узлы уязвимости в системах, получат громадные преимущества.

Критически важные правительственные системы используют интранет-сети, отделённые от Интернета. Считается, что самые важные системы – такие, как системы управления ядерным оружием – не подсоединены к другим системам. Однако в большинстве внутренних сетей государственных ведомств есть точки соприкосновения с Интернетом, и эти сети заражаются вредоносным программным обеспечением из Интернета. Но всё же, любой интранет – относительно контролируемая среда, поэтому аномальная активность (по крайней мере, теоретически) может быть быстро взята под контроль и изолирована.

Поскольку взлом этих сетей может сыграть решающую роль в военном конфликте, государства, обладающие серьёзными амбициями в сфере кибервойны, будут тщательно адаптировать вредоносное программное обеспечение для конкретных систем. Это полная противоположность вредоносному

---

88 Мэннис Аарон (исследователь из Университета Мэриленда),. Хендлер Джеймс (профессор компьютерных наук из Ренселейрского политехнического института) – Портрет настоящей кибервойны: Опасайтесь вредоносных программ http://www.inosmi.ru/world/20090806/251360.html 06/08/2009

программному обеспечению, которое строит бот-сети, проникая туда, где это не требует особых усилий.

Самые серьёзные случаи хищения персональных данных обычно включают в себя психологические атаки – мошенники стараются перехитрить жертву, чтобы получить важную информацию, упрощающую совершение преступления. То же самое может иметь место при подготовке атак на критически важные сети. В большинстве развитых государств существует широкая инфраструктура подрядчиков и учёных, которые выполняют свою гражданскую работу и контактируют с силовыми ведомствами. Анализ социальных сетей может быть использован для выявления лиц, которые, вероятно, имеют контакты с силовыми ведомствами, и для последующего внедрения вредоносного программного обеспечения через их компьютеры.

Представьте себе привычные сегодня фишинговые атаки – рассылаемые по электронной почте сообщения якобы из банков и компаний по выдаче кредитных карт, – устроенные разведывательными службами и нацеленные на узкие сообщества.

Вопрос о том, что может сделать вредоносное программное обеспечение, попав в систему, остаётся открытым. Сообщается, что китайские хакеры проникают в компьютеры и манипулируют ими для удаления секретных документов, регистрации нажатий клавиш на клавиатуре, включения веб-камер. Доподлинно неизвестно, могут ли действовать эти функции в течение продолжительного времени в безопасном интранете. Срок жизни любого вредоносного программного обеспечения, внедрённого в стратегически важные сети, может быть очень коротким, и его разработчикам нужно тщательно продумать, как добиться за это время максимальных результатов. Как вариант, это программное обеспечение может внедряться надолго и активироваться в случае необходимости. Возможны и сценарии передачи ценной информации, манипулирования информацией, повреждения сети или предоставления информации о размещении ключевых сетевых узлов с тем, чтобы их можно было физически уничтожить.

Однако пользоваться возможностями кибервойны непросто. Как только вредоносное программное обеспечение обнаружено, защитники могут ему противодействовать, усиливая систему и повышая её устойчивость перед несанкционированным доступом в будущем.

В разгар сражения возможность взломать информационную сеть противника может сыграть решающую роль. Однако в долгосрочной диалектике войны, при которой стороны постоянно отвечают на инновации друг друга, кибервойна станет ещё одной гранью конфликта – временами важ-

нейшей, временами периферийной. Те страны, которые первыми овладеют искусством кибервойны, смогут получить фундаментальное преимущество на начальных стадиях конфликта. Те страны, которые игнорируют кибервойну, делают это на свой страх и риск»[89].

Круг тех, кто может развязать гражданскую информационную войну, значителен – начиная от террористов, наркотических картелей до подпольных торговцев оружием массового поражения. Но все же в главную роль в ее развязывании будут играть западные спецслужбы, которые де-факто управляются «мировым правительством». А криминальная природа последнего определяется тем, что на самом деле именно оно организует и управляет структурами государственного и международного терроризма, экстремизма, и организованной преступности: международным банковским картелем (им из международного денежного оборота и налогообложения выведено более трех десятков триллионов долларов, что стало решающим инструментом войны со странами зоны евро), наркокартелями, торговлей людьми и человеческими органами, «чёрным рынком» торговли оружием, в том числе средствами массового поражения.

Информационная война нуждается в постоянной череде конфликтных поводов в виде нарушающих закон акций или возмущающих общественную мораль перформансов, в отношении которых можно разогнать медийную волну. Понятно, что перформансы типа непристойных плясок на амвоне православной церкви с последующим изготовлением видео-клипа с наложенным текстом или акция типа публичного группового секса в музее участницами группы с непристойным названием стоит денег, больших денег.

Ещё больших денег стоит организация неразрешённых митингов и демонстраций с призывами к свержению законно избранной власти (даже самые заядлые оппозиционеры не отрицают, что большинство народа проголосовало за Путина и поддержанную им партию), с провоцируемыми столкновениями с правоохранительными органами, с постоянным неподчинением законным требованиям полиции.

Госдума решила создать «список Таргамадзе». В него должны быть включены иностранцы, в том числе из стран постсоветского пространства, которые ведут подрывную деятельность на территории России, склоняя население великого государства к «оранжевой» революции[90].

Предполагалось, что документ с опальными фамилиями будет назван по имени Гиви Таргамадзе. Как утверждал сотрудники Следственного комитета РФ, грузинский политик Таргамадзе приложил руку к финансированию протестных акций в России, и, в частности, к субсидированию деятельности

89 *Мэннис ... – Портрет ... 2009*

90 *Об этом пишет в пятницу, 14 декабря 2012, газета «Известия».*

Источник: lenta.ru

Г. Таргамадзе

Сергея Удальцова, координатора «Левого фронта». «Мы обсудим расширение чёрного списка в связи с последними событиями и направим представление в МИД о включении тех, кто разрушает наше государство, в число невъездных граждан», – заявил представитель комитета Госдумы по международным делам Александр Бабаков.

«Единоросс Вячеслав Никонов, первый зампред комитета Госдумы по международным делам, пояснил, что список будет достаточно внушительным, а лицам, «подобным Г. Таргамадзе», будет навсегда закрыт въезд в Россию. «Я не считаю, что Таргамадзе и подобные ему лица, желающие антироссийских выступлений и восстаний, должны иметь право въезда на территорию нашей страны», – заявил он.

Его коллега по комитету, депутат фракции «Единая Россия» Шамсаил Саралиев заявил, что нельзя ограничиваться одними списками: «по отношению к тем, кто хочет развалить Россию, необходимо применять и более жёсткие меры». «У нас огромное количество врагов, Россию хотят развалить, расшатать и ослабить. Они дают деньги Удальцовым и прочим со словами «Вперёд, дерзайте. Мы спасём вашу страну и наведём порядок», – утверждает депутат.

Напомним, накануне СКР рассказал о «конкретной роли» Г. Таргамадзе в организации протестного движения в России. Следствие заявило, что располагает неопровержимыми уликами. «В этих материалах содержатся доказательства, подтверждающие не только финансирование российской оппозиции со стороны Гиви Таргамадзе, но и его конкретную роль в организации массовых беспорядков на Болотной площади, а также его непосредственное руководство действиями лидеров оппозиции при проведении «Марша миллионов» в Москве», – отметили в комитете.

О «выдающейся» роли Г. Таргамадзе и его беспрецедентном влиянии на российскую политику стало известно после выхода документального фильма «Анатомия протеста – 2» на телеканале НТВ. Журналисты рассказали о том, как координатор «Левого фронта» С. Удальцов и другие известные оппозиционеры встречались с зарубежными коллегами, готовя насильственный захват власти в России на иностранные средства и деньги беглых российских олигархов. Вскоре герои документальной картины стали фигурантами уголовного дела»[91].

---

91 1 газета «Известия». 14 декабря 2012

Один из авторов 6 мая 2012 года в связи с беспределом призывов и лозунгов демонстрантов у себя под окном собирался надеть казачью форму и занять место в рядах спецназа, но командиры сказали, что участие посторонних лиц не предусмотрено законом, и это может быть использовано оппозиционной и западной пропагандой.

Создаётся впечатление, что власти дают возможность этим медийным поводам развернуться в полномасштабную информационную войну.

История информационной войны.

Большой интерес представляет внимательное рассмотрение истории и возможностей информационной войны новым поколением российских военных исследователей[92]. Основные положения этой работы приводятся нами с минимальным редактированием.

«Сегодня много говорится об «информационной войне». Однако вряд ли кто сможет точно ответить, что это такое. Более того, даже специалисты не смогут ответить на вопрос о том, когда же всё-таки родилось само словосочетание «информационная война», когда впервые был поставлен вопрос о том, чтобы рассматривать информацию в качестве оружия?».

Далее, если выяснить эту информацию и дать ответы на поставленные вопросы, то, несомненно, сразу встанет целый ряд подобных вопросов, например, что есть информационная война? Какими средствами она ведется и, что ставится целью этой войны? Считать ли нападения хакеров военными действиями, если да, то какие средства ответа будут адекватными? Ниже мы попробуем дать ответы на эти и, возможно, другие вопросы по затронутой теме.

Первоначально военный аналитик, д-р Томас Рона (1923-1997) использовал термин «информационная война» в отчёте, подготовленном им в 1976 году для компании Boeing, и названным «Системы оружия и информационная война». Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью, как в военное, так и в мирное время. Этот отчёт и можно считать первым упоминанием термина «информационная война».

Публикация отчёта Т. Рона послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься «секретными материалами». Военно-воздушные силы США начали активно обсуждать этот предмет уже с 1980 года. К тому времени было достигнуто единое понимание того, что информация может быть как целью, так и оружием.

---

92 Гриняев С.Н. – Информационная война: история, день сегодняшний и перспектива

В связи с появлением новых задач после окончания «холодной войны» термин «информационная война» был введен в документы Министерства обороны США. Он стал активно упоминаться в прессе после проведения операции «Буря в пустыне» в 1991 году, где новые информационные технологии впервые были использованы как средство ведения боевых действий на трёхмерном ТВД. Официально этот термин впервые введён в директиве министра обороны США DODD 3600 от 21 декабря 1992 года.

Спустя несколько лет, в феврале 1996 года, Министерство обороны США ввело в действие «Доктрину борьбы с системами контроля и управления». Эта публикация излагала принципы борьбы с системами контроля и управления как применение информационной войны в военных действиях. Публикация определяет борьбу с системами контроля и управления как: «объединенное использование приёмов и методов безопасности, военного обмана, психологических операций, радиоэлектронной борьбы и физического разрушения объектов системы управления, поддержанных разведкой, для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению на поле боя, при одновременной защите своих сил и сил союзников, а также препятствование противнику делать тоже самое». В этом документе была определена организационная структура, порядок планирования, обучения и управления ходом операции. Наиболее важным является то, что эта публикация определила понятие и доктрину войны с системами контроля и управления. Это было впервые, когда Министерство обороны США, определило возможности и доктрину информационной войны.

В конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвящённый новой военной доктрине вооружённых сил США XXI столетия (концепции «Force XXI»/«Сила» XXI). В её основу было положено разделение всего театра военных действий на две составляющих – традиционное пространство и киберпространство, причём последнее имеет даже большее значение. Р. Банкер предложил доктрину «кибермaневра», которая должна явиться естественным дополнением традиционных военных концепций, преследующих цель нейтрализации или подавления вооружённых сил противника». На самом деле последующие исследования генерала Келера и его концепция геоцентрического ТВД показали ошибочность такого разделения.

«Таким образом, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включается и ионосфера (ионосфера – часть верхних слоёв атмосферы и входит в число заряженных оболочек земли в верхних слоях атмосферы, ближнего и открытого космоса). Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин «human network»/«человеческая сеть»).

Определение информационной войны Минобороны и спецслужбами США.

В октябре 1998 года, Министерство обороны США вводит в действие «Объединенную доктрину информационных операций». Первоначально эта публикация называлась «Объединенная доктрина информационной войны». Позже она была переименована в «Объединенную доктрину информационных операций». Причина изменения состояла в том, чтобы разъяснить отношения понятий информационных операций и информационной войны. Они были определены, следующим образом:

Информационная операция: действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем.

Информационная война: комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на её военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны – инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

Как указывают американские военные эксперты, информационная война состоит из действий, предпринимаемых с целью достижения информационного превосходства в обеспечении национальной военной стратегии воздействием на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации, информационных систем и инфраструктуры.

Информационное превосходство определяется, как способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое. Оно может быть также определено и как способность назначить и поддерживать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во всё время её проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях.

Информационное превосходство позволяет иметь реальное представление о боевой обстановке и даёт интерактивную и высокоточную картину действий противника и своих войск в реальном масштабе времени. Информационное превосходство является инструментом, позволяющим командованию в решающих операциях применять широко рассредоточенные построения разнородных сил, обеспечивать защиту войск и ввод в сражение группировок,

состав которых в максимальной степени соответствует задачам, а также осуществлять гибкое и целенаправленное материально-техническое обеспечение.

Информационное противоборство осуществляется проведением мероприятий, направленных против систем управления и принятия решений (Command & Control Warfare, C2W), а также против компьютерных и информационных сетей и систем (Computer Network Attack, CNA).

Деструктивное воздействие на системы управления и принятия решений достигается проведением психологических операций (Psychological Operations, PSYOP), направленных против персонала и лиц, принимающих решения и оказывающих влияние на их моральную устойчивость, эмоции и мотивы принятия решений; выполнения мероприятий по оперативной и стратегической маскировке (OPSEC), дезинформации и физическому разрушению объектов инфраструктуры.

Какова ситуация сегодня?

Пару лет назад Центральное разведывательное управление (ЦРУ) упоминало только Россию и Китай в качестве основных источников угрозы из киберпространства. Сегодня американские эксперты отмечают, что уже более 20 стран планируют и осуществляют различные виды информационных операций, направленных против Соединённых Штатов (вполне, впрочем, заслуженно). ЦРУ отмечает, что ряд противостоящих США государств, включают информационную войну как часть свих новых военных доктрин.

Рассекреченная оценка угрозы, проведенная Военно-морским флотом США, выделяет Россию, Китай, Индию и Кубу в качестве стран, которые открыто подтвердили политику подготовки к информационной войне, и которые быстро развивают их способности в этом направлении. Северная Корея, Ливия, Иран, Ирак и Сирия по сообщениям имеют некоторую способность к движению в этом направлении, а Франция, Япония и Германия уже весьма активны в этой области.

Как же видят в разных государствах основные подходы к ведению информационной войны?

Россия

До последнего времени у нас практически не существовало ясной государственной позиции по этой проблеме, что, собственно, и привело к поражению в Холодной войне. Только в сентябре 2000 года Президентом РФ была подписана Доктрина информационной безопасности России. В отличие

от подхода, обозначенного США, в российской Доктрине на первое место ставится обеспечение информационной безопасности индивидуального, группового и общественного сознания.

Для реализации основных положений Доктрины и обеспечения информационной безопасности России было создано Управление информационной безопасности в Совете Безопасности РФ.

Сегодня в работах по формированию отечественного представления информационной войны занимаются Министерство обороны, ФАПСИ, ФСБ и знаменитое Управление «Р» МВД, которое проводит расследования преступлений в высокотехнологической сфере информационных технологий.

США

Деятельность американской администрации в области защиты критической инфраструктуры берёт своё начало с формирования Президентской комиссии по защите критической инфраструктуры (President's Commission for Critical Infrastructure Protection) в 1996 году. Отчётный доклад этой комиссии выявил уязвимости национальной безопасности США в информационной сфере. Итоги работы комиссии были положены в основу правительственной политики в области обеспечения информационной безопасности критической инфраструктуры, сформулированной в Директиве президента № 63, подписанной в июне 1998 года (PDD-63).

Во исполнение указаний президента, обозначенных в этой директиве, был разработан Национальный план защиты информационных систем США, подписанный президентом 7 января 2000 года. На реализацию этого плана было затребовано 2,03 миллиарда долларов из федерального бюджета»[93].

Динамичное развитие информационно-телекоммуникационных технологий на основе широкого применения методов цифровой обработки ставит перед разведывательными службами промышленно развитых государств в качестве одной из приоритетных задач установление контроля использования не только технических средств, но и их программного обеспечения. Подтверждением указанного предположения является сообщение о том, что официальные лица США открыто признали факт тесного многолетнего сотрудничества между спецслужбой Агентства национальной безопасности (АНБ) США и компанией Microsoft. В частности, ещё в конце 1990-х гг. стало известно, что при изучении кода подпрограмм в операционной системе (ОС) Windows NT была обнаружена переменная с именем NSAKEY (то есть «ключ АНБ»). Речь также идёт о совместной работе Microsoft и АНБ США

93 *Гриняев С.Н. – Информационная война: история, день сегодняшний и перспектива*

над ОС Windows Vista. Кроме того, именно АНБ, когда этого требовали американские законы, всегда контролировало понижение стойкости криптографии в программных продуктах, предназначенных для экспортных продаж[94].

Что касается активного вмешательства разведывательных служб в работу ИТКС, то здесь уместно вспомнить ряд фактов непротоколированной обработки информации и обнаружения закладок в программном обеспечении импортного оборудования:

– в системах ПВО, закупленных Ираком в одной из западноевропейских стран (заложены «логические бомбы», в результате чего во время войны в зоне Персидского залива эти системы не могли быть задействованы)[95];

– в станции сотового оператора греческой сети сотовой связи Vodafone Greece в 2006 г. – программная закладка, которая дублировала звонки более сотни мобильных абонентов (включая премьер-министра, высокопоставленных военных чиновников и крупных бизнесменов) на 10 анонимных мобильных телефонов (встроена при участии АНБ США и американской компании SAIC в процессе модернизации станции при подготовке к Олимпиаде-2004 в Афинах)[96];

– в криптографических средствах, поставляемых швейцарской компанией Crypto AG в ряд стран – закладка, снижающая стойкость криптографических средств (встроена при участии экспертов АНБ США)[97].

С развитием и внедрением информационных технологий трансформируются привычные критерии оценки военной мощи и политических возможностей государства. Видоизменяются традиционные формы силового противоборства[98]. Наблюдаются постоянные попытки отдельных государств сформировать у широких кругов мировой общественности негативный образ России. Прилагаются усилия по изменению расстановки сил в наиболее важных регионах мира, основанные на антироссийских настроениях. Периодически реанимируется информационная поддержка действий сил сепаратизма на Северном Кавказе с основным упором на проблемы соблюдения прав человека. Иностранными спецслужбами оказывается комплексное воздействие на систему государственного и военного управления страной, её политическое и военное руководство. Расширяется антиправительственная и антигосударственная деятельность ряда неправительственных организаций, активно поддерживаемых из-за рубежа.

---

94 Крикунов А., Королёв А. – Особенности ...

95 Онорский Б. – Информационная война – основная форма борьбы ближайшего будущего? Обозреватель/Observer, 1998, № 5

96 Крикунов А., Королёв А. – Особенности будущих информационных войн

97 Гусаров А. – Защита информации в сетях связи. Военная наука и техника, № 2, 2007

98 Крикунов ... – Особенности ...

Так, например, в результате таких информационных атак, совмещаемых с агентурным и финансовым сопровождением, критическая ситуация складывается в Ставропольском крае. Его даже начинают именовать «российским Косово». Там наблюдается устойчивый тренд по замещению русского населения дагестанцами, азербайджанцами, чеченцами и другими представителями кавказских этносов. При этом используются методы, отработанные ранее в сербском крае Сербии и Метохии.

«В феврале 2001 года Конгрессу США был представлен отчёт о ходе реализации PDD-63. Одной из наиболее важных выполненных Министерством обороны США работ в этом направлении, является существенное продвижение по пути совершенствования приемов и методов работы с доказательствами компьютерных преступлений, что имеет большое значение при проведении расследований любых инцидентов, связанных с применением вычислительной техники. Так 24 сентября 1999 года была открыта Компьютерная судебная лаборатория Министерства обороны (Defense Computer Forensics Laboratory, DCFL).

Это – одна из наиболее современных структур, предназначенная для обработки компьютерных доказательств о преступлениях и мошенничествах, а также при проведении контрразведывательных мероприятий для всех организаций, проводящих криминальные и контрразведывательные исследования. Управление специальных исследований Военно-воздушных сил США определено в качестве Исполнительного агентства для DCFL. В настоящее время DCFL имеет 42 позиции для исследователей и судебных приставов, позволяющие обрабатывать компьютерные доказательства наряду со звуковой и видеоинформацией в судебных делах в самом широком диапазоне: от детской порнографии до вторжений в компьютеры и шпионажа.

Эта лаборатория министерства обеспечивает поддержку ФБР по вопросам расследования компьютерных преступлений. Специалисты DCFL уже накопили определенный потенциал и навык работы с инструментальными средствами анализа информации в ходе ряда успешных мероприятий по идентификации групп хакеров, а также при нейтрализации очагов уязвимости в нескольких контрразведывательных операциях, связанных с деятельностью по защите национальных сетей ЭВМ. Среди последних – такие нашумевшие мероприятия как «Солнечный восход», «Цифровой демон» и «Лабиринт лунного света» («Solar Sunrise», «Digital Demon», «Moonlight Maze»).

С целью улучшения способности активно защищать информационные системы и компьютеры была создана Объединенная оперативная группа по защите компьютерной сети Министерства обороны (Joint Task Force for Computer Network Defense, JTF-CND), а главнокомандующий космического

командования принял полную ответственность за защиту сетей ЭВМ министерства с 1 октября 1999 года. Как отмечают авторы отчёта, в ходе инцидента с вирусом «Мелисса» в марте 2000 года, JTF-CND, совместно с Группой реагирования на чрезвычайные ситуации с вычислительной техникой Министерства обороны (Computer Emergency Response Team, CERT), оказалась способной быстро оценить угрозу, сформировать оборонительную стратегию и направить ход соответствующих оборонительных действий. Далее, в мае 2000 года, в ходе эпидемии компьютерного вируса «LOVELETTER» был продемонстрирован ещё один пример чётких действий JTF-CND. Персонал JTF быстро идентифицировал потенциальное повреждение и обеспечил своевременное уведомление подразделений, служб и агентств министерства, которые позволили им эффективно ответить на вторжение.

С 2000 года Министерством обороны начата работа с союзниками по вопросу обеспечения информационной безопасности: Канада имеет официального представителя, работающего в JTF-CND, развивается система разделения информации между министерствами обороны в соответствии с основными положениями Меморандума о понимании и Концепции действий подписанными с канадской стороной»[99].

США до сих пор являются лидерами в создании информационного оружия. Ими еще в 1986 году была сформулирована Концепция «Соперничество», в которой декларируется: «Посредством правдивой и ложной информации об экономике, управлении, о вооружённой борьбе можно достичь целенаправленного регулирования процессов принятия необходимых для нас решений руководством другого государства».[100] В июне 1993 года распоряжением министра обороны и директора ЦРУ была создана Объединенная комиссия по безопасности, которая проработав 9 месяцев, подготовила доклад. В нем, в частности говорилось: «…Уже признано, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого ещё предстоит тщательно разработать, будет использоваться с «электронными скоростями»[101] при обороне и нападении. Информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела». Свежо предание …

В 1995 г. состоялся первый выпуск специалистов по проблемам информационной войны в Национальном университете обороны. Во всех военных учебных заведениях введены специальные курсы и налажена подготовка офицеров по этому профилю. В ВУЗах отрабатываются планы и проводят-

---

99 Гриняев С. Н. – Информационная война: история, день сегодняшний и перспектива

100 А. В. Манойло «Государственная информационная политика в особых условиях», Монография, М.: Изд. МИФИ, 2003 г.

101 Там же

ся тренировки по ведению информационной войны. А в 1996 г. Пентагоном были проанализированы и обобщены итоги проведения свыше десятка секретных штабных учений по ведению информационной войны, которые проводились в течение двух лет с 1994 года. Министерство обороны США в 1996 г. приняло «Доктрину борьбы с системами контроля и управления». Для ведения информационной войны в Вооруженных Силах США созданы специальные подразделения и структуры (центр информационной войны ВВС США, центр Сухопутных войск по разработке мероприятий по информационной войне, центр разработки мероприятия по информационной войне ВМС США, центр информационной войны ВМС США, центр технологии информационной войны, центр сетевых операций ВВС США, армейский центр сетевых операций, компьютерное и телекоммуникационное командование ВМС США, центр безопасности операций в глобальных сетях и другие). В документах министерства обороны США подробно излагается порядок подготовки к информационной войне, которая осуществляется по трём направлениям: в вооружённых силах, в спецслужбах и в национальном масштабе. Как было отмечено ранее, в 1996 г. была организована комиссия по защите критической инфраструктуры (President's Commission for Critical Infrastructure Protection). На результаты деятельности комиссии опирались при разработке направлений работы Правительства в области обеспечения информационной безопасности критической инфраструктуры, положения которой сформулированы в директиве президента №63 (PDD-63). Только в рамках одного военного ведомства, министерства обороны США, разработкой вопросов информационной войны заняты около четырех десятков организаций. Они задействованы в обеспечении безопасности информационных систем, проведением операций в информационных сетях, обеспечением, разведкой, расследованием преступлений в сфере компьютерных технологий. Ещё в 1994 г. в ВС США финансирование информационных технологий получило приоритетный характер, опередив даже ракетно-ядерные и космические программы. При этом субсидирование расходов на информационную безопасность составляет около 50 миллиардов долларов в год.

«Проведены работы по созданию системы сигнализации при обнаружении уязвимости информационной безопасности (Information Assurance Vulnerability Alert, IAVA) для распределения информации об уязвимости всем подразделениям и службам Минобороны. В 1999 году этой службой было подготовлено и выпущено 11 предупреждений (IAVT), 3 бюллетеня (IAVBs) и 20 технических консультаций. В 2000 году были выпущены 3 предупреждения, 3 бюллетеня и 9 технических консультаций. Агентство информационных систем Минобороны (Defense Information System Agency, DISA) сформировало банк данных, для немедленного распределения информации

об уязвимости каждому администратору системы вместе с краткой информацией о возможных ответных действиях по локализации последствий.

Безусловно, за прошедший год американскими коллегами проделана большая работа. Однако следует задуматься, а насколько она оказалась эффективной?

Информация, доступная по каналам Интерент, позволяет сделать вывод о том, что уровень информационной безопасности систем Минобороны США, несмотря на реализованные мероприятия, увеличился незначительно[102]. Атаки китайских хакеров на системы Минобороны в период кризиса, вызванного инцидентом с разведывательным самолетом Е-3, оказались достаточно эффективными.

Согласно ряду заявлений сотрудников администрации США, созданная национальная система информационной безопасности, оказалась слишком тяжеловесной и неповоротливой. В ряде случаев процесс доведения информации тормозился в силу бюрократических проволочек, что приводило к неприятным последствиям[103].

Во многих случаях при появлении нового вида компьютерных вирусов противоядие не было своевременно найдено ни сотрудниками CERT, ни JTF-CND.

Существенным препятствием в достижении поставленных целей остается нехватка квалифицированного персонала для работы в сфере обеспечения информационной безопасности, о чём свидетельствуют попытки привлечения студентов-компьютерщиков на работу в федеральные ведомства по контрактам в обмен на оплату их обучения в высших учебных заведениях»[104]. Кроме того, подразделения, которые занимаются борьбой с киберпреступностью, проявляют всё большую активность и успешно склоняют к сотрудничеству новых хакеров, угрожая тем серьёзными тюремными сроками в случае отказа. С помощью такого подхода американские спецслужбы сформировали целую армию информаторов среди хакерского сообщества[105].

Вообще говоря, наёмничество как способ замены регулярных вооружённых сил полубандитскими и всегда криминализованными иррегулярными подразделениями стало одним из основных трендов в военной политике США[106]. Это, безусловно, даёт возможность, во-первых, хотя бы формально уходить от ответственности за деяния своих наёмников. Во-вторых, это

---

102 США и Великобритания готовят ответную атаку против восточных хакеров («The Guardian», Великобритания)

103 В электрическую сеть США проникли шпионы («The Wall Street Journal», США)

104 Гриняев С. Н. – Информационная война: история, день сегодняшний и перспектива

105 Корли Эрик (Eric Corley) – Американские спецслужбы активно вербуют хакеров. Журнал 2600: The Hacker Quarterly

106 Спектор В. Н., Крикунов А. В. и Спектор Н. В. – Наёмничество космополитическое и внутригосударственное. Труды МАН ПНБ. М., том 3

позволяет более гибко осуществлять набор нужных кадров – не содержать их перманентно, а по ограниченным по времени контрактам, но с оплатой, превышающей предусмотренную для военнослужащих по штатному расписанию. И, наконец, в-третьих, такая система позволяет использовать высококлассных бывших военных специалистов, уволенных из вооружённых сил за нарушения/преступления, совершённые в ходе выполнения сомнительных приказов командования, и таким образом вознаграждать их за преданность. Наёмничество/аутсортинг даёт, конечно, дополнительные возможности, но при этом необходимо помнить, что то, что продаётся, может быть перекуплено (for a higher bid).

Мы уже упоминали, что в мирное время информационная война может рассматриваться как разновидность государственного терроризма. Однако переход к практике государственного терроризма ведёт к деградации самого государства по самому неприятному пути – по пути деградации демократических традиций[107].

Движение США по этому пути подтверждается и тем, что на Совете национальной безопасности в феврале 2003 года президент США утвердил «Положение о концепции и принципах ведения компьютерных информационных войн на территории других государств» (заметим, в мирное время). Данная концепция определяет, когда и при каких обстоятельствах президент США, директора Агентства национальной безопасности и ЦРУ, министр обороны США и другие должностные лица могут принять коллективное или индивидуальное решение на проведение специальной операции по нейтрализации или полному разрушению информационного пространства чужого государства, выводу из строя или нейтрализации линий связи и управления, как с территории США, так и сопредельных к противнику территорий.

Так, власти США причастны к разработке трёх новых вирусов для шпионажа и кибератак. Об этом говорится в докладе американской компании по производству программного обеспечения Symantec/Симантек.

По данным компании, руководство Соединённых Штатов имеет непосредственное отношение к созданию компьютерного червя Stuxnet, использованного для сбора данных об иранской ядерной программе в 2010 году, а также к разработке инструмента кибернаблюдения Flame. Специалисты указали на то, что коды этих вирусов-шпионов очень похожи[108].

Русскую притчу «повадилась лиса жернова лизать» можно по ситуации продолжить «жернова закрутились, и язык злодейке оторвали». Американский Национальный совет по разведке (НСР), который объединяет предста-

---

107 Спектор В. Н. – Десять шагов на пути США от государственного терроризма к фашизму (по Ягужинскому). Труды МАН ПНБ. М., том 3

108 Тяпшева Светлана – Доклад: США создали вирусы для кибервойн. 18.09.2012

Источник: ru.wikipedia.org

Сергей Леонидович Магнитский

вителей 16 разведывательных ведомств США (куча мала – врут президенту, врут друг другу, врут всем), презентовал в Вашингтоне аналитический доклад «Глобальные тенденции 2030: Альтернативные миры»[109]. Это «исследование» стало пятым по счёту с момента запуска данного провокационного проекта.

По первому докладу, в котором беззастенчивое враньё и аваланч дезинформации припудривались пылью политической демагогии, МАН ПНБ был сделан углубленный геополитический анализ, высветивший и враньё, и дезинформацию. Уже на протяжении двух-трёх лет жизнь показала точность анализа Академии, и Академия приняла решение в дальнейшем не тратить силы и время на анализ пропагандистского досужего бреда. По-видимому, зря. Этот бред имел определённые цели, и главная из них запугать и дезориентировать мировое общественное мнение, посеять смуту и недоверие хотя бы на пару-тройку лет, а там новую пугалку издать можно. Именно поэтому необходимо ловить этих «оракулов» на каждой, даже самой мелкой лжи, на самой кажущейся невинной дезинформации и показывать всему миру их истинное лицо.

Такой новой пугалкой стал Акт Магницкого, заказанный американским миллиардером Эдмоном Сафрой (позже убиенным) и его тоже не бедным англо-американским подельником Уильямом Браудером, с 1996 года обосновавшихся в России и образовавших международную ОПГ, включавшую российских силовиков и налоговиков.

Несмотря на многочисленные скандалы, связанные с проведением нелегальных финансовых сделок, таинственная семья Сафра (на международном жаргоне «таинственная семья» – нечто даже более мафиозное, чем «ельцинская семья) и сегодня представляет собой образец успеха в банковском бизнесе. <…>, что стало причиной безвременной кончины их «золотого мальчика», Эдмонда Сафра,

После Второй мировой войны семейство Сафра перебралось (от закона) в Бразилию. Их частная жизнь оставалась для остального мира тайной за семью печатями.

Банкиры Сафра известны осмотрительностью, все формальные записи фиксируются при помощи арабского письма, известного только хорошо образованным сефардам (испанским евреям).

---

109 Американская разведка сделала прогнозы на 2030 год. Российская газета, 10.12.2012

В 1966 году Э. Сафра основал Republic National Bank of New York/Республиканский Национальный банк Нью-Йорка. Предприятие оказалась более чем успешным. К середине 1980-х банк вошёл в тройку крупнейших на территории Нью-Йоркского региона, наряду с Citigroup и Chase Manhattan. Затем закон, ох уж этот закон, вынудил его с банком расстаться.

Источник: en.wikipedia.org

Эдмон Сафра

В 1996 году вместе с Эдмоном Сафрой Билл Браудер основал фонд Hermitage Capital Management для инвестиций в России. Фонд был известен своей активностью по защите прав миноритарных акционеров Газпрома, Сургутнефтегаза, РАО ЕЭС и Сбербанка. Браудер неоднократно вскрывал случаи коррупции в этих полугосударственных компаниях. В интервью Нью-Йорк Таймс он как-то сказал: Ты должен стать акционером с активной гражданской позицией (то есть как «юный пионер» должен быть всегда готов к борьбе с конкурирующими, в том числе государственными структурами и к внутренней дисциплине в ОПГ), если ты не хочешь, чтобы тебя дочиста обокрали.

Источник: ru.wikipedia.org

Уильям (Билл) Феликс Браудер

Одним из таких миноритариев со статусом партнёра стал С. Л. Магнитский. Он был руководителем отдела налогов и аудита в фирме Firestone Duncan, оказывавшей юридические услуги, в том числе и фонду Hermitage Capital Management (то есть много знал о делишках фонда, более того, разрабатывал для него схемы «оптимизации налогов», то есть ухода от них). Летом 2007 года российское отделение фонда Hermitage Capital заподозрили в уклонении от уплаты налогов. В ходе проведенных обысков была изъята документация фонда, а в аудиторской фирме Firestone – печати фирм, с использованием которых фонд работал в России.

В июне 2007 года управление по налоговым преступлениям ГУВД Москвы завело уголовное дело против аффилированных с фондом компаний. Следователи обвинили ООО «Камея» в неуплате налогов на сумму свыше 1,145 миллиардов рублей. Газета «Коммерсантъ» (отнюдь не проправительственная) писала: «Участники рынка тогда отмечали, что расследование является попыткой выявить незаконные схемы реализации акций «Газпрома», которые покупались российскими компаниями в пользу иностранных инвесторов, не имевших разрешения властей». В Интер-

Источник: mixednews.ru

Синагога Сафры

нете без указания подробностей проскользнуло упоминание, что ОПГ Браудера имело деловые связи с ОПГ Сердюкова. Магницкий, который по указанию Браудера и Сафры разрабатывал противозаконные финансовые схемы с участием представителей силовых и финансово-экономических государственных структур, входивших в ОПГ Браудера, и в фабрикации компрометирующих материалов на сотрудников правоохранительных органов из конкурирующих ОПГ или не входивших ни в какие ОПГ, после ареста начал потихоньку сдавать подельников, выдавая это за содействие следствию. Это вовсе не радовало Браудера, который был также обвинён в России в финансовых махинациях и уклонениях от налогов, но скрылся за рубежом от российского правосудия, оставив младшего партнёра г-на Магнитского «расхлёбывать совместно грязно заваренную кашу».

Эдмонда нашли мёртвым в собственных подожжённых апартаментах в Монако.

Эдмонд Сафра отмывал награбленные в России деньги (ясно, не все, а лишь малую часть – во спасение души) в проектах специфической благотворительной деятельности, одним из наиболее заметных из которых стало строительство синагоги в Нью-Йорке.

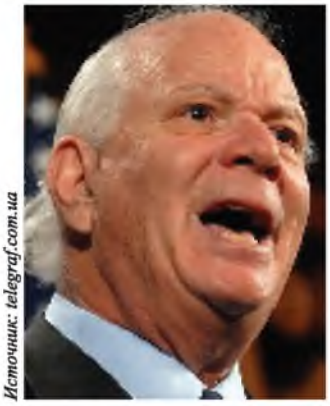
Известны разные версии относительно личности предполагаемого виновника поджога. Некоторые обвиняют в этом преступлении русскую мафию (почему бы и нет? – преступное организованное сообщество, которое Сафра и Браудер создали в России для ухода от налогов и других грязных делишек, наверняка не было заинтересовано в разговорчивости Сафры[110], также как и Магницкого.

При этом нельзя исключить, что заказчиком ликвидации обоих мог быть создатель своего ОПГ в России У. Браудер – Quid prodest. Понятно, что и устранение Магницкого и Сафры, и организация информационной войны против России, и устранение Сафры обошлись, скорее всего, Браудеру недёшево, также как Сафре прижизненное лоббирование Акта Магницкого в Конгрессе и Сенате США, в структурах Евросоюза и в различных международных структурах, подведомственных международному банковскому консорциуму. Однако все эти привходящие расходы обошлись Браудеру и братьям Э. Сафры в малые проценты от денег, «наколоченных» в России этими смердящими дельцами.

---

110 http://www.businessinsider.com/the-story-behind-the-safras-bankings-most-mysterious-family-2012-6?op=1#ixzz20URMxpl7

Председатель подкомитета Европарламента по правам человека Хейди Хаутала, отрабатывая деньги Сафры, так прокомментировала результат голосования о поддержке очередной американской акции информационной войны с Россией: «Этим голосованием Европейский парламент призывает восстановить справедливость по отношению к невиновному человеку, умершему в тюрьме. Его смерть выходит за все границы. Наступает момент, когда возможности молчать не остается». Могли бы, правда, и помолчать, дожидаясь окончания следствия.


Источник: telegraf.com.ua

Бенджамин Кардин

В 2010 году международная неправительственная организация по борьбе с коррупцией Transparency International посмертно удостоила С. Л. Магнитского награды «За честь и достоинство» (Integrity Award). Как отмечается в заявлении Transparency International, награждая посмертно Сергея Магнитского, «организация отдает дань памяти человеку, который до последнего вздоха отстаивал правду, честь и человеческое достоинство».

Председатель комитета премии «За честь и достоинство» Сион Ассидон сказал: «Сергей верил в закон и справедливость и погиб, самоотверженно их отстаивая в неравной схватке с масштабной коррупцией в российских правоохранительных органах. Приверженность господина Магнитского принципам открытости и прозрачности государственной власти была в полной мере проявлена в его решительной борьбе с произволом властей. Его необыкновенное мужество и неослабевающая воля перед лицом тяжелых испытаний придают силы всем нам, она послужит примером для других борцов за справедливость». Это, безусловно, относится только к «борцам за справедливость» до полного уничтожения законности.

«Акт Магнитского» касается не только РФ, а носит универсальный характер», – заявил сенатор США Б. Кардин (ИТАР-ТАСС) <…> Кардин утверждал, что поправка носит чисто технический характер и «касается надзорных функций Конгресса США» (с какого перепугу Конгресс США должен быть допущен к надзору в России). <…> «Суть законопроекта заключается в том, что он предусматривает введение карательных мер против сотрудников российских силовых ведомств и судей» – по виду сенатор фанатик (см. фото), а по высказываниям – человек, пребывающий в помраченном сознании, с бредовыми иллюзиями и галлюцинациями».

Учитывая остервенелое давление отлоббированных конгрессменов и сенаторов, требовавших заменить один дискриминационный закон (эмиграционная поправка) другим (Актом Магницкого) для сохранения инстру-

мента давления на Российскую Федерацию, президент Барак Обама во имя договорённости по «фискальному обрыву» был вынужден подписать документ, содержавший как единое целое отмену ставшей невыгодной американскому бизнесу поправки и политический дискриминационный акт.

То, что Акт Магнитского есть ни что иное как акт легитимизации скоординированной информационной войны Запада с Россией подтверждается множеством фактов и «засветившихся» политических провокаций. Так, главный редактор газеты «Комсомольская правда» Владимир Сунгоркин, похоже, одним из первых стал жертвой «Акта Магнитского», принятого 14 декабря в США[111] – провокационное письмо на бланке одного из консульских подразделений США о приостановлении его визы в США поступило на адрес Сунгоркина за несколько часов до объявления о принятии Акта. Принесенные ему впоследствии извинения без объяснения обстоятельств появления этого извещения являются очевидным свидетельством неспровоцированной враждебной акции.

Письмо главреду «Комсомолки» от посольства США оказалось подделкой

Письмо от имени посольства США, направленное на имя главного редактора «Комсомольской правды» Владимира Сунгоркина, оказалось подделкой. Журналистам «Эха Москвы» сообщили в посольстве США, что подобного письма не отправляли.

Источник: ria.ru

На краю «фискального обрыва» американские сенаторы присутствуют при подписании Акта Магницкого *– Sergei Magnitsky Rule of Law Accountability Act.*

111 vesti.ru»doc. html? id=983987

На имя Сунгоркина вечером в пятницу, 14 декабря, был прислан факс якобы от имени вице-консула посольства США Алеты Ковенски в котором, в частности, говорилось, что «в связи с подписанием президентом США закона Магнитского» действие въездной визы главреда «КП» «приостановлено до особого распоряжения». Скан этого письма был выложен главредом телеканала Russia Today Маргаритой Симоньян в её твиттере, а затем опубликован и на сайте самой «Комсомолки» (к 23:45 по Москве заметку удалили).

Сунгоркин сообщил, что факс был прислан ему около 16:30, в то время как о подписании президентом США «закона Магнитского» было объявлено лишь около 21:00 по московскому времени.

Время получения факса – не единственная деталь, заставившая усомниться в подлинности этого уведомления. Так, Алета Ковенски не числится в списке сотрудников посольства США в РФ, а руководит консульским отделом в американском посольстве в Туркмении. Кроме того, бланк присланного Сунгоркину письма отличался от того, который обычно использует посольство США в своей переписке.

На момент написания заметки автор подделки оставался неизвестен.

Упоминаемый в поддельном письме «закон Магнитского», вводит визовые и финансовые ограничения в отношении граждан РФ, подозреваемых в причастности к нарушениям прав человека. «Закон Магнитского» был принят в США одновременно с отменой поправки Джексона-Вэника, ограничивающей торговлю с Россией. Принятие «закона Магнитского» вызвало резкую критику со стороны властей РФ, а депутаты Госдумы разработали свой ответ на этот документ – проект закона, запрещающего въезд в Россию ряду американских граждан.

Похоже, последний, пятый доклад «Глобальные тенденции 2030: Альтернативные миры» по иллюзорности мышления превзошёл все предыдущие. Чего стоит только горячо желаемая, но абсолютно не привязанная к действительности перспектива развития Российской Федерации, представленная американскими спуками своему политическому руководству, а заодно и всему миру.

«Экономика России будет медленно сокращаться», говорится в этом докладе Национального совета по разведке США. При этом главная угроза для России – растущая доля мусульманского населения. Как-то по хулиганской поговорке получается – «ехал поезд из Тамбова, поцелуй скорей кирпич».

Как пишет «Газета. ru»[112], в докладе отмечается, что экономика останется ахиллесовой пятой России. Немалую роль в этом сыграет зависимость

112 Хамидуллина Зоя – Американская разведка видит в России угрозу глобальной безопасности. 09.12.2012

страны от добычи полезных ископаемых, в частности нефти и газа. «Попытки модернизировать экономику не увенчались большими успехами, а старение её рабочей силы будет тормозить экономический рост», – указывают авторы доклада.

«Таким образом, угроза для региональной и глобальной безопасности со стороны России будет расти в том случае, если страна не сможет создать более диверсифицированную экономику и более либеральное внутригосударственное устройство», подчеркивается в докладе. Аналитики американской разведки предлагают России для спасения положения улучшить условия для иностранных инвестиций и создать возможности для экспорта российских промышленных товаров.

Кроме того, в отчёте говорится, что численность населения страны сократится к 2030 году до 130 миллионов человек. Несмотря на сопоставимую с другими странами рождаемость, продолжительность жизни в России на 15 лет меньше (где связь? – прим. авторов). При этом самая большая опасность для России, по мнению экспертов, кроется в быстрой динамике роста мусульманского населения при одновременном сокращении численности этнических русских.

Этот прогноз американского разведсообщества по России продержался ещё меньше, чем любой из предыдущих – меньше недели. Он был убедительно опровергнут в Послании Президента России В.В. Путина Федеральному Собранию Российской Федерации. Не специально конечно. Давая картину реального состояния и перспектив развития страны, В. Путин едва ли ориентировался на прогнозы политических пустобрёхов из Американского национального совета по разведке.

Реальную угрозу для Российской Федерации со стороны информационных технологий представляют стимулируемые извне подрывные внутренние противники не режима, а страны в целом, деятельность которых облегчается множеством зон уязвимости, на которые правительственные ведомства и избираемая законодательная власть не обращает должного внимания.

Приведём несколько примеров таких зон уязвимости, начиная с кажущихся незначительными и кончая теми из них, которые являются открытыми настежь воротами для самых разрушительных информационных атак.

Реклама как причина существования информационной зоны уязвимости.

На с. 18 уже упоминались возможности использования рекламы в качестве информационного оружия. Всем известно, что телевизионная реклама

вызывает острое социальное неприятие, чуть меньшее раздражение вызывает внешняя реклама – она всего лишь уродует внешний вид городов и при большом ветре может прибить горожан. В стране, пережившей революции, войны и «диктатуру пролетариата» (т. е. ВКП/ б – КПСС), где постоянно существовала нехватка продуктов питания и товаров широкого потребления, реклама была последней потребностью населения.

Пришла пора, когда у имеющей доступ к народным деньгам публики, в том числе и на телевидении, популярным стал лозунг «Воруем все!», и оказалось, что реклама является практически неисчерпаемым источником личного обогащения, за доступ к которому и убить не жалко – Листьева и не пожалели.

Дальше всё пошло и покатилось: содержание рекламы утратило смысл легитимного источника информации – рекламировалось всё: и алкоголь, и несъедобные продукты питания с непонятными названиями на чужом языке, и калечащие лекарства, и продажные девицы. В стране, где более 70% населения жило ниже уровня бедности, широко рекламировались предметы роскоши и дорогостоящий, недоступный большинству населения товар с забавной характеристикой цены – «всего» или «только».

У взрослого населения это вызывало и вызывает рост социальной ненависти, у молодёжи становится движущей силой к совершению преступления – украсть, ограбить, если придётся убить, но добыть деньги, чтобы заполучить нечто, что «всего» в разы или «только» на порядки больше прожиточного минимума.

Таким образом, в современной России реклама из инструмента информирования населения о доступных и качественных продуктах и товаров превратилась в зону повышенной социальной уязвимости. При информационной атаке по этой зоне уязвимости практически гарантировано возникновение массового социального бунта.

Проблемы гомосексуализма как причина существования информационной зоны уязвимостии.

Проблема гомосексуализма (Malade des Anglais), изначально раскрученная с приданием ей политического звучания в британской коммунистической прессе (конец 50-х – конец 70-х годов XX века), отсутствовала в российской и не появилась в советской традиции. Джугашвили столь же откровенно не одобрял такой стиль «товарищества». Эта тема вдруг, как иностранный джин из грязной бутылки, возникла в «независимой» России (1991) вместе с невесть откуда взявшимися деморосами – «отсидентами» и «досидентами». Многомиллионным демонстрациям в Москве

и других российских городах, приведшим к окончанию эры большевизма, такого не обещали.

И началась борьба за свободу гомосексуализма и против неё, борьба, создавшая вполне выраженную зону уязвимости в российском социуме. Поощряемые из-за рубежа гомосексуалисты начали остервенелую борьбу за свободу пропаганды гомосексуализма как социально-культурного явления и за социальное равенство, которого, кстати, никто их и не лишал, – в том хаосе и смуте, которые воцарились в ельцинской России (между прочим, сам Ельцин не жаловал гомосексуалистов, но за пьянками и прочими заботами не замечал их в своём окружении), до них просто руки не доходили.

На это явление по механизму социальной аллергии отреагировал неорганизованный, но начавший организовываться традиционный социум. В режиме международного информационного противоборства любой повод для усиления социального раздрая в стране оппонента является основанием для проведения информационных атак с целью формирования дополнительной зоны уязвимости или расширения латентно существующей.

Вероятно, в российских органах государственно власти существует определенное количество чиновников, являющихся участниками гомосексуальных сообществ, стремящихся присоединиться к ним или оказывающих им определённые услуги за деньги иностранных «инвесторов. Другая группа чиновников, имеющих традиционные сексуальные предпочтения и ведущих бескомпромиссную войну с экспансией гомосексуализма, не хочет или не может в силу преимущественно юридического образования понять известную физиологическую истину и строить на её основании стратегию и тактику информационной борьбы.

Эта физиологическая истина довольно проста, и состоит она в том, что от 5 до 15% позвоночных имеют генетические аберрации, определяющие склонность к гомосексуализму и подобным сексуальным отклонениям. Таким образом, природа осуществляет терминацию **тупиковых ветвей** животных популяций.

Ergo, мы имеем дело с неизлечимо больными людьми, так как генетические пороки, как правило, неизлечимы. Этот факт должен найти самое широкое распространение, подкреплённое ведущими российскими специалистами и ссылками на зарубежные авторитеты, во всех средствах массовой информации – телеконференции, обзорные газетные и журнальные публикации и бюллетени в поликлиниках и больницах.

Следующим этапом информационного противодействия может стать заключение учёных психиатров о консциентальной контаминозности

этих неизлечимых генетических заболеваний, также широко отражаемое во всех российских СМИ, о последующих наследуемых изменениях в генетическом коде и в формуле крови заразившихся. Дополнительно может быть сделана ссылка на утверждение о том, что эти изменения формулы крови переводят заразившихся как и самих гомосексуалистов в группу риска по ВИЧ инфицированию[113], позже подтверждённое в углубленных исследованиях американских учёных как по ВИЧ, так и по гепатитам[114].

На последнем этапе следует развернуть благотворительную кампанию по обеспечению нормальных условий жизни российских граждан с генетическими сексуальными аберрациями, их защиты от ВИЧ и гепатит инфицирования с выдачей рекомендаций российским гражданам, не имевшим гомосексуальной практики, о соблюдении мер по избеганию гомосексуальных контактов.

Одновременно необходимо принять закон об ответственности за вовлечение в гомосексуальную практику двух или более не имевших такой генетической аберрации лиц, приравняв такое деяние к умышленному убийству двух или более лиц, максимально ужесточив санкции за совращение или вовлечение в гомосексуальную практику детей и подростков.

Абсолютным императивом российского законодательства должен стать запрет на усыновление/удочерение детей лицами с генетическими сексуальными аберрациями, гомосексуальными парами и лицами, имевшими доказанную гомосексуальную практику. Законодательно исключить агитацию и пропаганду гомосексуальной практики, выдачу публичной информации о сексуальных аберрациях граждан как защиту их личной жизни, равно как и публичный экзибиционизм таких аберраций.

В качестве меры по защите имущественных и социальных прав лиц с генетическими сексуальными аберрациями необходимо принять закон о государственной регистрации контрактов о сожительстве таких лиц.

Установление такого правового и социального статуса для лиц с генетическими сексуальными аберрациями, во-первых, находится в пределах международного права и, во-вторых, позволит значительно снизить связанную с этой проблемой социальную напряжённость, то есть уязвимость российского общества в условиях информационного противоборства, а также обеспечить защиту лиц с генетическими сексуальными аберрациями от социальной агрессии, а общества – от распространения гомосексуальных практик среди граждан традиционной сексуальной ориентации.

---

113 Спектор В. Н. – Сообщение на международном экологическом симпозиуме

114 Спектор В. Н., Спектор В. А. – Глобализация, человек, климат и экология планеты. МАН ПНБ. М., 140 с.

Источник: ru.wikipedia.org

Ральф Густав Дарендорф

Источник: www.livelib.ru

Элвин (Олвин) Тоффлер

Проблемы размывания традиционных норм общественного поведения как причина существования информационной зоны уязвимости.

Основные составляющие современного мира, который является сложно организованной системой, с глобальными информационными технологиями и коммуникациями, – национальное и международное, объективное и субъективное, материальное и идеальное. Все вкупе создает новый синтез – планетарно выраженную целостность. Это по новому организует и общественную жизнь. В футурологии 60-70 годов XX века общество будущего, к которому, как считали авторы, идет человечество, называлось по-разному: «посткапиталистическое» или «общество сервисного класса» (Р. Дарендорф), «супериндустриальное» или «общество третьей волны» (Э. Тоффлер),. Французский экономист, социолог Жан Фурастье, определяя общество как «цивилизацию услуг», считал технику главным фактором в «смене цивилизаций» – первичной (сельское хозяйство), вторичной (промышленность), третичной (сфера услуг) и современной, четвертичной (духовное производство)). Японский социолог и футуролог, один из авторов концепции информационного общества Ёнэдзи Масуда называл общество «информационно-компьютерным». В 1972 году он представил «План для информационного общества – национальная цель к 2000», который позже был расширен и вышел в виде книги «Информационное общество как постиндустриальное общество» (1980)), «постэкономическое» (П. Ф. Друкер) и другие. И все же самыми распространенными и общепринятыми стали понятия «постиндустриальное» и, позднее, – «информационное» общество.

«Концепция постиндустриализма наиболее ярко была представлена в работах Д. Белла. Отличительной чертой постиндустриальной стадии, по мнению Д. Белла, является переход от производства вещей к развитию производства услуг, связанных с образованием, здравоохранением, исследованиями и управлением. Знание и информацию американский учёный объявил не только эффективным катализатором трансформации общества, но и его стратегическим ресурсом.

Понятие «постиндустриальное общество» быстро вошло в употребление и широко используется в современной научной литературе, но сегодня всё более очевидным становится тот факт, что наиболее характерной чертой современного общества является всё-таки его тотальная информатизация.

Источник: www.coach-s.narod.ru

Питер Фердинанд Друкер

Развитие общества по подобному сценарию прогнозировали, в первую очередь, японские исследователи. Одну из наиболее интересных и разработанных философских концепций информационного общества изложил Ё. Масуда. Фундаментом нового общества, по его мнению, должна была стать компьютерная технология, главная функция которой виделась им в замещении либо значительном усилении умственного труда человека. Как и предполагал Масуда, информационно-технологическая революция быстро превратилась в новую производственную силу и сделала возможным массовое производство когнитивной и систематизированной информации, новых технологий и нового знания. Потенциальным рынком стала «граница познанного». Ведущей отраслью экономики стало интеллектуальное производство, продукция которого аккумулируется и распространяется с помощью новых телекоммуникационных технологий.

Источник: www.strf.ru

Дэ́ниел Белл

За последнее десятилетие к теме глобального информационного общества неоднократно обращались многие отечественные учёные, которые разработали собственные концепции нового общества и его безопасности: В.Л. Ино-

М., 2005; Тоффлер Э., Тоффлер Х. – Война и антивойна*/War and Anti-War, 1995. ACT. M., 2005, 416 с.*

земцев, А. В. Бузгалин, Г. Л. Смолян, Д. С. Черешкин и многие другие[115].

Общим итогом всех перечисленных подходов выступает мысль о том, что информация сегодня является основной детерминантой общества, к существенным особенностям которого следует отнести, во-первых, возможность быстрого обмена информацией и её преобразования в новое знание, а во-вторых, экспоненциальное увеличение объёмов производимой и поставляемой потребителю информации.

Подавляющее большинство исследователей считает, что бурное развитие информационно-телекоммуникационных технологий, которые проникают во все сферы жизни, открывает совершенно новые возможности для общественного прогресса. Однако эйфория по этому поводу постепенно проходит и наступает период трезвой оценки реального вклада новых информационных технологий и в производство, и в социальные трансформации. Например, степень компьютеризации США на порядки выше, чем в нашей стране, но исследование, которое должно было выявить долю национального продукта, произведенного благодаря применению информационных технологий, оценило их вклад примерно в 1%[116].

В нашей стране эта величина будет (если её вообще возможно посчитать) ещё меньше. Более того, она будет, скорее всего, отрицательной, то есть затраты на внедрение новейших информационно-телекоммуникационных технологий не окупаются ни в материальном плане: повышение производительности труда, снижение числа занятых в производстве единицы товара и. т. д., ни в моральном: удобство, возможность контроля, снижение затрат времени и т. п.

Не наблюдается и повышение качества обучения вследствие внедрения новых форм обучения и самообучения, основанных на информационных технологиях и телекоммуникациях, как того ожидали многие специалисты[117].

Тотальное внедрение информационных технологий привело к революционным изменениям во многих социальных компонентах современного общества и в значительной мере снизило устойчивость существующих в нём норм и отношений, которые выполняют теперь не столько регулятивную, сколько адаптивную функцию.

---

115 Атаманов Г. А. – Информационные технологии: плюсы и минусы внедрения. Изд. ВГСХА «Нива». Известия нижневолжского агроуниверситетского комплекса, 2006, № 4, с. с. 112-120

116 Кастельс М. – Информационная эпоха: экономика, общество, культура/пер. с англ.; под науч. ред. О. И. Шкаратана. ГУ ВШЭ. М., 2000,.608 с.

117 Дриккер А. С. – Эволюционный прогноз: пульсация народонаселения; Синергетическая парадигма. Нелинейное мышление в науке и искусстве. М., 2004, с. с. 429-446 (435)

Информационное общество, являясь открытым, самоизменяется, находясь в постоянном поиске внутреннего соответствия между своим расширением и усложнением, с одной стороны, и стремлением к устойчивости, порядку, безопасности, с другой. И именно в единстве этих тенденций и выстраивается новая структура и упорядоченность общества. Важной закономерностью развития в этой связи становится возрастающее значение механизма синхронизации, достижения соответствия между темпо-ритмическими колебаниями различных подсистем социально-культурной системы общества. Другими словами, тотальная информатизация несёт не только огромный потенциал повышения производительности труда, производства усовершенствованных товаров и услуг, реальное повышение качества жизни, но и создаёт новые опасности и угрозы для социальных субъектов.

Попытки решить глобальные проблемы на чисто системной основе (при отсутствии адекватного таким задачам общечеловеческого субъекта), оказались бесплодными. Например, модели устойчивого развития, оказались практически недостижимыми из-за предлагаемых средств и механизмов их реализации.

Их построение невозможно без качественных изменений человеческого фактора – достижения высокой духовности общества; широкого распространения моральных и этических принципов; стиля жизни, соответствующего как потребностям настоящего периода, так и будущего; ответственности каждого человека за сохранение жизни на планете. В этих моделях предполагалась также абсолютная управляемость общества за счёт согласования интересов жителей планеты.

Сегодня мы далеки от такого идеала: устойчивости и внутреннего единства людей современной цивилизации нельзя достичь при сохранении социальной и политической напряжённости в отдельных странах, регионах и в мире в целом. Отсутствие реального успеха в реализации теории устойчивого развития является следствием неспособности человечества поставить под контроль действия конкретных индивидов. Это обстоятельство обусловлено, прежде всего, господством активно внедряемой и поддерживаемой Западом либерально-монетаристской идеологии»[118].

Главная парадигма информационального (Кастельс) общества – «противоречие между колоссальными возможностями по воздействию на социальную организацию и сознание человека, предоставляемыми новыми информационными технологиями, с одной стороны, и угрозами их использования в деструктивных по отношению к индивидууму, социальной группе, нации, всему человечеству целях, с другой. То есть появляется необходимость изу-

118 Атаманов Г.А. Информационные технологии: плюсы и минусы внедрения, Известия нижневолжского агроуниверситетского комплекса. – 2006. – №4

Источник: ru.wikipedia.org

Мануэль Кастельс

чения нового вида опасности – информационной. Без учёта этого феномена невозможно прояснение пути обеспечения прогрессивного развития современного общества»[119].

Информационная опасность имеет множество форм своего проявления: создание виртуальных миров, которые подменяют реальность; манипулирование сознанием и поведением людей; подмена целей, ценностей, своего образа жизни внешне навязанными стандартами; искажение информации и т. д.

Эти процессы обусловлены социальными аспектами процесса информационного взаимодействия: отношением людей к информации, потребностью в ней и, в то же время, неспособностью чётко различать истинное и ложное, полезное и бесполезное.

В социальном аспекте такая угроза чревата, в первую очередь, возможностью утраты личностью, группой, обществом своих субъектных качеств и сознания позитивной (по отношению к данной стране, обществу, политической системе) идентичности, в том числе и в результате их вытеснения внешними информационными потоками, подмены реальной картины мира её виртуальными «проекциями», выстроенными при помощи новейших информационных технологий и внедряемыми в общественное сознание посредством изощрённых методов информационного воздействия[120].

Сознание массового человека оказывается насквозь структурировано немногими, но настойчиво внедряемыми в него утверждениями, которые, бесконечно транслируясь средствами информации, образуют невидимый каркас из управляющих мнений, установлений, ограничений, который определяет реакции, оценки, поведение, как отдельного индивида, так и общества в целом.

Одной из самых существенных предпосылок возникновения информационной опасности является тоталиризация информационной сферы. Информация уравняла в собственном существовании (как виды знаний) предметы, средства и способы их обработки, средства общения между людьми. Символы и тексты становятся такой же предметностью, выраженной в знании, как материальные объекты, организации, институты, поскольку всё это выражено в терминах программ, нормативов, функций, понятий, – в языке информации. Здесь всё измеряется «количеством сообщений».

---

119 Кастельс, М. Информационная эпоха: экономика, общество, культура/Мануэль Кастельс/пер. с англ.; под науч. ред. О.И. Шкаратана. – М.: ГУ ВЩЭ, 2000.

120 Атаманов ... – Информационные ...

Информационная сфера, постоянно расширяясь, развивается по своим, ещё не осознанным и не изученным субъектом, законам, постепенно выходит из под его управления, начинает довлеть над ним, диктуя свои правила и нормы поведения, то есть приобретает черты субъекта (становится «квазисубъектом»).

Информационная система, «захватывая» в пространство своего воздействия человека, начинает манипулировать его сознанием и поведением. Появляется опасность подчинения человека внешним, овеществленным процессам, что, в свою очередь, может привести к утрате им самого себя, а вместе с этим – и к опустошению общества, разрушению существующих в нём социальных, культурных, психологических и других связей.

Другой, не менее важной особенностью современности является, предоставляемая новейшими информационно-телекоммуникационными технологиями, возможность практически неконтролируемого национальными правительствами трансграничного перемещения информации.

Трансграничное информационное воздействие разрушает традиционно складывающиеся общественные связи и делает саму общественную систему неустойчивой и внутренне разбалансированной. Это усиление воздействия информации связано с тем, что «знания и информация становятся стратегическими ресурсами и агентом трансформации постиндустриального общества». В результате набирают обороты процессы информационной интервенции – захвата культурного, экономического, образовательного и других пространств одного общества другими, внешними потоками информации, что трактуется как информационная война. «Вместе со становлением информационных сообществ, – пишет по этому поводу А. И. Субетто, – появился феномен информационных войн, направленных на разрушение социогенетических механизмов развития отдельных обществ и цивилизаций, в том числе национально-этических архетипов, сложившихся систем ценностей и нравственности …».

Вместе с этим появилось информационное оружие, используемое не только против структур управления государством, экономикой и вооружёнными силами, но и против общества, группы, отдельной личности. Информационное оружие изменило не только методы ведения военных действий, но и само понятие войны. Стираются грани между военным и мирным временем, ещё более сращиваются военные и мирные технологии. Считается, что появилась возможность выиграть войну без проникновения на территорию противника. Это мнение, безусловно, в «чистом» виде не соответствует действительности, так как без дополняющего информационные атаки финансового, торгово-экономического и технологического проникновения на территорию противника как современной альтернативы «солдатского сапога», победа в войне, а не в отдельно взятом сражении, немыслима.

Очевидно, что инструментом информационной, политической и культурной экспансии технологически развитых стран по отношению к странам неразвитым или развивающимся становятся глобальные информационные сети. Такое положение явилось следствием того факта, что информация превратилась в массовый продукт, стала экономической категорией. Она продаётся и покупается. И в силу различия экономических и финансовых потенций социальных субъектов информационное общество породило новый вид неравенства – информационное.

Информационное неравенство – это характеристика состояния и уровня развития различных стран, регионов, сообществ и социальных слоёв (групп) по критерию их вовлеченности в движение к глобальному информационному обществу. Оно оценивается, во-первых, степенью доступа к современным информационно-коммуникационным технологиям, информационным системам и сетям и, во-вторых, степенью готовности населения к жизни и работе в информационном обществе. Речь идёт о своеобразной грани культуры – информационной (правильнее было бы – информатизационной).

Информационное неравенство достаточно легко конвертируется в неравенство экономическое и наоборот. В результате богатые – богатеют, бедные – становятся ещё беднее, пополняя ряды «новых маргиналов», «стран изгоев». Именно искусственная поддержка отставания в информационной сфере ряда стран Африки, Азии (частично – и стран СНГ) сегодня является одним из важных направлений информационной стратегии развитых стран Запада[121].

Ещё одна опасность, порожденная информационализмом, – рост статуса и власти владельцев информации. Опасность здесь кроется в том, что возникают новые возможности для шантажа и угроз, в том числе путем фальсификации данных, особенно в периоды острого политического противоборства. Вот что по этому поводу пишет С. А. Дятлов: «В современном обществе общественная значимость всё больше и больше отождествляется с информационной значимостью. Общественная власть и мощь перемещаются не к владельцам денег, а к владельцам информации, которые знают, как наиболее рационально использовать деньги и богатство во всё более и более усложняющейся современной экономике».

Это обстоятельство побуждает отдельных личностей, группы, организации к получению как можно большего объёма информации, в том числе и не всегда законными методами и средствами. Как заметил Э. Тоффлер, «методы производства Третьей волны усиливают стремление корпораций получать больше информации как исходного материала. Поэтому фирмы сосут данные, подобно гигантскому вакуумному насосу, обрабатывают их и распространяют

121 Атаманов ...

всё более и более сложными путями»[122]. Данный вывод справедлив не только в отношении корпораций, но и государств и государственных институтов. Такая значимость информации вызывает борьбу за контроль над данными. Тоффлер совершенно прав, утверждая, что для этой новой эры информационные потрясения столь же серьёзны, как и экология, и социальные потрясения.

Действительность оказалась не столь радужной, как это представлялось на заре информационализма. Компьютеризация породила и качественно новые явления, например, интеллектуальную эрозию; дебилизацию, вызываемую компьютерными играми; потерю грамотности; сужение кругозора; псевдообразование, не требующее работы мысли учащегося; переход от языка текстов к языку рисунков (обратное тому, что было в классической школе), то есть уход от мышления к рефлекторным реакциям[123].

Поистине впечатляющее достижение современных информационных технологий – Интернет. <…> Всё больше текстов переводится в электронный вид. Электронные библиотеки хранят огромное количество информации, бесценной не только для отдалённых, но и для наших ближайших потомков. В то же время информационные технологии оказались несостоятельными при решении несложной, на первый взгляд, задачи: найти сведения по запросу, составленному даже не в произвольной, а в строго формализованной форме. Подтверждается предположение, что достигаемый благодаря технологии порядок порождает больше хаоса, чем она сама в состоянии переварить. Кроме того, выяснилось, что колоссальный объём данных (сведений, а не знаний) начисто лишает пользователей воображения, то есть умения распорядиться этими данными. <…> В результате в колоссальных объемах увеличиваются не знания, а горы мусора из мозаики уже давно известных истин, гипотез, мифов, фантазий и т. п. и т. д. <…> Увеличивается не только объём, но и скорость производства социальной информации при сохранении информационной ёмкости ключевого носителя информации, по Дриккеру[124], – «транспортной РНК, которая ответственна за воспроизводство сложной «белковой» структуры/культуры», – человека.

Нас поджидает ещё одна угроза – возможность потери значительной части культурного наследия в результате отчуждения индивида от культуры, опосредованного новыми информационными технологиями.

Как мы уже отмечали ранее «ускорение темпов изменения (производства новой) информации, кроме того, ведёт к накоплению избыточной информации и «закупориванию» информационных каналов, вследствие их недостаточной пропускной способности, что, в свою очередь, приводит к запазды-

---

122 Тоффлер Э. – Третья волна. (пер. с англ.). ООО «Издательство АСТ». М., 2002, 776 с. (с. 385)

123 Атаманов …

124 Дриккер А. С. – Эволюционный прогноз: пульсация народонаселения; А. С. Дриккер – Синергетическая парадигма. Нелинейное мышление в науке и искусстве. М., 2004, с. с. 429-446

ванию в принятии решений подсистемами управления вследствие получения ими устаревшей или ложной информации. Информационная перегрузка является следствием недостаточного развития средств обработки информации, нехватки специалистов, компьютерной техники, неразвитости рынка информационных услуг, средств информационного поиска и др. Реальностью стала информационная и, её более известная форма, – компьютерная преступность. Информационные технологии используются повсеместно во внутриполитической борьбе[125].

«Во многом в связи с данным обстоятельством в современном обществе пересматривается и роль государства, которое не только должно определять общие стратегии, но также формулировать определённые «правила игры», обеспечивая координацию подсистем, согласование интересов, препятствуя, тем самым, порождению глубоких социально-экономических, культурных и других деформаций, снижая планку внутренней напряжённости в обществе и выводя его из тотальной зависимости от внешних субъектов информационного воздействия. Таким образом актуализируется проблема безопасности в информационном (информациональном) обществе.

В полной мере это относится и к России, которая «находится в движении» к информационному обществу, и ей свойственны все недостатки, присущие другим странам. В то же время Россию отличает значительно более высокий уровень информационного неравенства при движении от центра к периферии, широкое применение политических PR-технологий, «чёрных» информационных технологий и т. п. Несмотря на это в стране до сих пор отсутствует официальная программа построения информационного общества. Нет и взаимоувязанной и жизнеспособной системы нормативных документов, регламентирующих вопросы национальной (в том числе информационной) безопасности, начиная от концептуального уровня и заканчивая их юридическим обеспечением.

В результате информационные процессы в современном российском социуме развиваются в направлении, опасном для сохранения его целостности. Не только подорвано внутреннее единство общества, но и размыто его самосознание, понимание, как прошлого, так и будущего, миссии России в современном мире. Следовательно, восстановление эффективного регулирования и саморегулирования российского общества должно стать важнейшей стратегической целью и задачей, что требует преодоления информационной «нестабильности» и создания условий укрепления в стране и в сознании населения позитивной государственной идентичности. Но решение такой задачи тесно связано с поисками соответствующих программ и технологий,

---

125 Атаманов ...

способных блокировать негативное воздействие информации, приостановить «привыкание» населения к внешним информационным стереотипам и идеологическим символам, раскрывающим компоненты и принципы чуждого образа жизни и мысли.

Информационная безопасность здесь выступает как результат преодоления условий, порождающих соответствующую опасность, и закрепляется в формах, которые позволяют социальным субъектам сохранить способности выработки релевантных объективным потребностям целей и возможности их достижения. Технология же обеспечения информационной безопасности России в современных условиях может быть построена исключительно на основании самореференции и аутопойесиса с использованием механизмов гражданского общества. Это требует восстановления социально ответственной позиции наиболее разумной и образованной части населения – интеллигенции. Учёные-обществоведы, писатели, журналисты, деятели культуры, политики, вообще патриотически-настроенные личности, сохранившие чувство позитивной национальной идентичности и устойчивость к деструктивному информационному воздействию и потому способные быть «центром кристаллизации», на базе которого можно было бы создать своеобразный «проект» новой социальной целостности, должны консолидироваться и значительно повысить свою общественную активность. Получается, что только если активная, социально ориентированная и ответственная интеллигенция сможет в ближайшем будущем занять достойное место в пространстве социального бытия российского общества, то только тогда можно будет обеспечить выживание и развитие России в нужном направлении в условиях современного – информационального – глобального сообщества»[126].

В качестве одного из конкретных примеров рассмотрения этого комплекса проблем приведём работу профессора кафедры уголовного права Волгоградского юридического института МВД РФ, доктора юридических наук, проф. С. Л. Сибирякова[127].

«Национальная безопасность любого государства напрямую связана с уровнем девиантных проявлений его граждан, в первую очередь, в подростково-молодёжной среде.

К сожалению, следует констатировать, что последние годы (в частности, с 1993 по 1999 гг.) в России почти повсеместно отмечены ускоренным приростом девиантных (девиантный – имеющий отклонения от маршрута,

---

126 Атаманов Г. А. Информационные технологии: плюсы и минусы внедрения, Известия нижневолжского агроуниверситетского комплекса. – 2006. – № 4.

127 Предупреждение девиантного поведения молодёжи в системе обеспечения национальной безопасности России. Труды МАН ПНБ. М., том 2, вып. 1

от социальной нормы и т. п.) проявлений её молодых граждан, в том числе таких их наиболее опасных форм как: преступления и иные правонарушения, наркомания и токсикомания, пьянство и алкоголизм, проституция (как вершина айсберга импортированной «сексуальной революции», противоречащей вековым традициям табу на публичное обсуждение и экспозиции сексуальных отношений) и тому подобное.

Одновременно в условиях непрекращающегося кризиса во всех без исключения сферах жизнедеятельности нашего общества и государства завершается разрушение остатков элементов некогда существующей достаточно прочной, а главное отработанной системы национальной безопасности страны, важной составляющей которой был комплекс мероприятий антидевиантной направленности (в рамках, прежде всего, общесоциального и специально-криминологического предупреждения правонарушений и преступности).

В ряду последствий происходящих негативных процессов следует, на наш взгляд, отметить резкое падение уровня образования и культуры, а главное … нравственности среди всех слоёв населения, особенно среди подростков и молодёжи. <…> … резко изменились ценностные ориентации и приоритеты подростков (в первую очередь) и «молодых взрослых», то есть лиц 18-23 лет (по Игошеву К. Е.), не говоря уже об их «мировоззренческих» позициях, что, в совокупности не могло не привести к росту девиантных проявлений.

В частности главное, по мнению большинства опрошенных (70%) несовершеннолетних в городах Москва и Волгоград, – для чего человеку стоит действовать, – это ради устройства собственной спокойной жизни, включая возможность «красиво отдохнуть» (40%).

Политические цели (и проблемы) интересны (в той или иной мере) лишь для 6% юных респондентов.

Работает человек, в основном, для того, чтобы заработать на жизнь (57%) и немного – для карьеры (26%) опрошенных. При этом о пользе труда для других, престиже, «великих», а тем более – благородных целях вспоминалось крайне редко, да и то лишь в сфере экологии.

Учиться[128], – по мнению респондентов, необходимо, чтобы получить высокооплачиваемую работу (42%) и войти в круг преуспевающих людей (41%).

Самые популярные профессии среди подростков: юрист, бухгалтер, банкир, экономист, журналист, переводчик, менеджер, работник в области искусства и компьютерной техники; в г. Москве (респонденты) ещё хотели бы стать депутатами и членами правительства. (Опрос проводился одновременно в обоих городах в октябре-ноябре 1998 года среди учащихся 10-11 классов и в ПТУ в Москве – силами работников сектора В. В. Панкратова

128 а скорее получать диплом о каком-нибудь образовании.

НИИ Генеральной Прокуратуры РФ). Однако 30% опрошенных опасается, что им не хватит денег на дальнейшее обучение.

Отрадно, что на вербальном, по крайней мере, уровне для 38% москвичей и 20% волгоградцев большой ценностью по-прежнему является семья: «семья – это – то самое важное, ради чего и следует жить».

Значительная часть опрошенных любимым время препровождением считает общение с друзьями (47%), выпивку и слушание записей в кругу своей компании, танцы, тусовки в целом (42%), включая посещение концертов любимых эстрадных исполнителей и т. п.

Ни один из опрошенных не посвящает себя серьёзному занятию религией (христианство, ислам, буддизм) и только 5% интересуются какими-либо другими духовными явлениями (йога, кришнаиты, экстрасенсы и т. д.). Отметим в этой связи, что более ранние исследования, проводившиеся среди «молодых взрослых» (например, А. В. Никонов – Волгоград), показали, что «потусторонним», – НЛО, экстрасенсами и т. д. – интересовалось не менее 37% опрошенных.

<…> Следующее исследование, проведенное нами в январе 1999 г. («о месте и роли СМИ в системе предупреждения девиантного поведения молодёжи»), показало, что свою негативную, большей частью, роль в повышении уровня девиантных проявлений среди подростков играют «mass media»/СМИ, особенно центральные. Их смотрит (в первую очередь), читает и слушает 50-60% подростков, которых можно отнести к «неустойчивому» типу. Определённая часть представителей данного типа (10-15%), скорее всего, склонны к переходу в число «активных» девиантов.

Отсюда следует, что именно условно «неустойчивый» тип подростков и должен стать основным объектом раннего предупреждения и особо пристального внимания, как общества в целом, так и, особенно, соответствующих заинтересованных субъектов, в том числе и с точки зрения обеспечения прочного фундамента национальной безопасности государства.

На основании изложенного и результатов предыдущих изысканий в данной области можно сделать следующие выводы:

1. Как «уровень общего развития», так и, особенно, «уровень девиантности» среди значительной части подростков (35-40%) и «молодых взрослых» (25-30%) предельно близок к той «критической» черте, за которой может последовать необратимое (или, во всяком случае, трудно обратимое) нарушение своего рода «баланса здоровых и нездоровых» сил в обществе и, как следствие, – возникновение обширной зоны информационной уязвимости как реальной угрозы целостности общества и национальной безопасности страны.
2. Как известно, «чтобы получилась леди, необходимо начинать с бабушки», то есть на практике это означает 2-3 поколения,

как минимум; но при условии, что мы начинаем активно работать в нужном направлении уже с первым из них. Однако ни этого, ни даже соответствующих тенденций пока не отмечается ни в одном регионе страны.

3. Более половины «молодых взрослых» и не менее 2/3 подростков живут (точнее – «вынуждены» жить) «одним днём». Это означает, что большая часть молодого поколения, по сути, лишена не только достойного будущего, но и более-менее удовлетворительного настоящего – крайне негативная во всех отношениях и трудно устранимая тенденция.
4. Увеличивается разрыв между поколениями, причём, не только в традиционной уже форме (т. е. конфликт «отцов и детей»), но и между, например, подростками 14-17 лет и 20-23-х летними «молодыми взрослыми», что также неблагоприятно сказывается на общей ситуации в общественной жизни государства.
5. Возрастают масштабы и влияние уже сложившихся элементов «аномии», «социальной дезорганизации», «дифференцированной ассоциации» и других негативных тенденций, явлений и процессов.

В соответствии с основными выводами предлагается:

1. На федеральном уровне в рамках разрабатываемых концепций (системы) национальной безопасности предусмотреть, например, подсистему (или её элементы) предупреждения девиантных проявлений в подростково-молодёжной среде, включая её практическую реализацию, хотя бы поэтапную, например, в тех регионах, где имеются необходимые условия, ресурсы, силы и средства[129].

2. На региональном уровне, в том числе, не дожидаясь действий на федеральном уровне, предлагается начать реализацию уже разработанных, а главное – апробированных на практике, схем организации, например, «системы непрерывного этико-правового воспитания учащихся» (1-11 классов) и предупреждения их девиантного поведения.

3. Продолжить (по возможности в расширенном варианте) отслеживание рассматриваемой проблемы на всех уровнях с тем, чтобы своевременно уточнять социальные действия по преодолению негативных тенденций.

Эта работа является примером общего понимания социального неблагополучия в подростковой и молодёжной среде, что уже привело и ведёт к усилению социальной уязвимости. При этом проф. Сибиряков совершенно правильно утверждает, что развивающаяся ситуация несёт угрозу национальной безопасности России. Он также даёт апробированные рекомендации по преодолению этого тренда.

---

129 Сибиряков С. Л. – Предупреждение девиантного поведения молодёжи (методологические и прикладные проблемы»). Волгоград, 1998

Эти и другие элементы уязвимости представляют собой слабые места, позволяющие потенциальному противнику преодолевать кибер-защиту, как в ходе информационной войны, так и для осуществления диверсий, шпионажа, саботажа и провокаций в процессе информационного противоборства для ослабления возможностей защиты от информационной агрессии.

В целях ухода от ответственности все активные участники информационного противоборства (США, НАТО, Китай, Россия, Индия, Иран) формально или неформально привлекают отечественных хакеров к операциям в киберпространстве, высвечивая для работы каждой хакерской группы выявленные спецслужбами целевые элементы уязвимости.

Так, хакеры из группы GhostShell/Ячейка Призрак объявили кибер-войну России, говорится в заявлении, опубликованном ими в 3 ноября 2012 года.

Они назвали свои действия ProjectBlackStar/Проект Чёрная Звезда, их цель – публикация различной секретной информации[130].

В рамках своего «проекта» хакеры намерены опубликовать в Интернете различные документы – «счета, пароли, адреса электронной почты и другие данные правительственных, образовательных, политических организаций, правоохранительных органов, телекоммуникационных систем, научно-исследовательских институтов, медицинских учреждений и крупных корпораций». Сами по себе публикации таких документов едва ли вызовут значительный интерес интернет аудитории, но, безусловно, способны спровоцировать активность криминальных сообществ предоставлением им нелегально добытой дополнительной информации. Следует учитывать, что нелегальная добыча информации является уголовным преступлением, и её передача в публичный домен должна и, надо полагать, будет преследоваться по закону.

По мнению авторов заявления, граждане России «вынуждены жить жизнью, изолированной от остального мира, и эта жизнь навязана им политиками и лидерами их страны». Как утверждает д-р Р. Ли (США) «90% американцев не знают и не хотят знать ничего об «остальном мире». Это, безусловно, можно рассматривать как результат информационной войны власти с населением.

В GhostShell заявляют, что «располагают большим количеством российских документов, чем ФСБ, и готовы это доказать». Для представления этих доказательств лучшим адресом является приёмная ФСБ РФ, хотя бы для сравнения компетентности.

GhostShell ранее опубликовала 120 тысяч документов 100 крупнейших вузов мира, а в рамках проекта HellFire/Адский Огонь сделала доступными 1 миллион файлов, среди которых были закрытые данные ЦРУ и Уолл-стрит, сообщает «Интерфакс».

---

130 Хакерская группа GhostShell объявила кибервойну России. Интернет. 3.11.2012, © Flickr.com/gutter/cc-by-sa 3.0

Китайская народная республика.

Термин «информационная война» уже давно в лексиконе военных специалистов Китая. Недалек тот час, когда им будет сформирована единая доктрина информационной войны. Если революцию в военном деле определять как значимое изменение в технологии, предоставляющее преимущество в военном обучении, организации, стратегии и тактике военных действий, то, Китай, из всех стран, возможно сегодня проходит через революцию в киберпространстве.

Следует указать на то, что Япония и Китай проводят активную работу в области информационной войны. При этом Россия, в геополитическом плане, рассматривается и Пекином и Токио в качестве потенциального соперника. Если учесть с какой скоростью наши восточные соседи осваивают этот относительно новый вид противоборства, можно предположить, что российские Сибирь и Дальний Восток вскоре станут основными направлениями проведения информационных операций. Так руководством Китайской Народной Республики активно продвигается идеи создания на Дальнем Востоке региональной телекоммуникационной системы. КНР готово выделить на эти цели 150 миллионов долларов. В ВС Китая даже организован отдельный род войск, который предназначается для решения самых разнообразных задач – от радиоэлектронного противодействия до совершения психологических операций. Для реализации этих целей действуют информационный корпус, подразделения защиты информации и бригады атак компьютерных сетей. Китайская концепция информационной войны включает уникальные китайские представления о войне вообще, основанные на современной концепции «народной войны», 36 стратагем великого Сунь Цзы[131], а также местных представлениях о том, как воевать на стратегическом, оперативном и тактическом уровне. Многое из его подхода имеет отношение к акценту на обмане, войне знаний и поиске асимметричных преимуществ над противником. Информационная война определена как «переход от механизированной войны индустриального возраста к… войне решений и стиля управления, войне за знания и войне интеллекта».

Китай развивает концепцию Сетевых сил (воинские подразделения численностью до батальона), которые состояли бы из высококлассных компьютерных экспертов, обученных во множестве государственных университетов, академий и учебных центров. Основной акцент делается на привлечение активной молодёжи.

На сегодняшний момент было проведено уже несколько крупномасштабных учений этих сил по отработке концепции информационной войны.

---

131 Сунь Цзы «Искусство войны»

Любопытна оценка динамики развития противостояния Китай – США, данная ведущим американским специалистом в области национальной безопасности, ядерных и информационных вооружений Р. Кларком[132] и приводимая нами с минимумом комментариев.

«Армия Саддама Хусейна была четвертой по численности в мире. Его оружие, спроектированное и сделанное в Советском Союзе (или Китае), было уничтожено ещё до того, как его успели применить. Боевые действия на земле продолжались сто часов; за ними последовало 38 дней ударов с воздуха.

Среди тех, кто следил за ходом войны по телевизору, было и китайское военное руководство. Бывший директор Национальной разведки адмирал Майк Макконел считает, что «китайцы были немало шокированы, наблюдая ход «Бури в пустыне». Позднее они, возможно, прочитали «Первую информационную войну» и другие источники, что позволило им осознать, как сильно они отстали. Вскоре они назвали войну в Персидском заливе жонгда Ыапде – «великая трансформация». На протяжении нескольких лет китайцы открыто говорили о том, чему их научила «Буря в пустыне». Они отмечали, что раньше, в случае войны, надеялись одержать победу над Соединенными Штатами благодаря численному превосходству. Теперь они пришли к выводу, что данная стратегия неэффективна. Китайцы начали сокращать войска и инвестировать в новые технологии.

Одной из таких технологий стала wangluohua – «сетевизация» – освоение нового, компьютерного поля боя. Их публичные заявления поразительно напоминали речи генералов ВВС США. Один китайский эксперт объяснял в военной газете, что «вражеская страна может получить парализующий удар через Интернет». Другой, полковник, возможно, размышляя о США и Китае, писал, что «превосходящие силы, которые потеряют информационное превосходство, будут повержены, а меньшие, захватив информационное превосходство, смогут одержать победу».

Генерал-майор Ванг Пуфенг, возглавляющий кафедру оперативного искусства в одном из военных училищ, открыто заявлял о том, что цель страны – zhixinxiquan – «информационное превосходство».

Генерал-майор Дэй Квингмин отметил, что такое превосходство может быть достигнуто только с помощью упреждающей кибератаки.

Эти эксперты в области стратегии создали «интегральную сеть электронной войны», напоминающую повальное увлечение сетевыми боевыми действиями в Пентагоне. К концу 1990-х китайские стратеги сошлись на мысли, что кибероружие позволит стране компенсировать нехватку качественного вооружения, если сравнивать арсенал Китая с Соединёнными Штатами.

---

132 Р. Кларк, Р. Нейк «Третья мировая война. Какой она будет?, С-П., 2011 г

Адмирал Макконел отметил: «Из опыта «Бури в пустыне» китайцы сделали вывод, что они должны бросить вызов главенству Америки на поле боя, для чего им нужно создать технику, способную вывести из игры наши спутники и обеспечить вторжение в наше киберпространство. Китайцы считают, что ради защиты Китая в этом новом мире им нужно лишить Соединённые Штаты преимущества в случае войны».

В китайских формулировках то и дело встречается выражение «асимметричная война». Большая часть того, что нам известно о китайской доктрине асимметричной войны, сформулировано в небольшом томике, название которого переводится как «Неограниченная война».

Эта книга, написанная высокопоставленными чинами китайской армии, вышла в свет в 1999 году. В ней изложен план того, как более слабые страны могут изменить существующую расстановку сил и добиться преимущества, используя оружие и приёмы, которые выходят за пределы традиционного военного арсенала. Издатели английского перевода этой книги назвали её «генеральным планом уничтожения Америки», как гласит добавленный подзаголовок. А на обложке, на случай, если читатель не уловит основную идею, изображен Всемирный торговый центр, объятый пламенем. На обороте обложки приведены слова какого-то фанатика из правого крыла о том, что книга «доказывает причастность Китая к событиям 11 сентября».

Несмотря на некоторую «правизну» американского издания книги, она является одним из лучших источников, которые помогают нам понять отношение китайских вооружённых сил к кибервойне.

Китайский полководец Сунь Цзы** и его книга **«Искусство войны».

В книге пропагандируется тактика shashoujian – «жезл ассасина» – использование слабых мест в традиционных (кажущихся) преимуществах противника. Цель стратегии – «вести бой, исходя из имеющегося оружия» и «создавать необходимое для боя оружие». Здесь предлагается игнорировать принятые правила ведения войны, включая запрет использовать в качестве цели гражданское население, манипуляцию зарубежными средствами массовой информации, наркотики, контроль рынков и т. д. В книге, написанной десять лет назад, делается большой акцент на кибервойне.

Возможность использования кибероружия против превосходящих сил не означает, что Китай намеревается вести в войну с Соединёнными Штатами, просто военные понимают, что война возможна и поэтому нужен план.

Китайское руководство использует выражение «мирный подъём», говоря о запланированном превращении Китая в одну (но не единственную) из мировых сверхдержав. И всё же адмирал Майк Макконел считает, что «китайцы используют наши системы по причине их информационного преимущества, они ищут тактико-технические данные систем вооружения и изучают научные исследования в области физики».

Стремительный экономический рост Китая и зависимость от мировых ресурсов, так же как и разногласия с соседями (Тайванем, Вьетнамом), вероятно, наводят военных на мысль, что они должны быть готовы к возможному конфликту. И они готовятся.

Глава вооружённых сил США адмирал Майк Маллен (председатель Объединенного комитета начальников штабов) считает, что подготовка нацелена прямо на Соединённые Штаты: « [Китай] развивает мощности, связанные с ведением боя на море и в воздухе, во многом ориентированные на войну с нами», – заявил он в своей речи на собрании Морской лиги в мае 2009 года. «Кажется, они больше всего сосредоточены на военно-морских силах США и наших базах, расположенных в той части планеты», – продолжил он.

В ежегодном отчёте министра обороны за 2009 год, озаглавленном «Военная мощь Китайской Народной Республики», эти заявления поддерживаются. «Китайцы разработали РЛС дальнего обнаружения, благодаря которым они могут видеть, что происходит на нашей авиабазе в Гуаме. Они спроектировали противолодочные ракеты, которые приближаются так быстро, что их не в состоянии перехватить ни одна из наших систем обороны. Китай купил у России авианосец «Адмирал Кузнецов», который в настоящее время модернизируется на верфи в Даляне. Скоро китайцы начнут строить собственные авианосцы и откроют специальную программу обучения пилотов. Они установили вдоль побережья более двух тысяч ракет, направленных на Тайвань, и каждый год добавляют ещё сотню. Совсем скоро они разместят ракеты с радиусом действия 8 тысяч километров, что даст им возможность наносить

ядерные удары через океан. Всё это звучит несколько устрашающе, но при ближайшем рассмотрении понятно: одной модернизации недостаточно, чтобы противостоять традиционному перевесу сил США. Военный бюджет Китая уступает американскому в разы, он составляет всего лишь 70 миллиардов долларов, что в восемь раз меньше бюджета Пентагона без учёта расходов на войны в Афганистане и Ираке. Ударная группа американских авианосцев является одной из самых мощных неядерных сил в истории человечества. Она состоит из десятков кораблей, включая ракетоносцы, эсминцы, миноносцы, подводные лодки, транспорты снабжения, и способна преодолевать по 700 морских миль в день, что позволяет попасть по воде в любую точку планеты максимум за две недели. В составе военно-морского флота США имеется 11 боевых групп авианосцев, и сейчас ВМС ожидает три авианосца нового поколения, первый из которых планируется спустить на воду в 2015 году».

По данным Пентагона за 2009 год, Китай не успеет ввести бывший российский авианосец в эксплуатацию раньше 2015-го. Представители разведывательного сообщества США сходятся во мнении, что Китаю нужно ещё, по крайней мере, десять лет, чтобы суметь одержать уверенную победу над таким некрупным противником, как Вьетнам.

Отбросить же от своих берегов силы врагов, уступающих США, Китай сумеет не ранее 2015 года. Если только… Если только Китай не сумеет изменить соотношение сил, ведя кибервойну против американских авианосцев. Китайцы всегда восхищались американскими авианосцами, но их внимание к ним увеличилось в 1996 году, когда президент Билл Клинтон послал две боевые группы авианосцев на защиту Тайваня во время одного обмена особенно жёсткими заявлениями между Пекином и Тайбэем.

Китайские военные в соответствии с новой стратегией предложили «виртуальный план» уничтожения группы авианосцев в документе «Тактический канал передачи данных в информационной войне». Материалы, которые легли в основу этого несекретного документа, составленного двумя офицерами китайских военно-воздушных сил, были доступны через Интернет, а его целью стало показать, как с помощью относительно низкотехнологичных методов можно заблокировать или разрушить информационные системы, на которые полагаются вооружённые силы США. Такого рода тактические приёмы можно найти в стратегии «Неограниченная война».

Основной план: украсть технологию противника, найти в ней изъяны, воспользоваться ими и разработать собственную версию программы. Однако не ускользнула от китайских военных стратегов и способность кибероружия совершенно исчезать с поля боя. В случае войны Китай готов нанести удар по тылу врага, но не обычным оружием, а асимметрично, посредством кибератаки.

Даже значительная модернизация оборудования не позволит Китаю догнать США ещё много десятилетий. Однако если Китай будет использовать асимметричную тактику, включая кибервойну, будьте уверены: новые современные вооружённые силы Китая окажутся достаточно совершенными для того, чтобы бросить вызов американским войскам с помощью кибератаки.

Недавно Пентагон напугала статья в Orbis под названием «Как Соединённые Штаты проиграют морскую войну 2015 года». В ней Джеймс Краска ярко описал, как в недалеком будущем Китай сумеет бросить вызов Соединённым Штатам и победить.

Восточные хакеры.

Судя по нашим сведениям о кибермощностях Китая и по шпионским кампаниям, проведенным этой страной, Китай использует двойной подход. С конца 1990-х Китай систематически реализовывал всё то, что должна делать страна, способная вести кибернаступление и осознающая, что и сама может оказаться мишенью в кибервойне, а именно:

– создал гражданские группы хакеров;

– занялся масштабным кибершпионажем, в том числе и в области программного обеспечения и аппаратных средств;

– предпринял шаги для защиты собственного киберпространства;

– разместил в инфраструктуре США множество логических бомб.

Одновременно с разработкой киберстратегии Китай воспользовался услугами хакеров, которым близки государственные интересы. По оценкам Американо-китайской комиссии по обзору состояния экономики и безопасности, в Китае работает около 250 групп хакеров, достаточно продвинутых для того, чтобы поставить под угрозу интересы США в киберпространстве.

Мы видели, на что они были способны на заре своего существования, когда Соединённые Штаты проводили кампанию по прекращению массовых убийств в Косово. Американцы имели едва ли не самое совершенное интеллектуальное оружие и использовали его, чтобы уничтожить военный аппарат советской эпохи, не потеряв ни одного американского солдата (один боевой самолет всё же разбился из-за механической неисправности – Кларк врёт по профессиональным причинам – на самом деле потери американских ВВС за время Косовского кризиса составили более 50 летательных аппаратов, включая 2 стелтс адаптированных самолёта, не говоря уже о заметных потерях в другой технике и в живой силе).

К сожалению, интеллектуальным оружием нельзя компенсировать отсутствие интеллекта. Шесть бомб, сброшенных с американских самоле-

тов, ударили точно по цели, намеченной в штабе ЦРУ. Этой целью должно было стать Федеральное управление поставок и закупок – координационный орган сербских вооружённых сил. Однако же координаты были указаны неверно, и вместо управления бомбы попали в китайское посольство, располагавшееся в трёхстах метрах от предполагаемой цели.

Китайцы протестовали у консульств и посольств Соединённых Штатов, делали заявления в ООН и другие организации и требовали компенсации для пострадавших и их семей. После бомбардировки посольства сайты правительства США и НАТО подверглись атакам, которые нарушили нормальный процесс работы. На электронную почту государственных служащих обрушились тонны писем с протестами.

Некоторые сайты НАТО вышли из строя, другие работали с перебоями. Атака не нанесла большого вреда американским вооружённым силам или деятельности правительства. Она не слишком превышала масштабы сегодняшнего «хактивизма» – довольно спокойной формы онлайнового протеста. Однако эта атака стала первым опытом Китая в использовании киберпространства для выражения протеста.

Китайские «хактивисты» повторили то же самое в 2001 году, когда американский самолёт-шпион якобы проник в воздушное пространство Китая и был вынужден приземлиться. Обычные китайские хакеры проводили довольно примитивные кибератаки, но не бездействовала и китайская промышленная разведка. Китайское правительство взяло в оборот два кита американской компьютерной индустрии, Microsoft и Cisco.

Угрожая прекратить закупки продукции Microsoft, Пекин убедил Билла Гейтса предоставить Китаю копию закрытого кода операционной системы. Руководство Microsoft отказалось предоставить этот код своим крупнейшим коммерческим потребителям в Америке.

Затем Китай получил информацию о сетевом маршрутизаторе Cisco, обеспечивающем работу практически всех сетей Соединённых Штатов и большинства интернет-серверов. Когда-то у Cisco был завод по производству маршрутизаторов в Китае. Потом китайские компании начали продавать дешёвые копии маршрутизаторов. Как утверждают, в число покупателей вошёл даже Пентагон и ряд других федеральных правительственных организаций.

Такие маршрутизаторы стали появляться на рынке в 2004 году. Через три года ФБР и Министерство юстиции США обвинили братьев, владевших компанией Syren Technology, в продаже ворованных маршрутизаторов целому ряду клиентов, включая корпус морской пехоты, военно-воздушные силы и многочисленных военных подрядчиков. В пятидесятистраничном отчете, составленном ФБР, говорится, что эти маршрутизаторы могут использо-

ваться иностранными разведслужбами для разрушения сетей и «ослабления шифровальных систем».

Между тем, другая китайская компания, Huawei, продавала точно такие же маршрутизаторы по всей Европе и Азии. Они отличались только тем, что на них вместо торгового знака Cisco стоял Huawei. Благодаря знаниям недостатков продукции Microsoft и Cisco, китайские хакеры способны остановить деятельность большинства сетей.

Но разве сами китайцы не столь же уязвимы? Ответ на этот вопрос был бы утвердительным, если бы они использовали те же продукты Microsoft и Cisco, что и мы. Но по соглашению с Microsoft китайцы модифицировали версию, которая продается в их стране, дополнив её собственным программным кодом. Они даже разработали собственную операционную систему Kylin, построенную на базе Free BSD.

Именно Kylin использует Народно-освободительная армия Китая. Есть сведения, что Китай разработал собственный микропроцессор для использования в серверах и маршрутизаторах Huawei. Китайское правительство пытается установить программное обеспечение Green Dam Youth Escort на всех компьютерах под предлогом борьбы с распространением детской порнографии и других запрещённых материалов. Если это программное обеспечение заработает, и его установят на всех системах, Green Dam сможет отслеживать и вредоносное программное обеспечение, размещаемое вражескими государствами.

Помимо Green Dam существует ещё одна система, которую американские остряки называют великой китайской стеной, – Great Firewall. Эта управляемая правительством система на самом деле брандмауэром не является, она сканирует трафик в поисках антиправительственных материалов, таких как Всеобщая декларация прав человека. Эта система перехватывает доменное имя и перенаправляет вас на одобренный китайским правительством клон реального сайта, если вы, находясь в Китае, попытаетесь зайти, к примеру, на веб-страницу Христианской евангелической организации.

Она также способна отключить китайские сети от всего остального Интернета, что очень удобно, если вы предполагаете, что США собираются начать против вас кибератаку.

Джеймс Малвелон, один из ведущих американских экспертов по китайскому кибераресеналу, говорит, что, взятые вместе, Green Dam, Great Firewall и другие системы доказывают «существенные инвестиции китайских властей в блокировку, фильтрацию и мониторинг» собственного кибепространства.

В 2003 году Китай объявил о создании собственных кибервойск. На военно-морской базе острова Хайнань базируются третий технический отдел Народно-освободительной армии Китая и Лингшуйская база радио-

электронной разведки. По данным Пентагона, эти части отвечают за нападение и защиту в киберпространстве, кроме того, ими разработано невиданное ранее кибероружие, которое не остановит никакая оборона. В одной из публикаций китайцы перечислили десять вариантов использования такого оружия:

– размещение информационных мин;
– руководство информационной разведкой;
– изменение сетевых данных;
– запуск информационных бомб;
– сброс информационного «мусора»;
– распространение пропаганды;
– использование дезинформации;
– создание информационных клонов (именно так!);
– организация информационной обороны;
– создание сетевых станций слежения.

Китай действительно создал две сетевые станции слежения неподалеку от США, на Кубе. С разрешения правительства Кастро китайские военные разместили здесь оборудование для мониторинга американского трафика и коммуникаций Министерства обороны.

Примерно в то время, когда Китай объявил о создании киберчастей, США пережили один из худших на сегодняшний день эпизодов кибершпионажа. «Титановый дождь», как назвали его американцы, привёл к декодированию около 10-20 терабайтов несекретной информации Пентагона. Хакеры сделали своей мишенью военного подрядчика Lockheed Martin и другие военные сайты и – по причинам, которые до сих пор сложно объяснить, – Всемирный банк.

Слабые места сетей Пентагона и других организаций были заранее изучены, а затем использованы для доступа к информации через серверы Южной Кореи и Гонконга. Спецслужбы сумели проследить цепочку от этих промежуточных серверов до конечного сервера, находящегося в китайской провинции Гуандун.

Генерал-майор военно-воздушных сил США открыто приписал эти атаки не китайским «хактивистам», а китайскому правительству. К 2007 году китайское правительство, очевидно, участвовало в целом ряде проникновений в американские и европейские сети, успешно скачивая огромные объемы данных.

Директор британской службы контрразведки MI-5 Джонатан Эванс отправил письма 300 ведущим компаниям Великобритании, извещая о том, что в их сети, возможно, проникли китайские спецслужбы.

Германский коллега Эванса Ханс Ремберг также выдвигал обвинение

китайскому правительству, на этот раз во взломе компьютера Ангелы Меркель, канцлера Германии.

Компьютерный шпионаж коснулся и высокопоставленных американцев, включая и министра обороны Роберта Гейтса.

Китайские шпионы скопировали информацию с ноутбука министра торговли США Карлоса Гутьерреса, когда тот посещал Пекин, а затем пытались использовать её, чтобы получить доступ к компьютерам Министерства торговли.

Заместитель министра обороны Роберт Лоулес, комментируя происшедшее, признал, что у китайцев есть «серьёзные возможности для атаки и повреждения наших компьютерных систем… для выведения из строя наших важнейших систем. Они считают это основным компонентом асимметричной войны».

В 2009 году канадские исследователи обнаружили одну интересную компьютерную программу, которую назвали GhostNet. Она была установлена на 1300 компьютерах в посольствах разных стран по всему миру. Программа позволяла удалённо, без ведома пользователя включать камеру и микрофон компьютера и спокойно передавать изображение и звук на серверы в Китае.

Главной мишенью этой программы стали офисы, связанные с неправительственными организациями, занимающимися тибетскими вопросами. Работа программы, прежде чем была раскрыта, продолжалась на протяжении 22 месяцев.

В том же году из американской разведки в СМИ просочилась информация о том, что китайские хакеры проникли в электрораспределительную сеть США и поставили логические бомбы, с помощью которых можно было вывести эту сеть из строя.

Масштаб китайского хакерства против американской, европейской и японской промышленности и исследовательских организаций беспрецедентен. Экзабайты данных копируются с компьютеров университетов, промышленных лабораторий, государственных предприятий. Всё, от секретных фармацевтических формул, биоинжиниринговых моделей, нанотехнологий до систем вооружения, чертежей повседневных промышленных изделий с помощью Народно-освободительной армии Китая и частных хакерских групп попадает в огромную корпорацию под названием Китай.

Недавно Google заявил об очередном разоблачении весьма изощренной кампании, нацеленной на их интеллектуальную собственность, а также на электронную переписку лидеров китайского диссидентского движения. Хакеры использовали целевой фишинг (мошенничество, направленное на получение банковских конфиденциальных данных), чтобы заставить руководство Google посетить сайты, с которых автоматически загружалось вредоносное ПО, открывавшее хакерам доступ к корневому каталогу.

Если в ходе обычного фишинга сети закидываются повсюду в попытках поймать хоть несколько человек, достаточно доверчивых для того, чтобы клюнуть на электронные письма от нигерийских мошенников, целевой фишинг направлен на конкретного человека. Сначала через Facebook или Linked-in выясняется круг его общения, затем отправляется письмо от человека, которому он доверяет. Если бы вы были главой исследовательского центра Google, вы могли бы получить письмо от коллеги примерно такого содержания: «Привет, Чак! Думаю, эта история тебя заинтересует…» и ссылку на довольно безобидный сайт. Когда человек из Google нажимал на ссылку и попадал на сайт, хакеры, используя уязвимость «нулевого дня» в Internet Explorer, тогда ещё не обнаруженную и не исправленную, спокойно загружали вредоносное ПО (мэлвер) так, что ни одна антивирусная программа, никакие другие средства не позволяли этого заметить.

Мэлвер создавал «чёрный ход» в компьютере таким образом, что хакеры получали доступ к нему и прокладывали путь дальше по корпоративной сети до тех пор, пока не попадали на сервер, содержащий исходный код, – бриллиант в короне компании-разработчика программного обеспечения. Когда исследователи из Google обнаружили в середине декабря происходящее, они проследили хакерский путь, ведущий к серверу на Тайване, где и нашли копии своих собственных данных и данных, по меньшей мере, 20 других компаний, среди которых были Adobe, Dow Chemical и военный подрядчик Northrop Grumman. Отсюда следы вели в континентальный Китай.

Google обратился в ФБР, сделав публичное заявление об имевшем место взломе и планах уйти с китайского рынка к середине января. Некоторые скажут, что война с Китаем маловероятна. Зависимость Китая от американских рынков сбыта, триллионы, инвестированные в казначейские векселя США, означают, что Китай рискует многое потерять.

Один из чиновников Пентагона, пожелавший сохранить анонимность, в этом не уверен. Он отмечает, что экономический кризис в США повлиял и на Китай, в связи с чем миллионы китайских рабочих оказались на улице. Китайское правительство не выразило беспокойства, которое бы возникло в таком случае на Западе, и, очевидно, не собирается ослаблять свою власть над китайским народом.

Урок заключается в том, что Китай способен пережить экономические трудности и может пойти на них, если выгоды от войны покажутся достаточно высокими.

Что это могут быть за выгоды? Часто приводится банальный ответ: возможно, Китай окажется в такой ситуации, что ему придётся помешать Тайваню в подписании декларации независимости.

Однако когда серьёзные аналитики оценивают шансы открытого конфликта с Китаем, они видят, что Китай делает ставки на воды Южно-Китай-

ского моря. Расположенные там острова Спартли не особенно привлекательны для туризма. Да это не совсем и острова. Если собрать вместе все рифы, песчаные отмели и камни Южно-Китайского моря, получится не более пяти квадратных километров суши. Эти пять квадратных километров разбросаны на территории около 400 тысяч квадратных километров.

Не из-за островов враждуют Китай, Вьетнам, Тайвань, Малайзия, Филиппины и Бруней, а из-за того, что находится под ними и вокруг них. В здешних водах сохраняются крупнейшие в мире запасы рыбы, ресурс, который нельзя сбрасывать со счетов, учитывая рост населения стран, претендующих на эти территории.

Кроме того, острова окружает важнейший торговый путь, связывающий Индийский океан со странами Тихоокеанского региона, здесь проходят трубопроводы, по которым течёт значительная часть мировых запасов нефти со Среднего Востока. Кроме того, есть ещё нефть и газ самих Спартли.

Неосвоенные месторождения, согласно оценкам, обладают большими запасами газа, чем Кувейт, который сейчас занимает четвертое место в мире. Местного газа хватит любой из этих стран на десятилетия вперед.

Нефтяные месторождения уже разрабатываются объединёнными усилиями нескольких стран с использованием платформ. Если Китай решит поиграть своими накачанными военными мускулами, вполне вероятно, он попытается вырвать эти острова из рук соседей, <…>

При попытке Китая захватить эти острова США будут вынуждены, пусть и неохотно, отреагировать. США подписали договор о безопасности и с Филиппинами, и с Тайванем, а Chevron посодействовал Вьетнаму в разработке морских месторождений нефти. С другой стороны, США могут воздержаться от выступления против Китая в Тихоокеанском бассейне в том случае, если платой за вмешательство станут значительные повреждения или разрушения в собственной стране.

По словам министра обороны Роберта Гейтса, кибератаки «могут заставить США изменить первоначальные намерения использовать силу, чтобы помочь своим союзникам в Тихом океане».

Достаточно ли этого для того, чтобы удержать США от конфронтации с Китаем? Если вероятность того, что Китай выведет из строя наш наступательный потенциал, недостаточно пугает нас, может быть, нас удержало бы осознание собственной уязвимости перед кибератакой.

Установка логических бомб действительно могла иметь место. Один бывший правительственный чиновник сказал, что, по его убеждению, китайцы хотят, чтобы мы знали, – если мы вмешаемся в конфликт с Тайванем, электрораспределительная сеть США наверняка выйдет из строя.

«Они стремятся заставить Соединённые Штаты отказаться от применения военной силы в сфере их интересов».

Однако проблема в том, что устрашение работает только в том случае, когда другая сторона его слышит. Американские лидеры, возможно, не до конца поняли, что до них пытается донести Пекин.

США не сделали практически ничего, чтобы укрепить слабые места в своей электрораспределительной сети и других гражданских сетях.

Расставим оценки.

Я сфокусировался на Китае потому, что его кибервоенное развитие оказалось, как ни странно, до некоторой степени прозрачным. Представители американской разведки, однако, не считают Китай самой большой угрозой США в кибепространстве.

«Русские определенно лучше, они почти как мы», – сказал один из них. Существует, по-видимому, единодушное мнение: Китай привлекает больше внимания потому, что он – намеренно или нет – оставляет следы и «хлебные крошки», ведущие прямо на площадь Тяньаньмэнь»[133].

В этой же книге Р. Кларк признаёт «… Роб (его соавтор – прим. авторов) и я единогласны в том, что кибервойна – это не война без потерпевших, не новый чистый вид борьбы, который мы должны приветствовать. Но это и не секретное оружие, которое нужно скрывать от света дня и общественности.

Что касается публики, именно гражданское население Соединённых Штатов и частные компании, на которых держится благополучие всей страны, пострадают от этой войны в первую очередь. Может показаться, что у Америки есть преимущество, но кибервойна опаснее для США, чем для других стран. Эта новая война – не игра и не плод нашего воображения, не альтернатива обычной войне. В действительности она способна увеличить вероятность более традиционных военных столкновений с применением взрывчатых веществ, огнестрельного оружия, ракет. Если бы в наших силах было запихнуть джинна обратно в бутылку, мы бы так и поступили, но это невозможно».

Великобритания

Представление об информационной войне, которое господствует в Великобритании сродни взглядам в США. Оно характеризуется спектром действий, защищающих сственные информационные системы и одновременно оказывающих влияние на информационные системы противни-

133 Р. Кларк, Р. Нейк «Третья мировая война. Какой она будет?, С-П., 2011 г

ка. Кроме того, Британия использует юридическую структуру – Regulation of Investigatory Powers Act (RIP), принятую в 2000 году, и основанную на существующих в Англии законах, которая может применяться и к действиям в киберпространстве. Согласно документу, атака на киберсистемы может приравниваться к обычному уголовному преступлению с соответствующим наказанием. Вооружившись этой законодательной инициативой, английское правительство может читать и перехватываать электронную почту и дешифровать по требованию государственных чиновников, личные файлы.

В Великобритании на базе университета ДеМонфорт в городе Лестер запущен проект подготовки программистов для контрразведки MI5 и внешней разведки MI6. В конце октября глава МИД Соединенного Королевства Уильям Хейг объявил о наборе в эту программу молодых людей «поколения Xbox», попросту геймеров[134]. «Юные инноваторы», по словам министра, помогут в грядущие годы обеспечить безопасность островного государства.

Германия

Представление об информационной войне господствующее в Германии в основном совпадает с американскими и английскими взглядами. Но ФРГ, в силу своей немецкой скрупулезности и педантичности, имеет лучшую систематизацию и для достижения национальных целей предусматривает ведение наступательной и оборонительной информационной войны. При этом, определяя угрозы и вероятность возможных ответов разграничиваются: международные организации и СМИ, преступные сообщества (ОПГ, хакеры и т.д.), и индивидуумы (включая религиозных фанатиков и др.), а иностранные государства рассматриваются отдельно от негосударственных объединений (типа политических партий).

Спецслужбы Германии активно контролируют в своих интересах глобальное информационное пространство. Так, недавно стало известно, что в самой крупной компании на рынке телефонии и Internet-коммуникаций Deutsche Telecom в 2005-2006 годах имела место «прослушка» телефонов ряда клиентов[2]. В 2008 году широкую огласку получила шпионская операция германской разведывательной службы, которая установила на компьютер министра торговли Афганистана троянскую программу, и с ее помощью читала приходящую ему электронную почту[3]. В стране создан центр обеспечения безопасности информационной техники (Bundesamt für Sicherheit

134 Британские власти готовят «кибершпионов». Интернет: Кибервойна, поле битвы – Земля. 2012

Источник: gazeta.eot.su

Уильям Джефферсон Хейг

in der Informationstechnik) со штатом около 500 сотрудников и годовым бюджетом более 50 миллионов евро. Открыт испытательный центр по информационным технологиям Министерства обороны.

Но представление Германии об информационной войне может отличаться от американского и английского, как минимум, в двух случаях. Так управление СМИ ФРГ включает как элемент информационной войны. Кроме того, отдельно вводится определение для экономической информационной войны, подобно тому, какое есть у французов. Это является следствием двух причин: Германия оценила потенциал возможного экономического ущерба, который может быть нанесён немецкому бизнесу и экономике; Германия, возможно, испытала существенные экономические потери от Франции в операциях индустриального шпионажа в киберпространстве; также Германия может искать пути смягчения последствий потенциальных вторжений.

Вопросы кибернетической безопасности стоят на особом контроле ведущих стран Североатлантического альянса. Как сообщили немецкие средства массовой информации, немецкая армия уже находится в состоянии полной готовности к ведению кибервойны. Есть и соответствующее подразделение бундесвера, которое расквартировано в Гельсдорфе под Бонном.

Формирование киберкоманды началось в 2006 году, ее костяком стала группа специалистов, изначально созданная для защиты от хакерских атак компьютерных систем бундесвера. В новую структуру набирают в основном программистов, закончивших германские военные институты. По уровню подготовки своих военных программистов Германия уверенно догоняет ведущих в этой области США и Израиль.

Франция

Французы рассматривают концепцию информационной войны, состоящей из двух главных элементов: военной и экономической (или гражданской). Как считает С. Н. Гриняев «Военная концепция предполагает несколько ограниченную роль информационных операций. Их военная концепция видит место информационным действиям, имеющим место в значительной степени в контексте конфликтов малой интенсивности или в миротворческих операциях. В этом контексте, союзники не рассматриваются противниками.

Напротив, экономическая или гражданская концепция включает более широкий диапазон потенциального применения информационных операций.

Французское представление принимает намного более широкое и более глубокое представление для конфликта в экономической сфере. В этом случае французы не видят себя связанными рамками НАТО, ООН или согласием США. Их подход к экономическому конфликту учитывает то, чтобы быть и союзником и противником одновременно. Французы даже имеют экономическую школу для информационной войны.

Франция активно формирует структуры по контролю её граждан в киберпространстве. Есть информация о том, что французы создали собственную версию системы «Эшелон» (по сообщениям американской прессы система направлена на перехват фактически всех частных глобальных коммуникаций). Frenchelon, так некоторые назвали эту систему, по сообщениям используется для контроля и анализа французских коммуникаций, особенно в районе Парижа»[135].

НАТО

По сообщениям существует секретное натовское определение информационной войны, но оно не доступно в открытой печати. На проведенной объединённым штабом НАТО в начале 2000 года конференции по проблемам информационной войны все участники пользовались определениями, разработанными в их странах. Вместе с тем, известно, что натовское определение во многом схоже с аналогичным американским определением с учётом особенностей коллективного пользования, факторов уязвимости и с дополнениями, учитывающими национальные интересы всех стран – членов Альянса.

Североатлантический альянс провёл 12-16 ноября 2012 года ежегодные учения стран-союзниц по управлению кризисными ситуациями (CMX) и по кибербезопасности (Cyber Coalition), объявила штаб-квартира НАТО в Брюсселе.

В учениях приняли участие, как военные, так и гражданский персонал. Они были задействованы в столицах стран НАТО, в штаб-квартире организации и в обоих стратегических командованиях альянса, передает «Интерфакс».

В коммюнике отмечается, что CMX-12 будут внутренними командно-штабными учениями и не предвидится развертывать никакие вооружённые силы для их проведения. Антикризисное учение пройдёт в нынешнем году одновременно с учением по защите от кибератак **Cyber Coalition-12**.

НАТО начинает учения Cyber Coalition, в ходе которых с 13 по 16 ноября участники блока будут отрабатывать взаимодействие в условиях кибервойны. Вообще-то планы виртуальных атак разрабатывают многие государства. Самая большая опасность кроется в том, что последствия кибератак могут

135 Гриняев С.Н. – Информационная война: история, день сегодняшний и перспектива

Источник: ru.ino-ppic.ru

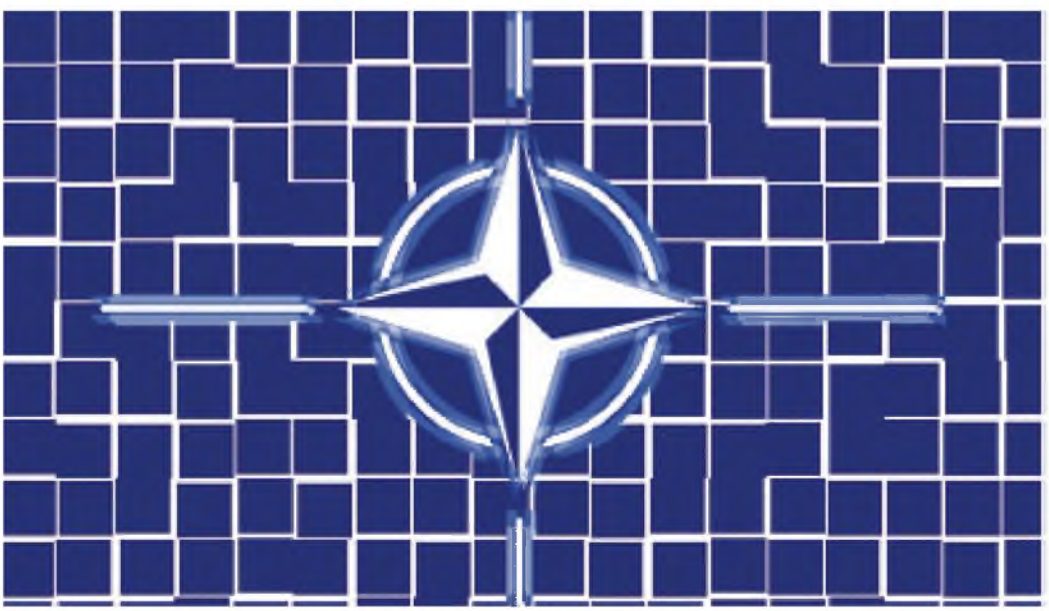
Владимир Валерьевич Евсеев

быть непредсказуемы, а приготовления к виртуальным войнам практически невозможно контролировать.

Согласно сценарию предстоящих военных игр хакерскому нападению со стороны условной африканской страны подвергаются два члена НАТО – Венгрия и Эстония. На один из венгерских городов падает военно-транспортный самолет Альянса, выведенный из строя компьютерным вирусом. Одновременно «враги» проводят кибератаку важнейших объектов инфраструктуры Эстонии. НАТО определяет государственную принадлежность противника и наносит по неприятелю уже комбинированный ответный удар, как в реальном, так и в кибернетическом пространстве.

В данном случае несколько озадачивает выбор жертв кибератаки со стороны коварных «африканцев». Эстония, да и Венгрия тоже находятся под боком у России. Поэтому эксперты склонны предположить, что под некой «африканской» страной-агрессором натовцы всё-таки подразумевают Российскую Федерацию[136]. Тем более, что в кулуарах представители НАТО не скрывают, что считают своими противниками номер 1 в киберпространстве именно Россию, Китай и Иран.

136 Сорокин Никита – Кибервойна, поле битвы – Земля. Интернет. 12.11.2012



НАТО *© Коллаж: «Голос России».*

Но остаётся загадкой, каким образом НАТО вообще сможет ответить на кибератаку, сказал в интервью «Голосу России» директор Центра общественно-политических исследований Владимир Евсеев:

«Если НАТО хочет провести, положим, ответную кибератаку, то, во-первых, для этого нужно время, быстро это организовать просто невозможно. Если же страны НАТО хотят нанести военный удар по тому государству, откуда исходила угроза, то это тоже смешно. Потому что эта атака может быть организована из любого места, в том числе из Соединённых штатов Америки, с серверов. Поэтому с этой точки зрения мне совершенно непонятно, кто кого собирается атаковать. Я думаю, что цель таких учений достаточно провокационная, и, я думаю, это идёт в общем русле ухудшения отношений между Россией и НАТО, ухудшения отношений между Россией и США»[137].

Цель второго учения – проверка технического и эксплуатационного потенциала киберзащиты Североатлантического альянса. Оба учения проводятся на основе вымышленного сценария, предполагающего эскалацию масштабных угроз химического, биологического и радиологического оружия, а также кибератак, направленных против НАТО и национальных инфраструктур стран-союзниц.

Учения будут управляться совместно Международным секретариатом НАТО, Международным военным штабом и двумя стратегическими командованиями альянса – операционным командованием Объединённых вооружённых сил (ОВС) и командованием по трансформации ОВС. Учение CMX пройдет в 18-й раз, начиная с 1992 года.

Наряду с государствами-членами организации в них примут участие партнёры НАТО – Финляндия и Швеция, так как некоторая часть условного сценария разыгрывается в географической близости от них. За учением будут наблюдать представители Международного Комитета Красного Креста (МККК) и Организации по запрещению химического оружия (ОЗХО).

Проведению учений будет содействовать Европейская внешнеполитическая служба. В учениях Cyber Coalition-12 наряду с союзниками по НАТО будут участвовать три государства-партнёра – Австрия, Финляндия и Швеция. В качестве наблюдателей будут присутствовать Австралия, Ирландия и Швейцария.

Среди государств, наиболее успешно осваивающих потенциальные поля сражений в киберпространстве, аналитики помимо США называют Японию, Россию, Китай и даже Северную Корею. В целом, по экспертным оценкам, возможностями для ведения кибервойн сегодня располагают от 20 до 30 стран. Назвать число таких государств более точно затруднительно ввиду специфики и закрытости сферы деятельности, именуемой информатика.

---

137 Евсеев В.В. – Интервью «Голосу России», октябрь 2012

Источник: android-zone.info

Евгений Валентинович Касперский

Самым известным примером эффективной кибератаки на межгосударственном уровне считается применение Соединёнными Штатами вируса Stuxnet, который в Иране поразил систему управления центрифугами, производящими обогащённый уран.

Также знаменит вирус Flame, который неоднократно атаковал компьютерные сети в том же Иране и на всём Ближнем Востоке. Кстати, многие подобные проекты являются результатом совместной разработки израильских и американских специалистов.

Сложная программа Flame была обнаружена «Лабораторией Касперского» в мае 2012 года в ходе исследования, инициированного Международным союзом электросвязи. По его итогам партнёр МСЭ в области кибербезопасности Международное многостороннее партнёрство против кибергроз (ИМПАКТ), передал 144 странам, входящим в его состав, информацию о способах блокирования и удаления данного вредоносного программного обеспечения. «Его сложность, а также сходство с печально известным червём Stuxnet указывали на то, что Flame – это очередная масштабная кибероперация, реализованная при поддержке одного из государств. Вначале считалось, что Flame начал действовать в 2010 году, однако после проведения первого анализа инфраструктуры его командных серверов, охватывающей как минимум 80 известных доменных имён, эта дата сместилась на два года назад», – говорится в «Лаборатории Касперского».

Отметим, что компьютерный вирус Flame занимается кибершпионажем и похищением информации с зараженных машин. Flame активно используется в ряде стран в качестве кибероружия и по сложности и функционалу превосходит все ранее известные виды угроз. Он способен похищать информацию, выводимую на монитор, сведения о системах, файлы, хранящиеся на компьютере, контактные данные пользователей и даже аудиозаписи разговоров.

Генеральный директор «Лаборатории Касперского» Евгений Касперский считает, что мир уже вошёл в эпоху кибер-терроризма. «Мы пережили недавно три шока: терроризм, финансовый кризис и политический кризис. Следующий мировой шок – кибер-терроризм и кибер-атаки. Мы зависим от компьютерных систем, и нет ни одной полностью защищённой страны. А страны, которые развиваются, более всего подвержены атакам», – сказал он[138].

---

138 Иран отбил кибератаку на нефтяные платформы; Индия потратит $ 200 миллионов на борьбу с киберпреступлениями. Интернет

В качестве примера Касперский привёл попытки нападения на ядерные системы Ирана и Саудовской Аравии. «Не все понимают, насколько глубоко этот компьютерный мир проник в нашу жизнь. Физическим миром управляют компьютеры, и, к сожалению, довольно просто подвергнуть атаке эти довольно простые системы. Речь идёт как о физическом разрушении, так и о сознательном производстве с дефектами», – сказал глава «Лаборатории Касперского». Он отметил, что построить такую атаку технически легко. Для этого нужны инженеры, программисты и небольшой бюджет, пишет «Взгляд».

Уже совершенно ясно, что вся сфера информатики в масштабах планеты представляет собой огромное поле боя, сказал в интервью «Голосу России» военный аналитик Александр Гольц:

«Я думаю, современная цивилизация здесь очень уязвима. Потому что информационные технологии управляют практически любыми сложными процессами, начиная от городского водопровода в развитых странах, или регулирования дорожного движения, и кончая атомными электростанциями, авиационным сообщением и так далее. Вторжение в эту сферу и нарушение этой деятельности чревато самыми тяжелыми последствиями. Я думаю, что сейчас мы проходим только самые начальные этапы работы над таким оружием. Собственно, это оружие – программы, которые позволяют войти в информационные сети противника. В Соединённых Штатах существует даже специальное командование. То есть наряду с территориальными командованиями и, скажем, командованием специальными операциями появилось и киберкомандование.

Такое подразделение есть и в российском министерстве обороны. В силу того, что в России всегда было очень продвинутое математическое образование, в разработке таких программ наши хакеры, может быть, и впереди планеты всей». Правда, многие из них работают не на нас.

Российское оборонное ведомство хорошо осведомлено о научно-практическом потенциале отечественной молодёжи – в начале октября был объявлен тендер на исследования в сфере информационной безопасности. Кроме того, как сообщала российская пресса, силовые ведомства в последнее время начали охотно нанимать на работу наиболее способных хакеров.

Можно представить множество вариантов фатальных последствий, к которым может привести намеренная, или случайная кибератака гидроэлектростанции, канализационной или очистной системы какого-нибудь мегаполиса или химического предприятия. По мнению многих специалистов, компьютерные вирусы в ближайшем будущем будут подвержены такой же опасности неконтролируемого распространения, как вирусы биологические.

Основатель крупнейшей в Европе компьютерной антивирусной компании Евгений Касперский считает, что только международное соглашение

Источник: old.svop.ru

Александр Матвеевич Гольц

способно запретить оборонным ведомствам разрабатывать вирусы и как-то нивелировать потенциальную угрозу в глобальном масштабе. К сожалению, всё не так просто, говорит Александр Гольц. Так, при согласовании международных соглашений по кибероружию странам неизбежно придётся разграничивать государственный контроль потенциально опасных разработок и свободу доступа своих граждан к информации. То есть к Интернету[139].

Различный подход разных государств к вопросам информационной свободы пока не даёт реальных шансов заключить какой-либо договор, сдерживающий разработчиков боевых вирусных программ. Получается, весь мир становится заложником киберпространства – самого гениального и непредсказуемого творения человеческого разума.

Что делать?

Анализ показал, что многие страны мира сейчас создают у себя системы защиты от информационной агрессии и американской культурной экспансии. В той же Франции, к примеру, по телевидению разрешается показывать не более 50% иностранных фильмов, абсолютное большинство которых, как известно, американские. Наше государство пока не приняло никаких существенных мер по защите своих граждан.

Учитывая сложность и специфичность информационного воздействия, для обеспечения безопасности Российской Федерации жизненно необходим специальный координационный управляющий орган по контролю мер по созданию и применению информационного оружия. Необходимо также создание межведомственного Аналитического центра по разработке новейших информационно-психологических технологий на базе Академии ФСБ, МИ МВД при возможном патронаже Совета Безопасности РФ.

Следует задуматься о формировании мощного государственного холдинга масс-медиа, работающего в тесном контакте со специалистами из Аналитического центра.

Для решения встающих проблем требуется объединение усилий в научных исследованиях проблем информационной войны, обеспечения информационной безопасности, а также в подготовке кадров, как исследователей, так и журналистов «нового типа».

---

139 Google: кибербезопасность – это не контроль Интернет-пространства

В современных условиях государству может быть нанесён политический, экономический, экологический и военный урон скрытно, в реальном масштабе времени и без объявления войны с использованием информационного оружия. К сожалению, в настоящее время в России для реализации указанных планов складывается весьма благоприятная обстановка. Как показали результаты проверок, проведенных ФСТЭК России, система взаимоотношений между участниками в сфере обеспечении информационной безопасности объектов информационной и телекоммуникационной инфраструктуры не регулируется законодательно, складываются стихийно, на основе рыночных механизмов, что создает условия для неконтролируемого воздействия на них и, в том числе, для злоупотреблений. На объектах информационной и телекоммуникационной инфраструктуры, в том числе обеспечивающих деятельность силовых и финансовых структур, широко применяется программное обеспечение иностранного производства или заказываемое у случайных поставщиков[140].

В течение последних десятилетий нашей стране целенаправленно навязывалась западная политика в области создания и внедрения средств телекоммуникации. Приватизированы и переданы в иностранные руки государственные пакеты большей части операторских компаний. В интересах иностранных компаний перераспределены частотные ресурсы, созданы условия для ввоза иностранной техники связи и вложения денежных средств. На фоне повсеместного внедрения оборудования ведущих мировых производителей в значительной мере были свернуты собственные научные исследования в области телекоммуникаций, а научные телекоммуникационные центры переориентированы в центры сертификации иностранного оборудования. Среди множества проблем особо следует выделить критическую зависимость отечественных ИТКС от поставок зарубежного информационно-коммуникационного оборудования, а также несоответствие темпов разработки и внедрения средств и способов защиты информации, динамике изменения спектра угроз и росту их интенсивности[141].

Программные и аппаратные закладки, реализующие упомянутые функции, весьма сложно выявить, особенно с учётом того, что ни один иностранный производитель не передаёт для анализа ни принципиальных схем, ни исходных текстов программного обеспечения. Трудоёмкость поиска

---

140 Проект Федерального закона «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры», рассматривался в Государственной Думе РФ 11 марта 2008 года

141 Крикунов А., Королев А. – Вопросы обеспечения информационной безопасности в информационно-телекоммуникационных системах при использовании импортных средств связи и информатизации. Информационно-аналитический журнал центра анализа террористических угроз и центра прогнозирования конфликтов. Ассиметричные угрозы и конфликты низкой интенсивности. Спецвыпуск. 2009, с. с..16-23

закладок становится соизмеримой с разработкой нового аналогичного оборудования. Кроме того, дистанционная загрузка программного обеспечения фирмой-разработчиком по каналам связи, ставшая практической нормой эксплуатации, не позволяет определить, какие модули программного обеспечения в текущий момент исполняются в оборудовании. В этих условиях органы государственной власти, предприятия ВПК и другие учреждения, использующие оборудование иностранного производства, рискуют стать легкодоступным источником информации для иностранных технических разведок.

Таким образом, в современных условиях чрезвычайно важной представляется практическая реализация положений Доктрины информационной безопасности Российской Федерации. Обстановка в современном мире, в том числе вокруг России, требует принятия адекватных мер противодействия иностранной информационной экспансии во всех её проявлениях в следующих основных направлениях:

– формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере;

– совершенствование законодательства РФ в сфере обеспечения информационной безопасности;

– координация деятельности органов государственной власти, министерств и ведомств по обеспечению информационной безопасности;

– систематическая деятельность по выявлению угроз в информационной сфере и их источников, структуризации целей и задач обеспечения информационной безопасности в области обороны, их реализации;

– активное противодействие влиянию на сознание населения с целью изменения национальных духовных и идеологических установок;

– развитие отечественной индустрии телекоммуникационных и информационных технологий, средств информатизации, телекоммуникации и связи, а также защиты информационных ресурсов от несанкционированного доступа, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

– совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учётом вхождения России в глобальную информационную инфраструктуру;

– обеспечение безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры, включая функционирующие в их составе ключевые ИТКС, системы и средства информатизации вооружений и военной техники, системы управления войсками и оружием, как уже развернутым, так и создаваемым на территории РФ;

– защита государственных информационных ресурсов и, прежде всего, в федеральных органах государственной власти и на предприятиях оборонного комплекса;

– установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями её распространения;

– подготовке специалистов в области обеспечения информационной безопасности.

Альтернативы перечисленным направлениям деятельности нет. Невыполнение требований по защите информации может привести к существенным потерям в информационной сфере и, в конечном итоге, в экономике, политике и обороноспособности страны.

Стремительное, порой непредсказуемое развитие международных событий в последнее время показывает, что несанкционированный доступ к информации и специальные воздействия в целях её хищения, разрушения, уничтожения или искажения, нарушение работы систем связи, информационного обеспечения и управления вплоть до полного их отключения могут послужить важнейшим аргументом в информационном противоборстве.

В связи с этим целесообразно разработать и постоянно осуществлять комплекс мероприятий по подготовке к информационной войне не только в вооружённыъ силах и в спецслужбах, но и в масштабе всей страны. В национальном масштабе подготовка к информационной войне заключается в совершенствовании национальной информационной инфраструктуры, включающей все электронные СМИ, банковские системы, системы связи, транспорта, энергетики, промышленности и сферы услуг. Кроме того, эта инфраструктура фактически дополняется непрерывно разрастающейся сетью Internet.

Сегодня эффективное решение задач, связанных с противодействием возросшим угрозам в информационной сфере и обеспечением независимости России от информационной экспансии стран, обладающих развитой информационной инфраструктурой и информационным оружием, возможно только при объединении усилий всех российских министерств и ведомств, отечественного ИТ-сообщества при консолидирующей роли государства. От успешного решения этих задач во многом зависят конкурентоспособность России и благополучие её граждан.

Внутренние мероприятия, включая и выявление узлов уязвимости, должны сопровождаться и дипломатическими усилиями на международной арене, направленными на принятие международных и межгосударственных соглашений по запрещению разработки, усовершенствования и применения информационных вооружений, как традиционных и современных, так и вооружений геоцентрического ТВД.

Общим основанием для принятия таких соглашений может стать использование столь распространённой в современном мире борьбы за права человека, которым в первую очередь угрожает применение информационных вооружений.

Основанием для запрета вооружений геоцентрического ТВД должны стать уже принятые и ратифицированные международные соглашения по запрету использования космоса в военных целях, тем более, использование космоса в качестве оружия массового поражения.

Россия последовательно добивается на международной арене именно такой постановки вопроса, но, увы, остается практически в одиночестве. «Уже проделана определённая работа, подготовлены и доложены материалы по вопросам информационной безопасности на 53 и 55 сессиях Генеральной ассамблеи ООН. Однако этого явно недостаточно. Необходимо приложить все усилия для того, чтобы в XXI веке достижения в области информационных технологий служили исключительно на благо человечества. Упустив момент сегодня, завтра мы рискуем стать на порог очередного витка гонки вооружений. В этом случае опасность развязывания глобальной информационной войны, объектом воздействия в которой станет самое тонкое достижение эволюции – сознание человека, станет реальностью»[142].

Бомба западнизации.

Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе. По этому поводу русский историк А. А. Зиновьев в своей работе «Идеология партии будущего» пишет: «Бомба западнизации», взорванная в России, произвела в ней неслыханные ранее опустошения не только в сферах государственности, экономики, идеологии и культуры, но и в самом человеческом материале общества. В таких масштабах и в такие сроки это до сих пор ещё не удавалось сделать никаким завоевателям и ни с каким оружием. Будучи предназначена (по замыслу изобретателей) для поражения коммунизма, «бомба западнизации» в практическом применении оказалась неизмеримо мощнее: она разрушила могучее многовековое объединение людей, ещё недавно бывшее одной из двух сверхдержав планеты и претендовавшее на роль гегемона мировой истории, до самых его общечеловеческих основ, не имеющих отношения к коммунизму. Целились в коммунизм, а убили Россию. Запад с помощью этого оружия одержал самую грандиозную в истории человечества победу, предопределившую, на мой взгляд, ход дальнейшей социальной эволюции на много веков вперёд».

---

142 Гриняев С. Н. – Информационная война: история, день сегодняшний и перспектива

Всё кажется правильно, но на самом деле всё совсем не так. «Бомба западнизации» как информационная бомба, как вирус иноземной культуры, мутировавший и окрепший, поражая страны Запада, стал «бомбой западнизации», заброшенной в Российскую империю, поражённую и ослабленную тем же вирусом иноземной культуры, по-иному мутировавшим к формату большевизма. Ergo силы, забросившие на постсоветское пространство «бомбу западнизации», вовсе не целились в коммунизм – их идеология неоконсерватизма, идеология мутировавшего от «перманентной революции» к «перманентной контрреволюции» троцкизма, связана со стремлением к завоеванию мирового господства, и они целились в мешавшую им Россию, в русскую культуру, выросшую на Православии, в русские традиции, в русский народ, а вовсе не в «коммунизм».

Они, безусловно, одержали неслыханную победу в этом информационном сражении, но победа в сражении – не победа в войне. Россия, как оглоушенный водкой мужик, валялась в грязи и в крови, но она смогла подняться, преодолевая действие этого страшного вируса, и, пусть пока нетвёрдой походкой, пошла вперёд к очередной блистательной победе русского духа, русских традиций, к возрождению великого государства Российского. Не понятно только, с какого «перепугу» действующие российские власти проявляют большую толерантность к иностранным агентам – операторам информационной войны, чем к требованиям большинства российского общества положить предел разгулу бесовщины и непотребства смутьянов, таскающих по стране «бомбу западнизации».

Поскольку такая война связана с вопросами информации и коммуникаций, то если смотреть в корень, это есть война за знания – за то, кому известны ответы на вопросы: что, когда, где и почему и насколько надёжными считает отдельно взятое общество или армия свои знания о себе и о своих противниках. Россия и русские начали восстанавливать знания о себе, но пока не задумались или в ходе информационного противоборства им не дают задуматься о получении знаний о противниках, и это очевидный элемент уязвимости.

Который уже раз приходится восхищаться способностями блог-оператора, выходящего в кибер-пространство под псевдонимом ***«avanturist»***[143], к построению информационной провокации, подсыпающей тлеющих угольков в портки политиков и генералов всего мира, в том числе и российских. Так, в одном из его наиболее известных блог-сообщений[144] он даёт весьма правдоподобное описание хода и результатов «Долгой войны» США с Евросоюзом и другими геополитическими субъектами, делая основной упор на информационные средства ведения этой войны. Он, безуслов-

---

143 www.avanturist.org 15 марта 2012, csef, Глобальные проблемы

144 Avanturist – Брюссельский сговор: Косово 2008 – «Судеты 1938». Кто станет «Польшей 1939»? 19.02.2008

но, «в теме», он, безусловно, располагает обширной и точной информацией, и он очень искусно выстраивает геополитическую провокацию.

Всегда ли он прав, прав ли он хотя бы в общем контексте или в конкретных существенных деталях? Нет, практически по всем этим вопросам он даёт ошибочные прогнозы. Однако он так близок к корректным выводам, что его аналитические сообщения возбуждают интерес и беспокойство политиков и военных руководителей во всём мире.

1.2.4. Консциентальное оружие

Оружие массового поражения сознания социумов, основанное на утилизации избыточной энергии жизни членов одного социального эгрегора, направляемой на эгрегоры противника через возможности информационного оружия для подавления возможностей осознания реалий актуальной действительности и подавления воли к сопротивлению.

Непредотвращённые последствия воздействия консциентального оружия в принципе неустранимы (эффект «манкурта»).

Опасную разновидность консциентального оружия представляет собой этно-религиозный экстремизм в безосновательно декларируемым владением истиной в последней инстанции, в его стремлении к мировому господству насильственным навязыванием своей мнимой правоты всему миру.

Актуальный пример акции из арсенала консциентального оружия в России связан с недавно возникшей проблемой ношения хиджабов в учебных заведениях Северного Кавказа – пять учениц школы посёлка Кара-Тюбе Нефтекумского района Ставропольского края «пришли», на занятия в хиджабах. Естественно, директор школы как должностное лицо государственного учебного заведения, ответственного за воспитание детей с соблюдением конституционных норм России, отправила их домой переодеться. Не более того. Практически тоже самое, как отправить домой умыться и переодеться неопрятного ребёнка любой национальности или веры. Казалось бы, вопрос исчерпан. Ан, нет, началась бюрократическая карусель, в которую втянули местного муфтия. Министр образования федерального правительства, который, по-видимому, никогда внимательно не читал Конституцию страны, которой он нанят служить, публично пробормотал что-то невнятное в стиле «никогда больше не допустим». Родители, отправившие своих детей в школу в хиджабах, подали на педагога в суд. В дело вмешалось казачество и общественные организации православных. Только после вердикта президента России как гаранта Конституции всё успокоилось. Оказалось, что девочки вполне могут ходить в школу в головных платках, не нарушая законов Ислама.

И это беда, когда для решения очевидного вопроса, но по предмету, несущему в себе угрозу общественной безопасности, это становится предметом вмешательства высшего должностного лица государства. Зачем тогда глава поселковой управы, зачем тогда полицейское подразделение и прокурорский надзор, зачем глава района, и если вопрос так запущен, то зачем тогда губернатор, не говоря уже о министре, который откровенно никому не нужен.

А всё могло быть так просто – упомянутые чиновники, обязанные знать ситуацию в регионе могли распределить между собой сферы ответных действий согласно должностным обязанностям, то есть «делать, как учили». Пограничники (ФСБ) могли отметить факт завоза в страну господином Х большой партии хиджабов (а они в действительности поступили в продажу в Ставропольском крае) и проинформировать ОФСБ по Нефтекумскому району, ОФСБ мог поручить Отделению полиции Кара-Тюбе проверить участие гражданина Х в экстремистских организациях, а Отделение полиции не могло бы, а должно было немедленно прореагировать на публичную акцию группы лиц, связанную с нарушением положения Конституции Российской Федерации, совместно с прокуратурой обсудить проблему с местным муфтием и решить вопрос о мерах по пресечению нарушения российского законодательства. Однако всё пошло как в станице Кущёвской соседнего Краснодарского края. Шло, шло, пока не дошло до президента.

Консциентальное оружие по своей сути представляет собой сумму реализованного и, в какой-то мере, реализуемого духовного и интеллектуального потенциала государства, действующего через механизм и материальную базу информационного оружия. Эффективность консциентального оружия зависит от наличия, метрологической проработанности и защищённости суверенной технологии генерации нуля времени.

Необходимо заметить, что страны христианской Эйкумены (за исключением, пожалуй, только мормонов) изначально, с III века новой эры (с «Константинового дара» – Библии как двукнижия, включающего Ветхий завет (***де факто*** – Тору) и Новый Завет, основанный на Нагорной проповеди Иисуса Христа и на части Евангелических текстов), получили ограничение своего суверенитета в генерировании нуля времени. России в этом смысле повезло больше других христианских стран – Русская Православная церковь, отстаивая свою независимость и независимость Российского государства, сохранила Юлианский календарь, оставив возможность маневра и более глубокой автономии в генерации нуля времени.

Консциентальное оружие всегда напрямую связано и основано на определённом идеологическом постулате. Так, оседлавшие американское общество неоконсерваторы как перекрасившиеся троцкисты выдвинули и в течение десятилетий эксплуатируют постулат «исторической миссии» США в «перманентном»

навязывании мировому сообществу «американской модели демократии»[145]. Эта модель как плохая одёжка тянет подмышками и режет в промежности даже самым верным союзникам США по НАТО, и она уж вовсе не к лицу ни православным, ни мусульманам, ни буддистам, а это как не кинь более 80% всего населения планеты – за что же такая напасть? Многие американские учёные-политологи весьма критично относятся к этой идеологической модели. Так, Ричард Хофстедтер даёт ей такую оценку: «Моралистскую и религиозную белиберду Доктрины исторической миссии, так типично американскую в своем непомерном примитивизме, легко отбросить как идеологический мусор. И всё же, эта отталкивающая чушь стала основой американской политической теологии и внешней политики»[146].

Однако другие сообщества не сформировали или не выдвигают своих обоснованных постулатов, будучи одурманены кто большевизмом, кто национал-социализмом, кто фашизмом, кто национальным или религиозным экстремизмом, кто сайентологией – токсичными для сознания масс продуктами переломного XX века, иногда именуемого Ха-Ха веком.

Нужно заметить, что у России, как у государства, территориально объединяющего две части Евроазиатского континента, многие века, когда осознанно, когда неосознанно, существовала **великая историческая миссия щита цивилизаций** – защиты Востока от нашествий европейских варваров и защиты Запада от нашествий азиатских варваров[147].

Именно с таким идеологическим постулатом Россия была, даже тогда, когда Российская империя считалась «европейским жандармом», и даже в формате СССР, когда русский народ, ценой ужасных потерь стал основной силой, спасшей Европу и не только её от национал-социалистической чумы, и есть, даже в настоящее, трудное для России время, цивилизационный оплот этой великой миссии, и народы Земли могут быть уверены, что Россия, верная этой исторической миссии, будет интересна и необходима всему человечеству.

1.2.5. Психотронное оружие, в том числе инфразвуковое оружие

Оружие массового поражения, в основе действия которого лежит принудительное разрушающее или управляющее (деформирующее) воздействие на человеческую психику и психику животных, основанное на воздействии низкочастотным полем, всегда более или менее отличным от базовой частоты поля Земли ($\nu_з$ = 7,83 Гц) и частоты нормального α-ритма мозга высших

145 Спектор В.Н. – Из огня, да в полымя или опасные шашни с «Дядей Сэмом». Труды МАН ПНБ, том 2, вып. 5, с. 112

146 Hofstadter Richard Social Darvinism in American Thought

147 Спектор В.Н. – Формирование нового мирового устройства: прогнозируемая роль отдельных государств и цивилизационных сообществ (монография, том 1). МАН ПНБ. М., 1997; Курепина Н.С., Спектор В.Н. – Факторы сегрегации и агрегации национально-государственных социумов

приматов, включая человека ($\nu_{\alpha\text{-ритма}} \approx 7{,}83$ Гц), с настройкой его частоты, $\nu_i \neq \nu_з$, $\nu_{\alpha\text{-ритма}}$, на предельное нарушение функционирования структур головного мозга, периферической нервной системы и сосудистой системы человека.

В интервью редакции: «Россия и мир» (Информационно-аналитическое издание Фонда исторической перспективы «СТОЛЕТИЕ») 16.05.2011председатель Русского геополитического общества С. Шатохин заявил, что «Есть предположение, что «HAARP» (HAARP – High frequency Active Auroral Research Program – программа по исследованию активных высоких частот ионосферы. Фактически, система HAARP представляет собой установку, которая предназначена для осуществления модификации ионосферы, то есть внесение в нее определенных изменений, – прим. авт.) является ещё и психотронным оружием, способным воздействовать на психическое и моральное состояние людей определённых регионов планеты.

В письменном дополнении к интервью он дал более полное объяснение своего предположения. В структуре ХААРП создана группа VLF (Very Low Frequency – очень низкие частоты), которая работает над тем, чтобы с помощью HAARP генерировать очень низкие и сверхнизкие частоты, посредством процесса, называемого модулированным нагреванием (ионосферы). Такие эксперименты проводятся с 1999 года. Их действие направлено на нарушение психики и в целом на подрыв здоровья неограниченного количества людей. Влияние на процесс голосования на выборах и референдумах – самое «безобидное» применение. Они из любого числа людей на любой территории могут сделать «зомби». Могут инициировать и физические болезни, не связанные «с головой», например, воздействовать частотами на сердечнососудистую систему людей на значительной территории. Своими разработками они способны привить любое состояние массе людей – отчаяние, страх, беспричинную радость, ненависть и т. д.»

Одним из методов, применявшихся уже в современном психотронном оружии, является нейролингвистическое программирование (НЛП), как технически подтверждённая методика глубокого долговременного гипноза и закладки управляющей информационной бомбы в подсознание человека (зомбирование через неосознанное подсознательное), а в пределе в коллективное подсознание широких масс людей.

Публично признанными разработчиками метода НЛП стали два американских психолога: Ричард Бэндлер и доктор психологии Джон Гриндер. Работы по созданию и практическому применению метода НЛП может быть даже раньше, чем в США, в закрытом режиме велись и в СССР[148].

---

*148 *В молодости Дж. Гриндер работал тайным агентом ЦРУ в Германии, Италии и Югославии. В начале семидесятых его имя стало известным среди любителей генеративно-трансформационной грамматики, восходящей к Ноаму Хомскому. Он также работал младшим ассистентом профессора лингвистики под руководством Грегори Бейтсона в Крест Колледже.*

Источник: www.lawinrussia.ru

Сергей Антонович Шатохин

Основной целью перспективного психотронного оружия, управляемого группой СНЧ ХААРП (три наземных станции: Аляска, Норвегия, Гренландия; космические станции: геостационарные комплексы и мобильный комплекс на базе БПЛА Х-37 и два мобильных надводных комплекса на базе линкора «Висконсин» и крейсера «Вирджиния»), является воздействие на экипажи боевых машин (военных судов, субмарин, танков, самолётов, автомобилей, БТР) с целью их поражения или дестабилизации. Возможно массовое воздействие на отдельные территории с целью поражения населения, для создания массовых состояний агрессивности, сонливости, депрессивности и т. д. В международной специальной литературе опубликована информационная спекуляция о проведении СССР операции «Русский дятел», вызвавшей депрессивные синдромы на территории целого штата США. Относится к категории оружия, применяемого скрытно.

В своей, как обычно крайне политизированной работе «Климатическое оружие: блеф или реальность?» президент Академии геополитических проблем, доктор исторических наук, генерал-полковник Леонид Ивашов [149] пишет: «Развитие мировой научной мысли США используют в интересах своих военных программ. Не стали исключением и программы по созданию и применению климатического, психотронного и других типов оружия, основанного на новых физических принципах. Публикации в открытой зарубежной печати совершенно очевидно и ясно свидетельствуют: в последние годы в США не только активно разрабатывается, но и испытывается так называемое волновое или геофизическое оружие». Далее Ивашов сообщает интересную информацию о том, что в Пентагоне существует весьма значимая структура – Отдел перспективного вооружения, В, включающий два департамента: департамент «С» (по-видимому, от английского climate – климат) и департамент «Р» (не исключено, от английского policy – политика) и что этому департаменту был передан крейсер «Вирджиния», оснащенный неким комплексом секретного оборудования.

Л. Г. Ивашов сообщает также, что третье направление трудов Отдела перспективного вооружения, В – воздействие волновых процессов на психи-

149 Ивашов Л. – Климатическое оружие: блеф или реальность? Информационно-аналитический журнал Центра анализа террористических угроз и Центра прогнозирования конфликтов, № 9 «Асимметричные угрозы и конфликты низкой интенсивности, 2010, с. 70 (впервые опубликована в газете «Военно-промышленный курьер»)

ку и сознание человека. Этим занимается департамент «Р». Вызывая искусственные магнитные бури и применяя рассеянное или целенаправленное излучение волн различной длины и частотного диапазона, можно затормозить и расстроить функционирование головного мозга. В секретных задачах этого департамента значится разработка методов влияния на большие массы людей на различных расстояниях, чтобы порождать у них страх, апатию, подавленность или же, наоборот, возбудимость, агрессию, состояние аффекта. Проще говоря, управлять поведением населения любой страны.

Источник: ru.wikipedia.org

Ричард Бэндлер

Источник: www.kood.ru

Джон Гриндер

Российские учёные обнаружили проведение таких опытов американцами в РФ в августе 1999 года, когда в качестве «подопытных» оказались жители Москвы и Московской области, а также Краснодарского края. Как уже говорилось, в 2000 году департамент получил списанный из ВМФ крейсер «Вирджиния», на который установили соответствующее оборудование и направили специалистов для его обслуживания. Работа этой аппаратуры фиксировалась в 2003 году в ходе операции против Ирака и в 2005-м – в дни «оранжевой революции» на Украине. В отчёте о данных апробациях была подчеркнута их высокая эффективность.

Есть информация, что сейчас «Висконсин» и другие носители оборудования, аналогичного тому, что имеется на этом линкоре, применяются против Ирана и Турции с целью свержения неугодных американцам режимов, а также России (Северный Кавказ). Фиксируются волновые воздействия на российское население – и извне, и с территории самой РФ.

Наконец генерал Ивашов сообщает: «…Соединённые Штаты не только оторвались от всех других стран мира в классе современных высокоэффективных обычных вооружений, но и получают в руки новое оружие массового

поражения глобального воздействия. Ядерные боеприпасы выглядят весьма устаревшими на фоне описанных систем, отсюда – «миролюбивые» призывы Вашингтона к всеобщему ядерному разоружению.

С другой стороны к этому вопросу подходит участник многих переговоров с Западом по контролю вооружений генерал-лейтенант Службы внешней разведки (СВР) Геннадий Евстафьев («Известия»). Его глубокий и основанный на личном опыте международного военного переговорщика анализ представляет безусловный интерес.

Бывший посол СССР в ФРГ Валентин Фалин и спецслужбист-отставник Геннадий Евстафьев написали доклад, который был роздан депутатам и сенаторам[150].

Один из бывших руководителей СВР, генерал-лейтенант Геннадий Евстафьев: «…большую роль играют «свои внутренние эксперты» в России, меньшую – наблюдатели БДИПЧ, ОБСЕ. Как видно, на эту роль сегодня претендует ассоциация «Голос». Вопрос не только в том, что она не раскрывает публично источники своего финансирования, вопрос в том, что источники

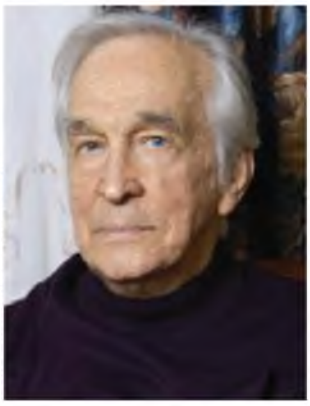
Слева направо: Эсминец «Buck», линкор «Wisconsin» и крейсер «St. Paul»
(генерал без сопровождения полковника и капитана не ходит).

150 Московский комсомолец, 21.09.2006

этого финансирования понятны любому ветерану холодной войны»[151].

Источник: www.pircenter.org

Геннадий Михайлович Евстафьев



Источник: www.liveinternet.ru

Валентин Фалин

«Новая американская администрация выступила с инициативой по сокращению вооружений. Сама по себе идея сверхглубоких сокращений стратегических ядерных вооружений, сопряженная, как утверждают, с прекращением развертывания ПРО в Европе, не может не приветствоваться. Отрадно, что новая администрация США наконец-то косвенно признала то, о чём давно говорили в Москве: ПРО США в Европе не имеет никакого отношения к ракетно-ядерным программам третьих стран, а назначена преимущественно против российских стратегических сил. Но стоит заметить и несколько «подводных камней», о которых вашингтонская администрация старается не упоминать.

Первое. Столь глубокие сокращения стратегических наступательных вооружений Россией и США невозможны без подключения к процессу сокращения ядерных стратегических вооружений третьих стран. И если в отношении Великобритании и Франции – фактически в стратегическом отношении сателлитов Вашингтона – особых проблем, вероятно, не возникнет, то вопросы о ядерном потенциале КНР остаются. Ведь постоянно растущий ядерный потенциал Поднебесной никакими международными соглашениями на сегодняшний день не ограничен и вообще является нетранспарентной величиной. Конечно, Россия является стратегическим партнером КНР, однако сфера стратегических вооружений не допускает никакой неопределенности.

Второе. Чтобы идти на сверхглубокие сокращения стратегических вооружений, нужно новое качество политических отношений между двумя странами, а главное – высокий уровень взаимного доверия. Но США пока не отказались ни от одного из своих ошибочных и дестабилизирующих заблуждений. Ни от продвижения НАТО на Восток, ни от размещения военной инфраструктуры на территории стран Восточной Европы, ни от милитаризации космоса и Арктики, ни от доктрины наступательных операций за пределами зоны ответственности НАТО, ни от милитаризации Грузии,

151 Иван Афиногенов – [http://www.russianskz.info/2011/11/. Ноябрь 2011

ни от ренацификации Украины. Чтобы двигаться по пути сокращения ядерных потенциалов, США должны доказать нам и всему миру приверженность международной стабильности и взаимному партнёрству. А этого пока не видно.

Третье. Насколько можно пока судить, основным предметом сокращений планируется сделать баллистические ракеты наземного базирования и подводные лодки. Но вот как быть со стратегической авиацией? В рамках договора СНВ-1 США выторговали принцип «условного зачёта», когда, в частности, для самолета B-1B, который может нести до 22 ядерных боеголовок, засчитывался один ядерный заряд. Для B-52 – вместо 20 всего 10 крылатых ракет. Затем, после подписания в 2002 году Договора СНП (сокращения наступательных потенциалов), B-1B и B-52 по большей части вообще стали считать неядерными носителями. Конечно, в обмен США пообещали хранить ядерное оружие в 100 километрах от мест базирования самолетов. Это не шутка. Сверхновые бомбардировщики B-2 вообще изначально рассматривались как неядерные. Надо ли напоминать, что количество стратегических бомбардировщиков США в разы превышает количество стратегических бомбардировщиков в российских ВВС. А общее количество ядерных боеголовок, которые США смогут при желании установить на них, превысит 3000 штук, т. е. будет в три (!) раза больше предлагаемого Вашингтоном ориентира. И это при том, что стараниями Вашингтона механизм контроля над авиационной компонентой СЯС сведен к минимуму.

Четвертое. В Вашингтоне, вероятно, выводят за скобки крылатые ракеты морского базирования с дальностью более 600 км. Конечно, они не могут рассматриваться в качестве стратегического оружия в чистом виде. Конечно, в рамках существующих договоренностей по ограничению стратегических ядерных потенциалов США приняли обязательство не развертывать КРМБ в количестве, превышающем 880 ракет. Но в условиях тотального господства ВМС США на море данный тип вооружения приобретает, безусловно, стратегическое значение, тем более, что боевая дальность ракеты «Томагавк» последних модификаций превышает 3500 км. И к тому же 880 КРМБ – это ПОЧТИ РАВНО оставляемому России стратегическому ядерному потенциалу.

Пятое. Вероятно, трудно говорить о возможности сверхглубоких сокращений стратегических ядерных вооружений вне ограничения развития военных ядерных технологий в целом. В Вашингтоне болезненно относятся к ядерной программе Ирана, но почему-то выказывают гораздо меньшую обеспокоенность ядерными потенциалами Израиля, Пакистана, а теперь уже – по мере нарастания американо-индийского сближения – и Индии, фактически, идя по пути легализации ядерного статуса Дели, подрывая всеобъемлющий характер Договора о нераспространении ядерного оружия, США

отказались ратифицировать Договор о всеобщем и полном запрещении ядерных испытаний. Более того, США сделали всё от них зависящее, чтобы торпедировать вполне разумное предложение России об отказе от размещения ядерного оружия за пределами национальной территории стран-обладателей, которое сейчас возобновлено Россией. О каком стремлении США к безъядерному миру можно в таком случае говорить?

Шестое. США обладают колоссальным преимуществом в обычных вооружениях, прежде всего в высокоточном оружии. А главное – США способны концентрировать мощные наступательные группировки практически в любой части мира, опираясь на разветвленную военную инфраструктуру, которая, напомним, всё ближе и ближе к границам России. А теперь представьте, насколько наглее вели бы себя США в ходе агрессии Грузии в Южной Осетии, если бы не были уверены в адекватности и гарантированности российского ядерного возмездия.

Наконец, мы привыкли к стратегической стабильности на относительно больших уровнях стратегических ядерных потенциалов. Однако на сверхнизких уровнях стратегических ядерных вооружений всё становится гораздо сложнее. Возникает реальный риск принятия ошибочного операционного или даже политического решения, а порог применения ядерного оружия существенно понижается. И вполне возможно, что решение о первом обезоруживающем контрсиловом ударе станет выглядеть не таким уж безумным. Кстати, единственный случай, когда Россия и США действительно стояли на грани ядерной войны и когда сценарий обезоруживающего удара действительно рассматривался, – Карибский кризис – произошёл в момент, когда стороны находились на сравнительно низких уровнях стратегических ядерных сил.

Мораль: любая инициатива, исходящая от США, предназначена, прежде всего, для обеспечения американских и только американских интересов. Но в чём же их стратегический замысел?

Реализовав предложение по размену не созданной системы противоракетной обороны, завершение строительства которой в современных экономических условиях для США является весьма проблематичным, на реальный российский ядерный потенциал, США не просто укрепляют своё глобальное военно-политическое доминирование. Реализация американского предложения выводит Россию из числа стран, которые способны оказывать серьёзное влияние на глобальный военно-политический баланс сил, фактически заставляя её для сохранения статуса ввязаться в гонку обычных вооружений в один из наименее благоприятных для этого моментов.

Конечно, если Россия перестаёт быть фактором, который необходимо постоянно учитывать, США будут куда комфортнее продолжать стратегиче-

ский диалог с КНР, о котором всё больше говорят в кулуарах большой политики. Ведь в Вашингтоне прекрасно знают о колоссальной степени зависимости КНР от американского рынка. Не ясно вообще, может ли «китайское экономическое чудо» существовать вне стратегического партнёрства с США. В ситуации «один на один» Вашингтону будет куда проще заставлять Пекин действовать в фарватере своих интересов, используя все уязвимые места и слабости современной китайской государственности.

Так что желание новой американской администрации «удушить Россию в объятиях» ядерного разоружения понятно. Однако неужели в США так уверены, что Москва, как и в лихолетье 1990-х годов, будет играть с Вашингтоном в поддавки? Тем не менее, надо поблагодарить американцев за предложение, но обозначить понимание его сути. Только удостоверившись, что любой зондаж «мирных инициатив» воспринимается доброжелательно, но без восторга, США начнут предлагать действительно мирные инициативы. Без кавычек»[152].

Важно сделать всех конкурентов и соперников беззащитными перед американской демократией. <…> Советский Союз вслед за началом реализации американских проектов в области использования атмосферных явлений в военных целях тоже приступил к работам в этом направлении и добился определённых успехов. Одновременно были образованы структуры военной и научно-технической разведки для наблюдения за исследованиями в США. Но в 90-е годы научные разработки у нас свернули (базовый объект в Нижегородской области законсервировали), а часть полученных результатов передали заокеанскому «партнёру» РФ. Разведывательные подразделения, проявившие активность после применения климатического и психотронного оружия против России, срочно расформировали, сотрудников уволили со службы…».

1.2.6. Инфразвуковое оружие

Оружие массового поражения (предтеча психотронного оружия), применяемое независимо, параллельно или совместно с другими видами психотронного оружия и использующее в качестве поражающего средства достаточно сильный инфразвук (верхняя граница диапазона – $\nu_в$ = |16-25| Гц; нижняя граница – условно $\nu_н \approx 0{,}001$ Гц). При совпадении воздействующего звука с ритмами мозга (альфа-ритм, бета-ритм, гамма-ритм, дельта-ритм, тета-ритм, каппа-ритм, мю-ритм, сигма-ритм и другие) может возникнуть нарушение активности церебральных механизмов мозга. В зависимости

152 Геннадий Евстафьев «Подводные камни «американской инициативы. http://www.izvestia.ru/politic/article3125399/index. html

от силы инфразвукового воздействия результатом может быть возникновение у объекта от чувства страха, ужаса или паники и психозов на их почве, до соматических расстройств, вплоть до летального исхода. Очень высокий уровень инфразвука может вызвать нарушение в статических и динамических органах равновесия тела, которые являются частью внутреннего уха.

Инфразвук – своего рода «акустическое нейтрино» – способен проходить без заметного ослабления через стекла и даже сквозь стены. Все случаи контакта человека и инфразвука можно поделить на две большие группы: контакты с бегущей волной и контакты в полости резонатора.

Опытные образцы инфразвукового оружия уже применялись США в Югославии. Так называемая «акустическая бомба» производила звуковые колебания очень низкой частоты. На совещании с постоянными членами Совета безопасности РФ Дмитрий Медведев сообщил о том, что в войнах уже ближайшего будущего будет широко применяться инфразвуковое оружие[153].

Как уже отмечалось в разделе «психотронное оружие», подразделение СНЧ ХААРП воздействием на ионизированные оболочки способно генерировать низкочастотное излучение, что переводит инфразвуковое оружие в разряд перспективных СМП в арсенале вооружений геоцентрического ТВД.

1.2.7. Кибернетическое оружие

Оружие представляет собой средства уничтожения, искажения или хищения информации; средства преодоления систем защиты; средства ограничения допуска законных пользователей (один из авторов сам неоднократно весьма селективно лишался допуска к собственным файлам, которые очевидно не могли нравиться определённым силам в США); средства дезорганизации работы технических средств, компьютерных систем для разрушения систем управления всех уровней (от муниципального до общегосударственного) и всех назначений (от производства продуктов питания до систем управления ТВД и национальной безопасности). По вторичным эффектам (нарушение водо- и энергоснабжения, обеспечения продуктами питания, разрушения ЖКХ, банковской системы и т. п.) применения кибернетического оружия оно, безусловно, относится к оружию массового поражения, в первую очередь гражданского населения.

Освоение кибернетического пространства военными уже привело к переоценке многих постулатов военной науки прошлого и настоящего, и даже фундаментальных представлений о характере обеспечения глобаль-

153 Птичкин Сергей – Нападать не будем, а за себя постоим: Президент утвердил Военную доктрину Российской Федерации. «Российская газета» – Федеральный выпуск № 5104 (25). 08.02.2010

ного доминирования. Появились новые теоретики военного дела и новые теории.

Наиболее интересным текущим результатом этого процесса (он явно только начался, и ещё преподнесёт сюрпризы) является, вероятно, доктрина «Геоцентрического театра военных действий», выдвинутая командующим космическими войсками ВВС США генералом Робертом Келером. В её основе – представление о фундаментальной взаимосвязи кибернетического и космического пространств.

Современное кибернетическое оружие в качестве основного средства генерации поражающего воздействия использует материальную базу космических войск. Так, в США в 2007 году было создано единое киберкосмическое командование и сформирована специализированная 24 киберкосмическая армия. Руководящий документ AFDD3–12 Киберкосмические операции/Cyberspace Operations, утверждённый 15 июля, был впервые опубликован 14 октября 2010 года. В нём было отмечено, что киберпространство – первая в истории искусственная арена боевых действий. До его появления войны велись только в естественных доменах, то есть на суше, на море, в воздухе и в космосе.

Теоретической и логистической основой кибернетического оружия является информационное оружия, а само кибернетическое оружие служит материально-технической базой реализации информационного оружия.

1.2.8. Климатическое оружие, включая экологическое оружие.

Оружие на новых физических принципах, является оружием массового поражения, использующим в качестве поражающего фактора внешние воздействия, приводящие к изменению климатических условий на достаточно большой территории на достаточно продолжительное время. Объектами поражающего действия климатического оружия является флора и фауна, а также население атакуемой территории[154].

В 1958 году представитель Белого дома заявил, что министерство обороны США «изучает возможности манипулирования состояниями мирового океана, земли и неба, изменяя таким образом погодные условия». Сказанное тогда, скорее всего можно расценивать как декларацию о намерениях, но впоследствии намерения стали последовательно реализовываться, а уже в начале XXI века стали официально объявленной политикой США.

---

154 Спектор В. Н. – Глобализация, человек, климат и экология планеты. Интерполитех-2010. Секция № 1. Москва, Президент отель, 2010;

Спектор В. Н., Спектор В. А. – Глобализация, человек, климат и экология планеты (монография, в печати), М., 2012, 197 с.

Считается, что американская армия во вьетнамской войне в 1970-е годы первой в мире применила метеорологическое оружие. Американцы, взрывая ракеты с химреактивами над расположением вьетнамских войск, тем самым провоцировали затяжные ливни. Украинский физик Геннадий Черняк из конструкторского бюро «Южное» в Днепропетровске, считает, что есть и иная версия о природе метеорологического оружия, которая связана с часто употребимым в последнее время термином «глобальное потепление». «Есть теория, что парниковый эффект – лишь выдумка, которой США прикрывают применение метеорологического оружия», – заявляет ученый. Российский аналитик Владимир Дерновой считает основоположником американского метеорологического/климатического оружия профессора Гордона Мак-Дональда из Института геофизики при Калифорнийском университете: «Ещё в середине 60-х годов он сформулировал основы его применения. Как писал учёный, «задача состоит в определении нестабильностей в атмосфере. Если к ним добавить небольшое количество энергии, высвобождаются гигантские энергетические потоки!».

В свою очередь американцы уверены, что ураганы на них насылает Россия. В августе 2005 года после урагана «Катрина», самого разрушительного в истории США, унесшего 1836 жизней, Скотт Стивенс заявил, что ураган «мог быть инициирован разработанным ещё в СССР «погодным оружием», которое с помощью мощных электромагнитных волн генерирует нестабильность воздушных масс». Стивенс, вне всякогосомнения, подразумевал работу советской станции «Сура». Он же считал, что применение таких технологий в отношении США началось еще в 1976 году. Кстати, по этому поводу есть версия, что тот же ураган «Катрина» – это были неудачные испытания метеорологического оружия, только, не российского, а американского.

1.2.9. Тектоническое оружие

Оружие массового поражения, использующее в качестве поражающего фактора ударное локальное нарушение взаимодействия магнитосферы с магнитным полем Земли на выбранной территории, что приводит к возникновению турбулентности в магматических слоях (вязко-текучая среда) со сверхкритическими скоростями потоков.

Потоки магмы со сверхкритическими скоростями по механизму дилатансии[155] обретают в пике волны дилатансии свойства сверхтвёрдого тела с боль-

155 Зюзина Г. Ф., Спектор В. Н., Краснов А. П., Чижевский О. Т., Дьячков А. И. – Явление разрушения волны дилатансии в многокомпонентных системах при сверхкритических скоростях деформирования (дилатантно адаптированные структуры). ФГУП ФНПЦ «Прибор». Зарегистрировано открытие от 27 января 2010 года № 385 (регистрационный номер Диплома 484) с приоритетом от 12 мая 1995 года

шой запасённой энергией Евд >> 100 Мегатонн в тротиловом эквиваленте (оценочно). В результате ударного взаимодействия волны дилатансии с неровностями, например, в сочленениях тектонических плит нижней поверхности твёрдой коры происходит их деформирование и разрядка запасённой энергии, что приводит к катастрофическим последствиям на поверхности Земли – землетрясения, извержения вулканов, возникновение цунами и т. п.

По результирующему воздействию таких природных проявлений геотектоническое оружие классифицируется как средство массового поражения.

США в 1964 году впервые испытали геотектоническое оружие. Они запустили в ближний космос большое количество медных иголок, которые изменили проводимость нижней ионосферы. Как следствие, на Аляске произошло мощнейшее землетрясение, затронувшее и советские территории – Чукотку и Камчатку, где практически сразу активизировались вулканы. После того как иголки снизились и вошли в плотные слои атмосферы, последовала целая серия землетрясений. Причем, одно из них очень мощное, в Чили, которое привело к сползанию в океан значительной части побережья. Надо отметить, что геотектоническое оружие плохо управляемо. Однако, череда последних разрушительных землетрясений в Иране (в том числе в традиционно тектонически спокойных районах) и в Китае позволяет предположить, что разработки в этом направлении ведутся и насегодняшний день в части управляемости (наведении на цель) этого оружия массового поражения достигли значительных успехов.

Мощность геотектонического оружия постоянно возрастала. Как показал проведенный США эксперимент, взрыв ядерного оружия в верхних заряженных оболочках земли позволяет за счёт изменения состояния магнитосферы, взаимодействующей с собственным магнитным полем Земли, многократно усилить и пролонгировать действие геотектонического оружия.

1.2.10. Пучковое, включая лазерное оружие

Являясь, безусловно, оружием геоцентрического ТВД, не классифицируется как средство массового поражения. Оно предназначено для обеспечения функционирования собственного оружия геоцентрического ТВД (защиты) и уничтожения современного ОМП (межконтинентальных ракет, спутников системы СОИ и GPS) и оружия геоцентрического ТВД (беспилотных космических летательных аппаратов и управляющих центров в околоземном космическом пространстве и на геостационарных орбитах) противника в космосе.

В связи с высокими уровнями рассеяния высокоэнергетических излучений в атмосфере наиболее эффективное использование пучкового оружия

достигается при его генерировании в космосе на борту спутника или космического ЛА, а также под действием накачки с наземных СВЧ- излучателей.

Современное лазерное оружие имеет широкий спектр боевых применений даже в земной атмосфере. Маломощное лазерное оружие применяется в постановке световых меток для артиллерийских систем со снарядами с активной фазой полёта (например, самоходный гаубичный комплекс МСТА) и для авиационных бомб пассивного наведения, в прицелах огнестрельного оружия для повышения точности стрельбы. Мощные лазеры используются для ослепления операторов военной техники, в первую очередь самолётов и вертолётов, в активных системах наведения оружия, в первую очередь ракетного, а также для разрушения защитных экранов средств военной техники, в первую очередь остекления кабин летательных аппаратов.

Однако в условиях земной атмосферы эффективность лазерного оружия ограничена несколькими неблагоприятными факторами: поглощением оптически активными компонентами атмосферы (пары воды, окислы азота и серы, летучие гидриды, пары углеводородов и другие), рассеянием на микрочастицах (пыль, туман, дымы и другие) и дефокусировкой пучка (чем мощнее лазер, тем сильнее дефокусировка). Военная наука и промышленность научилась значительно снижать отрицательный эффект фактора поглощения лазерного излучения производством приборов, обеспечивающих излучение с узкими спектральными характеристиками в окнах прозрачности атмосферы.

Достаточно полно особенности применения ВМФ современного лазерного, а также перспективного пучкового и лазерного оружия приведены в работе Б. И. Радионова и Н. Н. Новичкова.

В Соединённых Штатах Америки с 1983 г. развернуты работы по программе так называемой «стратегической оборонной инициативы» (СОИ). В рамках СОИ американские специалисты ведут исследования принципиально новых боевых средств, и в частности лазерного, пучкового и кинетического оружия. Оно, по мнению западных экспертов, способно уже в ближайшем будущем произвести

Источник: folki.yandex.ru, guns.arsenalnoe.ru

Общий вид самоходной гаубицы «Мста-СМ» и управляемого снаряда «Краснополь»

подлинную революцию в способах и формах вооруженной борьбы на море[156].

Лазерные пучки способны эффективно разрушать различные типы целей в результате теплового или ударного воздействия. Атмосфера прозрачна для лазеров, работающих в видимом или оптическом диапазоне волн (0,3-1,0 мкм). Поражающее действие мощного лазерного излучения, энергия которого переносится практически с максимально возможной в природе скоростью света (300000 км/с$^{-1}$), проявляется, прежде всего, в мгновенном повышении температуры облучаемой поверхности, что может привести к локальному перегреву, воспламенению или другому термомеханическому разрушению. При возрастании плотности энергии в лазерном пучке до 1,0 кДж/см$^{-2}$ можно прожечь корпус самолета или ракеты из алюминиевого сплава, вызвать преждевременный подрыв заряда взрывчатого вещества, вывести из строя бортовую аппаратуру цели. Для магниевых сплавов потребуется почти такая же плотность энергии, а для титана в полтора раза большая. Поглощение лазерного излучения происходит на сравнительно малой глубине вещества.

В США прошли испытания по применению лазерного оружия против дозвуковых воздушных мишеней BQM-34A. Высокоэнергетический газодинамический лазер на двуокиси углерода, установленный на борту самолета-лаборатории NKC-135, работал в ИК-области спектра на длине волны 10,6 мкм. Воздушные мишени BQM-34A имитировали атаку надводного корабля крылатой ракетой, летящей по настильной траектории вблизи водной поверхности. В ходе испытаний одна мишень была полностью разрушена, две другие повреждены. Были продемонстрированы возможности точного целеуказания и наведения лазера на цель, а также достаточно точного удерживания лазерного пучка на выбранных участках мишени.

Зарубежные военные специалисты считают, что лазерным излучением можно поражать пкр, корабельные оптико-электронные средства наблюдения, разведки и наведения оружия, а также другие цели. Определенную опасность лазерное оружие представляет и для органов зрения человека, поскольку воздействие на глаза излучения с плотностью потока энергии более 1,0 Дж/см^2 приводит к полной потере зрения.

В случае применения лазерного оружия на морских ТВД будет происходить значительное поглощение энергии пучка за счет влияния атмосферы, в первую очередь – влажности и солевого тумана. К тому же нередко проявляются такие нелинейные эффекты, как расфокусировка пучка за счёт перегрева воздуха на трассе его прохождения и электрический пробой атмосферы (солевой туман), что обусловливает ужесточение требований к величине выходной мощности лазера и частоте повторения импульсов.

---

156 Радионов Б. И. и Новичков Н. Н. – Крылатые ракеты в морском бою (монография). Военное издательство. М., 1987, 214с. rbase.new-factoria.ru›Tomahawk

Энергетические возможности лазеров, условия распространения лазерного излучения в атмосфере, дальнейшее развитие систем управления лазерным пучком, наведения и целеуказания будут играть важную роль в определении места нового оружия в ближайшем будущем.

По мнению специалистов в области морских вооружений, лазер можно с успехом применять для борьбы с высокоскоростными низколетящими маневрирующими воздушными целями, и в первую очередь с ракетами. Обычные средства ПВО требуют учёта времени полёта ракеты или самолёта на перехват цели и расчёта координат упреждения. В случае применения лазерного оружия необходимость в этом отпадает, поскольку цель не имеет времени на выполнение маневров уклонения. Для перенацеливания пучка с применением информационных технологий требуются доли секунды.

Порог теплового поражения воздушной цели лазерным оружием можно существенно повысить, если покрыть поверхность корпуса слоем вещества с достаточно низкой теплопроводностью (например, абляционным материалом). Падающая на ракету энергия будет поглощаться в тонком слое покрытия, разогревать и уносить его, оставляя основную поверхность не нагретой. Слой абляционного покрытия, например, могут сохранять свои теплозащитные свойства под воздействием потока лазерного излучения почти в течение минуты. По нашим данным, в случае применения абляционных покрытий на основе полиорганосилсесквиоксанов – в течение более часа[157], что превышает время полёта ракеты, то есть неограниченно.

На Западе считают, что уязвимость ракет от лазерного оружия связана с небольшими поверхностными неровностями типа вмятин, царапин и мест соединения металлических панелей, которые могут послужить начальными точками процесса разрушения при воздействии лазерного пучка, хотя при других условиях эти неровности не вызовут ослабления прочности конструкции. Любые неровности обычно являются уязвимым местом, поскольку способствуют концентрации мощности оптического излучения и ослаблению структуры металлов. Даже небольшое загрязнение поверхности может быть опасно, так как повышает коэффициент поглощения энергии лазерного пучка.

Одним из способов преодоления этой проблемы считается полировка поверхности, другая возможность связана с нанесением покрытий с высокими характеристиками отражения. Установлено, что специальные покрытия могут увеличить отражательную способность металлов до 99,1%, хотя в теоретических расчетах эта величина принимается равной 99,8%. Однако это не означает, что такие покрытия обеспечивают неуязвимость крылатых ракет при атаке

---

157 Spector V.N. – Consequences of the synthetic regimes for the solid state reactions of oligoorganosilsesquioxanes with various substrates. Plenary Lecture. In: Proceedings of XI International Symposium on Organosilicon Chemistry. France, Montpelier. 1996

лазерным оружием. Покрытие может загрязниться, но, даже без учёта этого фактора, оно всё же поглощает некоторую часть падающей энергии. Достаточно мощный лазер способен нагреть поверхность цели до таких температур, при которых начнется поглощение более значительного количества энергии.

В США надеются найти способ «остановить» пучок на пути к цели. В определенной степени это может происходить естественным путем, когда лазерный пучок нагревает поверхность настолько, что начинается испарение металла. Некоторая часть паров металла остается над поверхностью, поглощает падающую энергию и образует плазму, которая тоже поглощает энергию лазерного пучка. При достаточно высокой поверхностной плотности излучения эта плазма образует волну, движущуюся навстречу падающему пучку до точки, где мощность лазера уже недостаточна для поддержания её дальнейшего продвижения. Данное явление может предотвращать проникновение энергии лазерного оружия к поверхности цели, вызывая её резкое падение при увеличении выходной мощности лазера. Как было показано на выставке по проблемам конверсии[158], организованной Госпланом СССР для ЦК КПСС и Совета Министров СССР, существуют оптически прозрачные композитные покрытия, способные генерировать плотную плазму при подходе фронта световой волны лазерного излучения, достаточную для полного гашения мощности приходящего на цель излучения встречной волны автогенерируемой плазмы.

Рассмотренный механизм воздействия плазмы может использоваться в средствах противодействия противоракетному лазерному оружию, обеспечивая создание у цели защитного облака плазмы. Военные специалисты Запада исследуют специальные покрытия, которые при облучении лазерным пучком могли бы испаряться с образованием такого защитного слоя. Однако реализация этого способа защиты усложняется тем, что образование плазмы зависит от взаимодействия с окружающей атмосферой, на которое большое влияние оказывает скоростной напор. Независимая проверка показала низкую эффективность абляционного механизма генерирования горячей плазмы.

Определенное влияние на распространение лазерного пучка в атмосфере, возможно, будут оказывать метеоусловия, хотя предполагается, что интенсивные пучки высокоэнергетических лазеров будут проходить сквозь дым, туман, дождь. Однако работы академика Кунцевича позволили создать дымовые завесы, устойчивые к прожиганию.

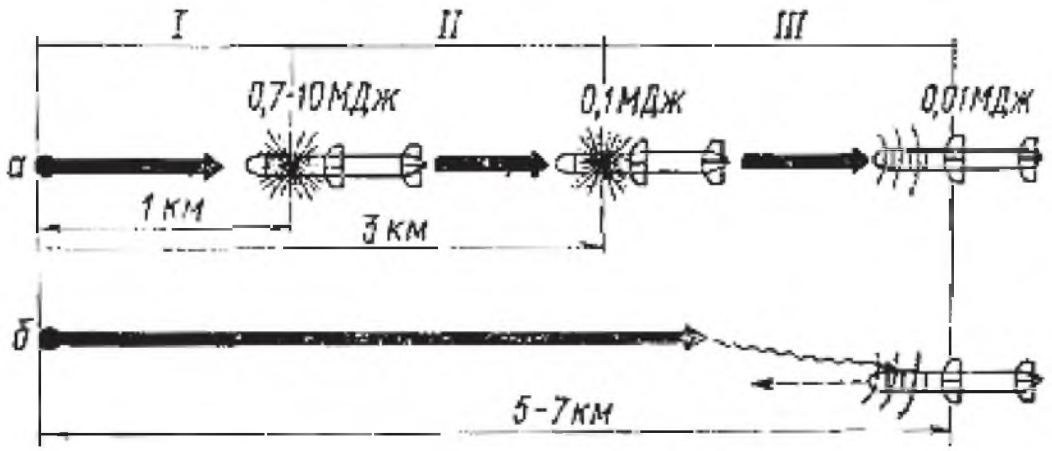
За рубежом проводятся испытания различных методов создания канала в атмосфере с помощью лазеров. В настоящее время эффективность этих методов для повышения характеристик лазерного оружия точно не установ-

158 Степанов Р. Ф., Спектор В. Н. и другие. Оборонный отдел Госплана СССР. М., 1989

лена. Нагрев, необходимый для образования канала в тумане, возможно, окажет влияние на расширение лазерного пучка или вызовет слишком сильную турбулентность, влияние которой нельзя будет скорректировать оптическими средствами. При действии по быстродвижущейся цели, вероятно, потребуется создание новых каналов для каждого импульса лазера или очистка значительного воздушного пространства между лазером и целью. Проблемы могут возникнуть и в том случае, если в процессе образования канала в воздухе появятся материалы, поглощающие лазерное излучение (например, остатки дыма или продукты ионизации от лазерного излучения). В то же время организация расчистки атмосферы для прохождения лазерного пучка может оказаться неэффективной, если система управления лазерным оружием не сможет опознать цель в сложных метеоусловиях.

При организации противодействия лазерному оружию с нанесением по нему ответного удара необходимо подтверждение действия оружия именно такого типа и определение его местоположения. Уже созданы устройства, определяющие облучение цели лазером и направление распространения лазерного пучка. Однако они будут иметь ограниченную эффективность в том случае, если лазер сможет мгновенно уничтожить цель одним импульсом. Для защиты бортовых датчиков от атаки лазерным оружием могут использоваться материалы, меняющие свою прозрачность и отражающую способность под действием лазерного облучения, а также устройства отклонения пучка атакующего лазера.

Несмотря на возможность применения различных средств и способов

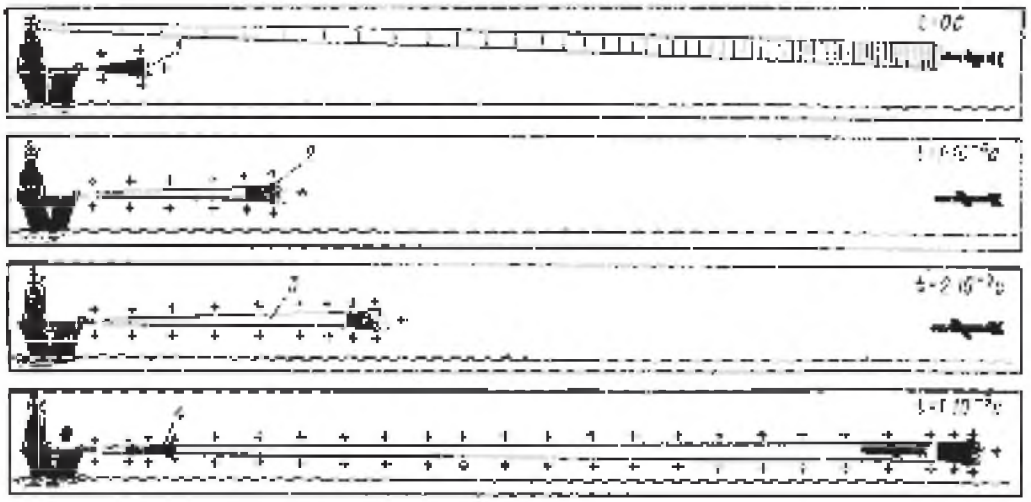


Источник: paralay.com

Рис. Схема воздействия корабельного пучкового оружия на атакующую ракету:

а – прямое воздействие:

I – тепловое воздействие на конструкцию и инициирование ВВ; II – электростатическое инициирование ВВ; III – вывод из строя бортовой электронной аппаратуры: б – косвенное воздействие – повреждение бортовой электронной аппаратуры.



Источник: paralay.com

Рис. Схема применения пучкового оружия для отражения атаки низколетящих ПКР:
1 – луч РЛС обнаружения; 2 – пучок заряженных частиц; 3 – атмосферный канал с разреженным воздухом; 4 – повторный пучок заряженных частиц.

противодействия лазерному оружию со стороны условного противника, американские специалисты полагают, что само его появление внесёт качественный скачок в способы вооружённой борьбы на море. Учитывая высокую энерговооружённость боевых кораблей ВМФ и сравнительно небольшие ограничения по массогабаритным характеристикам (МГХ) бортовых систем вооружения, применение лазерного оружия в спарке: прожигающий канал и атакующий лазер, вероятно, имеет определённые перспективы, хотя такой тип оружия следует скорее отнести к модернизированным традиционным вооружениям, способным действовать в составе перспективных комплексов.

В настоящее время в США начаты поиски путей создания мощного пучкового оружия дальнего действия, характеризуемого почти мгновенным переносом энергии и её глубоким проникновением в цель. Идея его разработки была признана реальной ещё в то время, когда были созданы первые мощные ускорители элементарных частиц, и стало известно, что мощный пучок этих частиц потенциально может нести количество энергии, достаточное для нанесения объёмного механического повреждения твёрдым предметам. Кроме того, пучки частиц вызывают радиационные повреждения, на которые реагируют элементы полупроводниковой радиоэлектроники.

В формировании пучка могут использоваться такие элементарные частицы, как электроны, протоны и нейтроны. Фокусированные нейтронные пучки (хотя фокусировка электрически нейтральных нейтронов без существенной потери мощности представляет собой самостоятельную задачу) наиболее эффективны для уничтожения или вывода из строя экипажа. При большом

числе элементарных частиц выделяемая за короткое время энергия теоретически достигает величины, достаточной для поражения цели.

Простой линейный ускоритель, который может быть использован для создания пучкового оружия, состоит из трёх основных частей: источника частиц, устройства для ввода их в ускоритель и ряда устройств собственно ускорителя. При встрече частиц пучка с целью большая их часть проникает внутрь вещества и проходит через него или поглощается им. При этом каждая частица теряет свою энергию, передавая её электронам вещества. Поскольку происходит серия упругих соударений частиц с электронами, направления движения частиц сохраняются, а энергия, потерянная ими, преобразуется в тепло. Поэтому в месте соприкосновения пучка с целью температура резко возрастает[159]. В результате материал, на который падает пучок, плавится или разрушается вследствие температурных напряжений.

На дальности 1 км для полного поражения ПКР требуется, чтобы импульсы пучка излучения имели энергию 0,7-10 МДж. На дальности 2 км электростатическое инициирование взрывчатого вещества боевой части ракеты обеспечивается при энергии импульса около 0,1 МДж, на дальности 3 км от корабля может быть повреждена электрон-

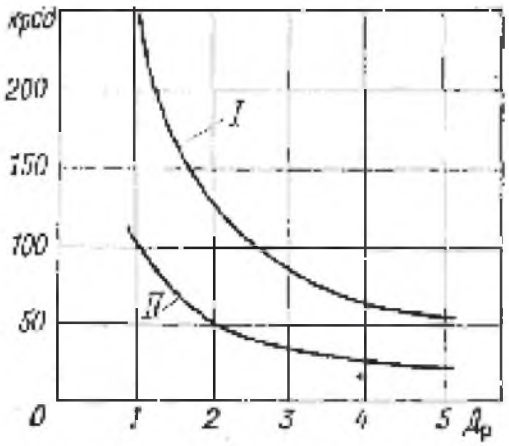


Рис. *Зависимость точности наведения пучка оружия направленной энергии (а) от дальности до ракеты (Др) при её поражении одним импульсом с вероятностью P = 0,865:*
I – диаметр ракеты 1,0 м;
II – диаметр ракеты 0,4 м.

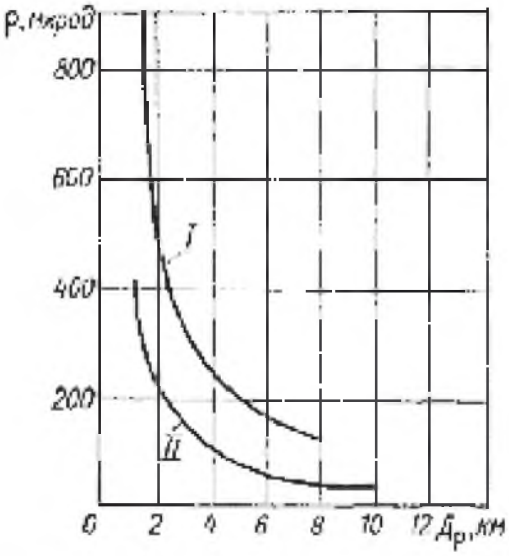


Рис. *Зависимость угловых размеров ракеты (ρ) от дальности до неё (Др):*
I – диаметр ракеты 1 м;
II – диаметр ракеты 0,4 м;
ρ – 200 Дж/г-1

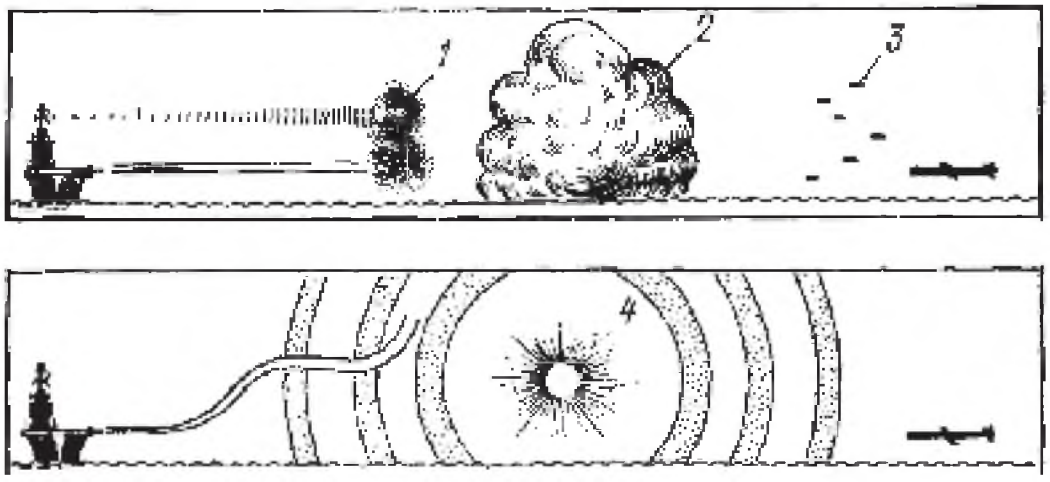
159 Б.И. Радионов и Н.Н. Новичков «Крылатые ракеты в морском бою» Воен. изд-во, 1987

ная аппаратура ракеты при энергии импульса около 0,01 МДж. Повреждение электронной аппаратуры пкр происходит на дальностях 5-7 км от суммарного воздействия электромагнитных импульсов и доз радиации даже тогда, когда пучок не прямо наведен на цель.

В то время, как обычная ракета сближается с кораблем со скоростью, соизмеримой с числом М (мах), разрушительная энергия пучка частиц перемещается в пространстве почти со скоростью света. Именно это свойство и привлекает внимание западных специалистов, видящих в пучковом оружии идеальное средство для борьбы со скоростными целями. Американские специалисты считают технически возможным создание корабельного пучкового оружия для перехвата крылатых ракет в зоне самообороны.

Предполагается, что даже в том случае, если захват дозвуковой ракеты с помощью РЛС обнаружения произойдет на дальности 1 км от корабля, когда до его уничтожения останется 4 с, корабельное пучковое оружие сможет захватить и сбить приближающуюся ракету. Импульсный пучок электронов с энергией1 ГэВ, силой тока в импульсе 5000 А и продолжительностью импульса 0,1 мкс может в принципе создать канал с разреженным воздухом в атмосфере. Через этот канал последующие импульсы могли бы распространяться с небольшим рассеянием заряженных частиц и с минимальными потерями энергии.

Однако, как считают американские специалисты, на многие вопросы относительно свойств распространения пучков заряженных частиц в атмосфере можно ответить, располагая только экспериментальными данными. Энергия, теряемая частицами, будет нагревать воздух в непосредственной близости от пучка. Одновременно вокруг него за счёт ионизации будет созда-



Источник: paralay.com

Рис. Схема противодействия корабельному пучковому оружию:

1 – облако дипольных отражателей; 2 – дымовая завеса;

3 – ложные цели; 4-подрыв фугасного заряда.

ваться большое число положительно заряженных атомов и свободных электронов. Образовавшиеся положительные заряды должны уменьшать электрическое поле частиц в пучке. В то же время самоиндуцируемое магнитное поле (генерируемое потоком электронов) должно преодолевать силы расталкивания частиц, которые обычно рассеивают заряженный пучок в вакууме. Этот эффект должен обеспечить сохранение пучка электронов, удерживаемого устойчивым каналом. Но, как отмечается в иностранной печати, эксперименты показали, что длинные пучки под влиянием указанных причин испытывают магнитодинамические неустойчивости: они запутываются и складываются кольцом, как резиновый шланг. Более того, эти неустойчивости имеют тенденцию к разрастанию до полного разрушения пучка. Выход из положения специалисты видят в том, чтобы пробить в атмосфере канал с разреженным воздухом, через который пучок мог бы распространяться с небольшим рассеянием частиц и с минимальными потерями энергии. Для этой цели, т. е. для «прожигания» канала, предлагается использовать мощное импульсное излучение тех же частиц.

При распространении электронов с энергией 1,0 ГэВ в таком разреженном канале, по расчетам, может теряться не более 20% их первоначальной энергии, а радиус пучка должен увеличиваться втрое после перемещения на 1 км. Для «прожигания» канала считается также реальным использовать высокоэнергетические лазеры.

Американская фирма «Сандиа» продемонстрировала возможность эффективного удержания и прямолинейного распространения пучка электронов в цилиндрическом ионизированном канале, создаваемом ультрафиолетовым лазером. Испытания проводились в камере длиной 1,5 м, наполненной разреженным азотом с небольшой примесью легко ионизирующегося органического газа (диэтиланилина). Сначала луч лазера создал канал ионизированного газа, а через 10^{-9} с в этот канал был введен пучок электронов с энергией 1,5 МэВ из электронного ускорителя. Диаметр пучка изменялся в пределах 0,3-6,0 см.

Американские специалисты считают возможным создание тактического пучкового оружия на основе потока заряженных частиц в сочетании с лазерным излучением. При этом лазерный пучок будет создавать в атмосфере канал для потока заряженных частиц, наводимого на 1 цель.

Трудность создания пучкового оружия западные специалисты связывают с необходимостью разработки для него очень точной системы наведения, которая должна обеспечить угловую ошибку менее одного микрорадиана. Для наведения пучка заряженных частиц возможно применение той же техники, что и для наведения высокоэнергетических лазеров.

Поскольку пучки частиц высокой энергии могут обладать объёмным

характером поражения, то такое воздействие принято характеризовать количеством энергии, поглощенной в единице массы вещества. Типичный уровень поражающего воздействия пучка – мегарад, равный поглощению 10 Дж энергии в грамме вещества. По оценкам иностранных военных экспертов, для выведения из строя электронной аппаратуры ракеты пучковым оружием необходимо воздействие дозы 0,01-1,0 Дж/г$^{-1}$, для разрушения электронной аппаратуры – 10 Дж/г$^{-1}$, для подрыва боевой части и остатков топлива – 200 Дж/г$^{-1}$, для расплавления корпуса из алюминиевого сплава – 1000 Дж/г$^{-1}$. Однако, как полагают западные эксперты, системе ПВО с пучковым оружием можно противодействовать.

Для дезориентации корабельных РЛС можно первоначально создать на определённой дальности от цели облако пассивных помех с помощью дипольных отражателей. Для полной дезориентации корабельной системы ПВО необходимо осуществить запуск специальных ракет – постановщиков дымовой завесы и ложных целей. Дипольные отражатели создадут дополнительный эффект для разрыва импульсного излучения электронов.

Для воздействия на разреженный канал, обеспечивающий распространение пучка электронов, может быть запущена специальная ракета с небольшим фугасным зарядом, после подрыва которого канал резко изгибается и пучок полностью разрушается.

Новые средства борьбы с крылатыми ракетами, основанные на использовании энергии лазерного излучения и пучков элементарных частиц, привлекают к себе внимание наиболее воинственных кругов западных держав, видящих в их создании и внедрении одно из направлений достижения военно-технического превосходства.

ГЛАВА 2
СРЕДСТВА И МЕТОДЫ ИНФОРМАЦИОННОЙ БОРЬБЫ.

Средства и методы ведения информационной борьбы можно подразделить на традиционные, современные и перспективные, а также на пассивные (защитные, оборонительные), активные (направленные на поддержание паритета) и агрессивные (направленные на достижение доминирования).

Традиционные методы информационного противоборства (до середины 50-х годов прошлого века) опирались преимущественно на человеческий ресурс – системный анализ данных и информационных сообщений операторами всех уровней с целью определения системы трендов в информационных мероприятиях потенциального противника, включая выявление дезинформации и ложной информации, и выработка ветви рекомендаций по оптимальному противодействию несущим угрозу информационным акциям для лиц, принимающих решение по стратегии и тактике ответных действий.

Ответные действия традиционно состояли в распространении собственных информационных материалов, включая целенаправленную дезинформацию, публикациями в журналах, газетах и специализированных изданиях, радио- и телепередачами, выступлениями аналитиков на международных форумах и соответствующими дипломатическими акциями. Весьма действенным методом традиционного противоборства была намеренная утечка информации, предназначавшаяся для «случайного» (иногда весьма сложного) попадания в руки агентуры потенциального противника.

Классическим примером такого мероприятия можно считать успешную акцию Абвера накануне Второй мировой войны по доставке в НКВД СССР через третьи страны информации, компрометирующей высший командный состав РККА (маршал Тухачевский и другие). В результате Красная армия лишилась многих имевших боевой опыт командиров и комиссаров и оказалась обезглавленной ещё до начала военных действий. Кроме того, эта акция в значительной мере деморализовала как общество, в какой-то мере утратившее веру в начальствующий состав армии, так и офицеров, опасавшихся принимать самостоятельные решения. Здесь мы не будем обсуждать причины успешности прохождения этой дезинформации, отметим только, что она стоила большой крови Советскому народу. В качестве вывода из этой истории заметим, что объективный анализ информации не допускает личностных мотивов.

Источник: www.ww2history.ru

Иосиф Виссарионович Сталин

Источник: 900igr.net

Михаил Николаевич Тухачевский

Источник: klasnaocinka.com.ua

Олег Владимирович Пеньковский

Пожалуй, основной составляющей традиционных методов информационной борьбы нужно признать систематический сбор максимально полной информации.

Большая, но не всегда достоверная часть информационных данных, собиравшихся традиционными методами, поступала из средств массовой информации и открытых документов (публиковавшихся и частных).

Другим, не слишком стабильным источником информационных данных был радиоперехват и регистрация эмиссии проводов телефонной и телеграфной связи. Обратной стороной этой борьбы было воспрепятствование широкому распространению нежелательной информации среди населения страны потенциального противника радиотехническими средствами – Запад глушил передачи Советского радио, СССР глушил Голос Америки, БиБиСи и другие враждебные голоса.

Однако наиболее надёжным источником получения интересной, как правило, скрываемой информации была агентурная работа, как засылаемых разведчиков-нелегалов, так и вербуемых информаторов.

Так, благодаря предательству Пеньковского[160], расположение пусковых шахт и ракетных установок стратегического назначения стало известно потенциальному противнику, а несколько позже сотрудник организации, разрабатывавшей бортовое радиоэлектронное оборудование, благодаря нарушению золотого правила обеспечения безопасности «no need to know», сумел скопировать и передать за рубеж техническую документацию перспективных разработок КБ им. Сухого.

---

160 ***Олег Владимирович Пеньковский (1919-1963),*** *полковник (разжалован в 1963 г.) ГРУ ГШ Министерства обороны СССР. В 1963 обвинён в шпионаже (в пользу США и Великобритании) и в измене Родине, расстрелян по приговору Военной коллегии Верховного суда СССР. Многие специалисты называют Пеньковского самым результативным агентом Запада из когда-либо работавших против СССР.*

Источник: www.uran.ru

Николай Николаевич Красовский

Источник: ru.wikipedia.org

Юрий Сергеевич Осипов

Источник: www.bolshoyvopros.ru

Владимир Александрович Котельников

Предатели понесли заслуженное наказание, но государство понесло огромные финансовые потери и потери времени. Хотя насчёт наказания Пеньковского не всё так ясно, – в некоторых источниках (например, в полуфантастической книге А.И. Первушина «Битва за звезды: Ракетные системы докосмической эры». Либрусек,. 2005[161]) высказывается мнение, что ему удалось сбежать на Запад.

Вербовка же иностранных специалистов КГБ СССР, и без того бывшая довольно трудным и опасным делом, была осложнена осложнена запретом ЦК КПСС вербовки членов зарубежных коммунистических партий.

Современные методы и средства информационного противоборства (50-е годы – конец XX века) связаны с реализацией научно-технических достижений в математике (например, академики Красовский[162] и Осипов[163]),

---

161 lib.rus.ec›Книги›351340/read

162 ***проф. Красовский Николай Николаевич*** *(1924-2012), академик (математика и механика), доктор физико-математических наук. Герой Социалистического Труда. Почётный гражданин Екатеринбурга. Основатель крупной научной школы по теории оптимального управления и дифференциальных игр. Иностранный член Академии наук Венгрии; Почётный доктор УГТУ-УПИ, Почётный профессор УрГУ. Кавалер Ордена «За заслуги перед Отечеством» II и III степени; Ордена Ленина; Ордена Октябрьской революции; Ордена Трудового Красного Знамени; Золотой медали им. А.М. Ляпунова (РАН); Большой золотой медали им. М.В. Ломоносова (РАН), Золотой медали им. академика С.В. Вонсовского (Уральское отделение РАН); Знака отличия «За заслуги перед Свердловской областью» III степени. Удостоен Ленинской премии; Государственной премии СССР; Демидовской премии; Премии IEEE, премии Фонда содействия отечественной науке в номинации «Выдающиеся учёные».*

163 ***проф. Осипов Юрий Сергеевич (1936),*** *академик (математика, механика), доктор физико-математических наук. Президент Российской академии наук. Член Европейской академии наук и искусств, иностранный член Австрийской академии наук, Венгерской академии наук, Национальных академий наук Армении, Грузии, Казахстана, Киргизстана, Монголии, Таджикистана и Украины. Почётный член Российской академии художеств. Кавалер Ордена «За заслуги перед Отечеством» I, II и III степени, Ордена Александра Невского; французского ордена Почётного легиона, в 2011 году получил звание командора; Командорского ордена (Польша); Ордена Дружбы (Вьетнам); Ордена князя Ярослава Мудрого IV ст. (Украина); Ордена «За заслуги» I и III ст. (Украина); Ордена Святого преподобного князя Даниила Московского I степени; Ордена Святителя Макария; Золотой медали им. Леонарда Эйлера (РАН); Золотой медали им. Эйнштейна (ЮНЕСКО); Золотой медали им. В.И. Вернадского (НАН Украины); Великий офицер ордена «За заслуги перед Итальянской Республикой»; Рыцарь Ордена Белого Креста Всемирной конфедерации Рыцарей (Австралия). Удостоен Ленинской премии, Государственной премии Российской Федерации, Международной премии им. просветителей Кирилла и Мефодия и Демидовской премии.*

в физике атмосферы (например, академик Марчук), в физике твёрдого тела и в полупроводниковой электронике (например, академик Золотов), в радио- и электротехнике (например, академик Котельников[164]), в материаловедении (например, академик Андрианов) и в ряде других перспективных направлениях науки.

Вначале вооружения на новых физических были ошибочно отнесены к нетрадиционному и террористическому оружию[165]. Правда китайские военные специалисты – полковники Кьяо Лянь и Вань Сяньсу оправдывают применение в конфликтах нетрадиционных методов и тактики, что позволит развивающимися странами (в особенности Китаю) компенсировать военное отставание от США. Некоторые рекомендуемые ими меры включают атаки на вебсайты, финансовые учреждения, терроризм, информационную войну в СМИ, войну на улицах городов (Чайна-тауны). Тем не менее, эти вооружения, хотя пока не являются традиционными (скорее, перспективными), но отнюдь не относятся к террористическому оружию.

Это следует и из выводов индийского специалиста – бригадира В. К. Нэйра, который, анализируя уроки конфликта в Персидском заливе для стран третьего мира, описывает существенную американскую военную уязвимость и подчеркивает значение заявления адмирала флота Советского союза Сергея Горшкова: «Следующая война будет выиграна той стороной, которая лучше освоит электромагнитный спектр»[166].

До 1985 года в области информационного противостояния существовал паритет между СССР и США (активная борьба), по крайней мере, в части современных и перспективных средств и методов ведения информационной борьбы. Где-то, например, в психотронных и резонансных вооружениях СССР опережал оппонента, где-то, например, в теоретических и фундаментальных исследованиях взаимодействия электромагнитных излучений

---

164 ***проф. Владимир Александрович Котельников (1908—2005),*** *советский и российский учёный в области радиотехники, радиосвязи и радиолокации планет, академик (радиотехника). Дважды Герой Социалистического Труда. Кавалер Ордена «За заслуги перед Отечеством» I и II степени, 2 Орденов Почёта, 6 орденов Ленина, 2 орденов Трудового Красного Знамени, Ордена «Знак Почёта», Знака отличия «За заслуги перед Москвой». Удостен Большой золотой медали им. М. В. Ломоносова АН СССР, Золотой медали им. А. С. Попова, Золотой медали им. М. В. Келдыша, Золотой медали им. А. Г. Белла, премии Международного научного фонда Э. Рейна (Германия), Ленинской премии, 2 Сталинских премий, премии Совета Министров СССР.*

Теорема Котельникова (1933) *– одна из важнейших теорем теории информации. Была также независимо от него открыта Найквистом и Шенноном. За неё Котельникова на постсоветском пространстве считают «отцом» цифровых технологий в передаче данных. Президент IEEE Брюс Айзенштайн так отозвался о Котельникове: «Академик Котельников – выдающийся герой современности. Его заслуги признаются во всем мире. Перед нами гигант радиоинженерной мысли, который внёс самый существенный вклад в развитие радиосвязи». «Over the years the West had its Shannon; and the East had its Kotel'nikov». Именем В. А. Котельникова назван астероид №2726 (в Международном каталоге циркуляр №9214). Его имя носит военно-морское судно и Институт радиотехники и электроники РАН.*

165 Салливен Джон П. – Террористическое и нетрадиционное оружие. Моркнига. Москва, 2009 (перевод с английского

166 Горшков С. Г. – Морская мощь государства. Военное издательство МО СССР. М., 1976.

Источник: www.famous-scientists.ru

Гурий Иванович Марчук

Источник: ru.wikipedia.org

Кузьма Андрианович Андрианов

Источник: isaran.ru

Евгений Васильевич Золотов

с заряженными оболочками планеты как основы климатического и метеорологического оружия слегка уступал, хотя сами действовавшие установки (программы «Сура», СССР и «Астра», США) имели примерно равную мощность и эффективность.

Кроме того, изначально военная часть программ «Астра», США и «Сура», СССР включали разделы, назначенные на разработку оборудования и методов обеспечения информационной борьбы, в первую очередь радикальное нарушение связи и манипулирование системами управлении потенциального противника всех уровней, вплоть до полевой связи.

Вплоть до начала XXI века геофизические установки типа ХААРП (Аляска, США) и Сура (Российская Федерация), также как аэрокосмические средства принимали сравнительно небольшое участие в информационном противоборстве РФ и США. На этом этапе военных устраивал тот факт, что по утверждению депутатов Госдумы РФ значимость этого качественного скачка в системе вооружений сравнима с переходом от холодного оружия к огнестрельному или от обычного к ядерному. Хотя уже изначально одно из их применений планировалось как средство, направленное на исследование свойств и поведения ионосферы с особым ударением на достижение способности понимать и использовать её для улучшения работы систем связи и наблюдения, как в гражданских, так и, в первую очередь, в военных целях.

Их совершенствование шло преимущественно в отработке и усовершенствовании комплексных систем в качестве климатического и ударного оружия.

Безусловно, помимо этих систем, были значительно усовершенствованы технические средства наблюдения и перехвата, включая аэрокосмические. Однако основной упор делался на развитие методов электронной разведки

Источник: ru.wikipedia.org

Сергей Георгиевич Горшков

и электронной борьбы в компьютерных сетях. КГБ СССР/ФСБ РФ, АНБ, ЦРУ и ФБР США, БНД ФРГ, МИ-5 и МИ-6 Британии, Моссад (Израиль) и другие службы безопасности и разведки изощрялись в совершенствовании электронных и электронно-оптических средств перехвата и наблюдения (наземных/подземных, подводных, атмосферных/стратосферных/ионосферных/космических {геостационарных и мобильных} и средств их подавления (ПДЭТР).

В Википедии приводится определение электронных методов и средств разведки как совокупности методов и организационных структур для ведения разведывательных действий с помощью радиоэлектронных средств (РЭС) и другой электронной техники и достаточно полное раскрытие темы, которое приводится в настоящей работе с минимумом сокращений и поправок.

Источник: u.wikipedia.org

***Менвис-хилл,** объект в Великобритании, который входит в разведывательную систему ECHELON/Эшелон.*

Электронные методы разведки

Радиотехнические методы

Радиоэлектронная разведка (РЭР) – получение информации путём приема и анализа электромагнитного излучения (ЭМИ) радиодиапазона, создаваемого различными РЭС.

Радиоразведка – добывание сведений о противнике путём радиопоиска, перехвата, анализа излучений и радиопеленгования радиоэлектронных средств. Радиоразведка использует такие методы и средства, как:

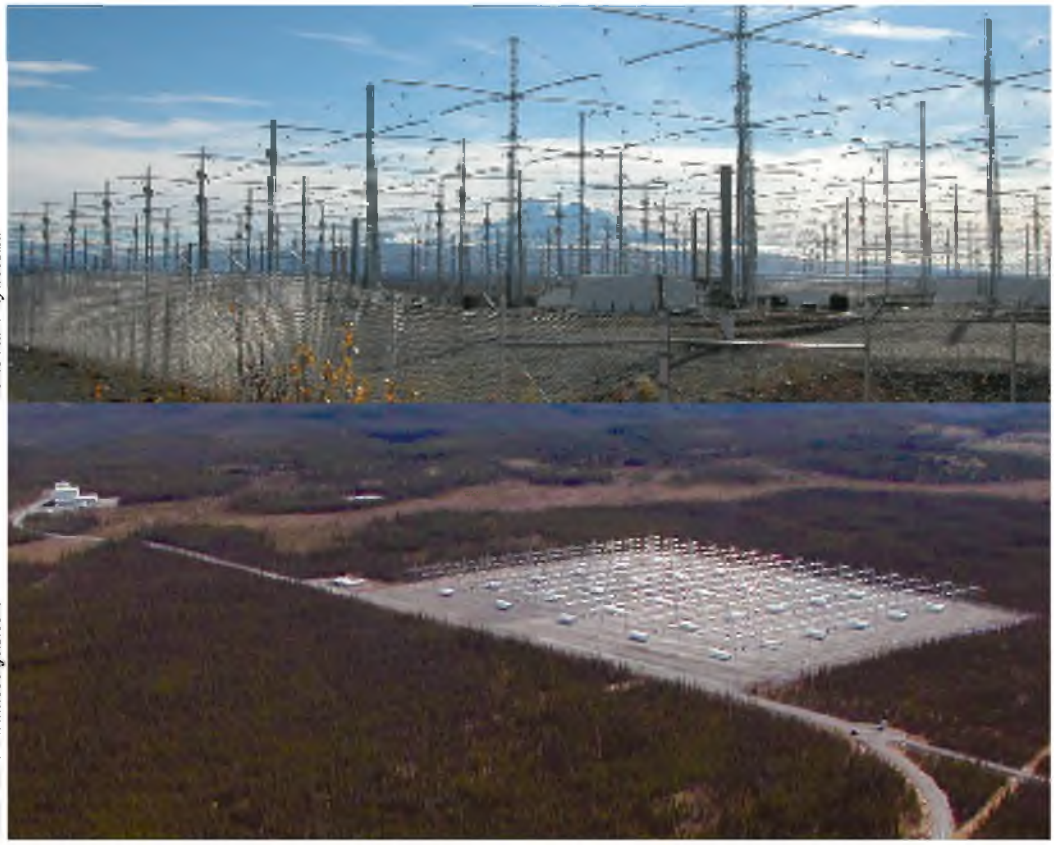
выделение и анализ сигнала из широкополосных линий связи;

фильтрование, обработка и анализ факсов;

анализ трафика, распознавание ключевых слов, получение текста и анализ тем;

системы распознавания речи;

непрерывное распознавание речи;



Источник: mywebs.su

Источник: www.liebenfels.com

***Радиокомплекс «Сура»**, Нижегородская область (57 с. ш., 46 в. д.);*

***Радиокомплекс в Тромсе**, Северная Норвегия: военная база США (проект «Астра»).*

идентификация говорящего и другие методы выбора голосовых сообщений;
снижение нагрузки или подрыв криптографических систем.

Радиотехническая разведка (РТР) – вид разведывательной деятельности, целью которого является сбор и обработка информации получаемой с помощью радиоэлектронных средств о радиоэлектронных системах по их собственным излучениям, и последующая их обработка с целью получения информации о положении источника излучения, его скорости, наличии данных в излучаемых сигналах, смысловом содержании сигналов. Объектами РТР являются: радиотехнические устройства различного назначения (РЛС, импульсные системы радиоуправления, радиотелекодовые системы, а также ЭМИ, создаваемые работающими электродвигателями, электрогенераторами, вспомогательными устройствами и т. п.). Средства РТР устанавливаются на самолётах, спутниках, кораблях, других объектах и позволяют:

- установить несущую частоту передающих радиосредств;
- определить координаты источников излучения;
- измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры), в том числе с использованием прикладных следствий теоремы отсчётов Котельникова;
- установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная);
- определить структуру боковых лепестков излучения радиоволн;
- измерить поляризацию радиоволн;
- установить скорость сканирования антенн и метод обзора пространства РЛС;
- проанализировать и записать информацию.

Радиолокационная разведка – вид технической разведки, в ходе которой информация добывается с помощью радиолокационных станций. РЛС могут быть стационарные наземные, переносные и установленные на самолетах, спутниках, кораблях, других мобильных объектах. Для ведения РЛР применяются:

- РЛС БО (бокового обзора), РЛС ШО (широкополосного обзора), РЛС ПрО (прожекторного обзора), которые устанавливаются на космических и воздушных носителях и используются для получения видовой информации о местности и объектах на ней, над которыми пролетает носитель с аппаратурой;
- наземные и корабельные РЛС, объектами которых являются морские, воздушные и космические цели;
- передвижные и переносные РЛС наблюдения за полем боя, обеспечивающие обнаружение движущихся целей (живой силы и техники) в зоне обзора, приблизительное определение количества целей и скорости их перемещения.

Электронно-оптические методы

Оптоэлектронная разведка – получение информации путём приема и анализа электромагнитных излучений ультрафиолетового, видимого и инфракрасного (ИК) диапазонов, которые создаются или переотражаются объектами разведки.

Фотографическая разведка – получение видовой информации с помощью специальных фотокамер, которые могут быть установлены на космических и воздушных носителях и в наземных условиях.

Телевизионная разведка – получение информации с помощью телевизионных камер.

Инфракрасная разведка – получение информации об объектах при использовании в качестве источника информации либо собственного теплового излучения объектов, либо переотраженного ИК-излучения луны, звездного неба, а также переотраженного излучения специальных ИК-прожекторов подсвета местности. В соответствии с этим все приборы ИКР делятся на 2 группы: тепловизоры, теплопеленгаторы, радиометры; приборы ночного видения (ПНВ).

Фотометрическая разведка – используется для обнаружения и распознавания устройств, в которых используются лазерные источники излучения.

Источник: bastion-karpenko.ru

Современная РЛС с минимизацией излучения в боковые лепестки

Авиационная фотокамера большой дальности, KS-127B (США).

Лазерная разведка – процесс получения видовой информации с использованием лазерных сканирующих камер, которые устанавливаются на воздушных носителях.

Электронно-акустические методы

Акустическая разведка – получение информации путём приёма и анализа акустических сигналов, распространяющихся в воздушной среде от различных объектов. Акустическая разведка осуществляется перехватом производственных шумов объекта и перехватом речевой информации. В акустической разведке используются: пассивные методы перехвата; активные методы перехвата; контактные методы перехвата.

Дистанционное подслушивание разговоров – используется для перехвата речевых сигналов с использованием микрофонов направленного действия, закладок и других средств

Обнаружение и распознавание источников шумового акустического излучения – используется для распознавания источников повышенного звукового давления.

Гидроакустическая разведка – вид технической разведки, в ходе которой добывается информация о противнике путём приема, регистрации, обработки и анализа принятых гидроакустических сигналов. Гидроакустическая разведка позволяет обнаружить и классифицировать морские цели, определить расстояние до них и параметры их движения, то есть получить данные для применения оружия.

Прожектор инфракрасный STS-IR-8015

ИК-прожектор IR-64

Перспективный тепловизор ThermaCAM P65

Fluke Ti25

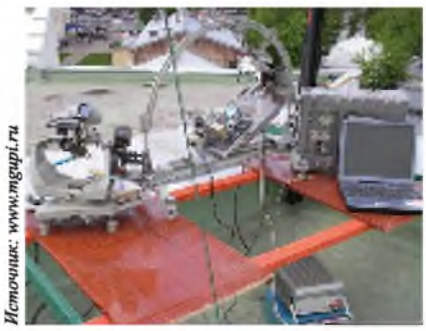
Теплопеленгатор «Кобра» (Ростовский ОМЗ)

Прибор ночного видения Tracker 2x24 LT.

Разные методы с использованием электронных датчиков.

Сейсмическая разведка – получение информации путём обнаружения и анализа деформационных и сдвиговых полей, возникающих в грунте при различных воздействиях на них.

Магнитометрическая разведка – получение информации путём обнаружения и анализа локальных изменений магнитного поля Земли под воздействием объектов с большой магнитной массой.



Источник: www.mgupi.ru

Инфракрасный радиометрический комплекс наземного базирования. (Ростовский ОМЗ)

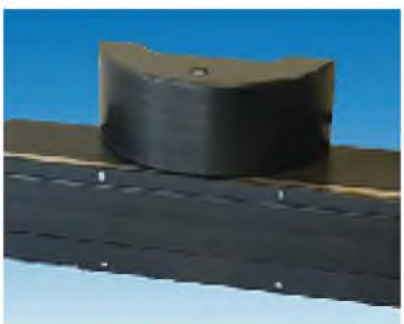
Методы разведки в телекоммуникационных системах.

Разведка в системах телекоммуникаций включает в себя получение несанкционированного доступа к информации, перехват сообщений, перехват данных о кредитных карточках, прослушивание телефонных разговоров в мобильных и проводных сетях, определение географического местоположения владельцев сотовых телефонов, расшифровку закодированных сообщений, отслеживание действия пользователя в разных сетях и многие другие функции.

Лазерная трехмерная сканирующая система Riegl.

Источник: www.spymarket.info

Профессиональный микрофон направленного действия



Источник: www.mns.spb.ru

Многолучевой впередсмотрящий эхолот, *Reson.*

Сетевая разведка – комплекс мероприятий по получению и обработке данных об информационной системе клиента, ресурсов ИС, средств защиты, используемых устройств и программного обеспечения и их уязвимостях, а также о границе проникновения.

Компьютерная разведка (интернет-разведка) – комплекс информационных технологий для систематического нахождения информации в открытых источниках и, возможно, доставки данных в машиночитаемой форме.

Стороны (субъекты и объекты) при ведении электронной разведки

- Одно государство против другого государства
- Государство против потенциально неблагонадёжных граждан и организаций
- Государство или межправительственная организация против преступных сообществ
- Коммерческая организация против других коммерческих и общественных организаций, физических лиц и государственных органов
- Физическое лицо против других физических лиц или организаций
- Преступная организация против других преступных организаций, легальных организаций, физических лиц, а также государственных и международных правоохранительных организаций (Возможны также другие коллизии).

Межправительственные структуры глобального перехвата информации

Система радиоэлектронной разведки «Эшелон» – основное направление – спутниковая РЭР, участники: США, Великобритания, Австралия, Новая Зеландия.

Система объединённого учета данных о противнике (СОУД) – создавалась как объединённая система РЭР стран Варшавского договора, в настоящее время участвует только Россия (данные об участии других стран в открытых источниках не приводятся, можно предположить, что планируется как минимум восстановление подобной структуры в рамках развития ОДКБ).

Enfopol (Enforcement Police) – основное направление – антикриминальная и антитеррористическая разведка в сетях телекоммуникаций, участники: страны Европейского союза

Технические средства электронной разведки

Средства радио- и радиотехнической разведки

- Приёмные антенны направленного и ненаправленного действия
- Радиоприёмники
- Радиопеленгаторы
- Устройства панорамного обзора
- Анализаторы спектра принимаемых сигналов
- Устройства для автоматического отсчёта сдвигов пеленга и частоты
- Выходные устройства для приёма сигналов телефонных и телеграфных
- уплотнённых каналов радиосвязи
- Оконечные устройства слухового приёма (телефоны, динамики)
- Устройства документирования сигналов
- Приборы расшифровки, обработки и хранения принятой информации
- Средства управления, связи и передачи добываемой информации.

Средства съёма акустической информации

Средства, устанавливаемые заходовыми (то есть требующими тайного физического проникновения на объект) методами:

- радиозакладки;
- эндовибраторы
- закладки с передачей акустической информации в инфракрасном диапазоне;
- закладки с передачей информации по сети 220 В;
- закладки с передачей акустической информации по телефонной линии;
- диктофоны;
- проводные микрофоны;
- «телефонное ухо»

Средства, устанавливаемые беззаходовыми методами:

- аппаратура, использующая микрофонный эффект;
- высокочастотное навязывание;

- стетоскопы;
- лазерные стетоскопы;
- направленные микрофоны.

Автоматические дистанционные датчики для обнаружения людей и техники

- Сейсмические датчики
- Радиодатчики
- Акустические датчики
- Химические датчики
- Магнитные датчики
- Контактные датчики.

Средства негласного перехвата и регистрации информации с сетей телекоммуникаций

- Средства съёма информации с кабелей связи
- Системы перехвата сигналов с компьютерных сетей и контроля телекоммуникаций
- Системы контроля телексной связи
- Аппаратура перехвата факсимильных сообщений.

Оптоэлектронные средства

- Приборы ночного видения
- Комплекты для ночного наблюдения и видеосъёмки
- Специальные фото и видеокамеры с пин-холовской оптикой
- Носимая техника негласного видеоконтроля с радиоканалом
- Миниатюрные системы фото и телемониторинга.

Прочие электронные средства

- Ретрансляторы
- Специальные технические средства для негласного контроля перемещения
- транспортных средств и других объектов
- Радиозакладки для компьютеров и оргтехники
- Средства контроля побочных излучений от ЭВМ.

Примеры существующих электронных средств разведки

- Мобильная автоматическая станция радиотехнической разведки 85В6Е
- Авиационная станция телевизионной разведки И-249Б
- Комплекс радиотехнической разведки Р-381Т
- РЛС ближней разведки **СБР-3 «ФАРА»**
- Станция гидроакустической разведки **AN/WLR-9B**
- Микропередатчик клавиатуры **OF1122**
- Факсимильный радиопередатчик **4305-TAX4**
- Супер теле- фото камера **РК-6500** (ФРГ)
- Наручные часы – камера **РК-420** (ФРГ)
- Радиомикрофон с цифровым (шумоподобным) сигналом **ТХ – 815/865**
- Westinhouse, США)
- Проводная система акустического контроля с использованием электросети Сеть – **IP (PTLS4)**
- Направленный микрофон **РН – 470**
- Авиационная аппаратура лазерной разведки **Л-140**

Использованный в настоящей работе обзор (Википедия) средств и методов информационной борьбы, к сожалению, в большей мере относится к классическому варианту, но столь же полного обзора, опирающегося на весьма основательную литературную базу[167] и перекрёстных ссылок на другие источники технической справочной информации, по-видимому, на сегодняшний день в русскоязычной литературе найти не удаётся.

Недостаточное внимание к современным методам и средствам информационной борьбы/войны, можно объяснить разными причинами.

1) большинство современных методов и средств этой борьбы является усовершенствованием либо глубокой модернизаци – ей традиционных. 2) в предвкушении кардинальных изменений, связанных с разработкой и успешными натурными испытаниями перспективных систем информационной борьбы, применение современных средств постепенно передаётся в воинские подразделения низшего звена, в службы безопасности крупных корпораций, в частные охранные предприятия, частные сыскные бюро,

---

167 Вартанесян В.А. – Радиоэлектронная разведка. М.: Воениздат, 1975; Демин В.П. и др. – Радиоэлектронная разведка и радиомаскировка. М.: Изд-во МАИ, 1997; Лагутин В.С., Петраков А.В. – Утечка и защита информации в телефонных каналах. М.: Энергоатомиздат, 1996; Мельников Ю.П. – Воздушная радиотехническая разведка. М.: Радиотехника, 2005; Меньшаков Ю.К. – Защита объектов и информации от технических средств разведки. М.: РГГУ, 2002. ISBN 5-7281-0487-8; Радзиевский А.Г., Сирота А.А. – Теоретические основы радиоэлектронной разведки. М.: Радиотехника, 2004; Хорев А.А. – Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998; Энциклопедия «Оружие и технологии России. XXI век», т. т. 10, 11 и 13

Источник: blogs.privet.ru

Автоматизированная станция 85В6Е «ОРИОН».

Источник: digitalcombatsimulator.com

Аппаратура лазерной разведки Л-140 «Отклик»

Источник: www.sis-tss.ru

Скоростной анализатор спектра Скорпион V3.0

Источник: russianarms.mybb.ru

комплекс радиотехнической разведки Р-381Д «Рама».

Источник: spetzradio.ru

Пункт радиотехнического контроля Охота

Источник: www.secur.su

Портативный персональный индикатор поля BugHunter

Для станковых пулеметов ПКМСН, НСВС-12,7 «ФАРА-1» обеспечивает:

- *Автоматическое обнаружение движущейся цели на охраняемых рубежах и наведение оружия на цель.*
- *Эффективную стрельбу по движущейся цели в условиях отсутствия оптической видимости.*
- *Повышается эффективность штатного ночного прицела пулемета НСВС-12,7НЧ*

в частные военные компании, формирования наёмников или попадает в руки международных террористических сообществ и структур организованной преступности.

3) на геополитическом поле резко изменился характер информационного противостояния США и СССР/РФ. Если до 1985 года в условиях при мерного, хотя и асимметричного паритета превалировало активное противостояние этих стран и возглавляемых ими военно-политических блоков – НАТО и ОВД, то, начиная с 1985 года, наблюдалось постепенное разрушение паритета и дивергенция подходов к ведению информационной войны СССР/РФ.

В то время как США проводя агрессивную информационную борьбу, стремились к доминированию и господству в мире, СССР, напротив, скатывался к пассивным формам, при этом, не используя даже традиционные средства в полном объеме. Тем самым, Советский Союз сам решил свою судьбу. Вместо эволюционного перехода на качественно новый уровень – гуманизации большевизма и перехода страны к системе народной демократии, партия, ведомая престаревшим руководством, предавала идеологию, скреплявшую новую человеческую общность – советский народ, и сдавала международные позиции этой новой общности. По сути дела, для диверсифицированной и, в основном, самодостаточной экономики СССР, падение цен на нефть конца 80-х годов не было катастрофой, всего лишь крупной неприятностью, связанной с системными перекосами и организованной противником по информационной борьбе. Подобную, даже более фундаментальную неприятность, связанную с повышением цен на нефть в 70-х годах, США и их союзники по НАТО пусть с трудом, но пережили.

Источник: www.bati.ru

Мобильная станция радиомониторинга, пеленгования и контроля радиоканалов АРК-МС1И (АРГУМЕНТ-И) и технологический отсек станции.

На фоне сдачи позиций СССР, которые в большей части проявились в ведении информационной войны и поражения в ней, и памятуя о ряде предыдущих фундаментальных ошибок руководства КПСС, связанных с «развенчанием» культа личности Сталина (практически все ком –

мунистические партии за исключением Китая испытали резкое уменьшение своих рядов, например, КП Великобритании потеряла более 50% членов партии), Берлинская стена, события в Венгрии, Чехословакии и в Польше, расстрел рабочих в Новочеркасске – произошёл распад СЭВ и ОВД. Это сопровождалось ростом антисоветских/антироссийских настроений не без помощи западной пропаганды.

Драматический распад СССР (1991) с многомиллионными демонстрациями в Москве, Ленинграде и в столицах союзных республик (с применением войск для их подавления), который сопровождался ростом национализма, оставил Россию один на один с США и их союзниками, в том числе и в информационном противостоянии.

Взгляды высшего военно-политического руководства ведущих иностранных государств на противодействие угрозам кибернетических войн.

В современных условиях информация превратилась в важный ресурс, определяющий состояние национальной безопасности государства. США, Китай, Япония и другие технологически развитые государства, используя свое преимущество в производстве аппаратного и программного обеспечения для вычислительной техники, средств телекоммуникации и связи, стремятся к полному доминированию в мировом информационном пространстве. Для реализации этой доминанты планируются и проводятся информационные операции, а в ряде случаев и информационные войны[168].

«Президент США Дж. Буш, выступая 20 марта 2001 года перед сотрудниками Центрального разведывательного управления в штаб-квартире ЦРУ в Лэнгли, уже в то время перечислил главные угрозы безопасности Соединённых Штатов. На втором месте после терроризма в этом перечне значится информационная война. И уже за ней – распространение оружия массового уничтожения и средств его доставки. Как считают американские военные специалисты, на повестку дня поставлен вопрос о переносе акцента в вооруженном противоборстве с традиционных его форм ведения (огонь, удар,

168 Тараскин М.М. (доктор технических наук, доцент, заместитель начальника управления войсковой части 61535, полковник), Чешуин С.А. (заместитель начальника кафедры зарубежной военной информации Военного университета, полковник) – Взгляды высшего военно-политического руководства ведущих иностранных государств на противодействие угрозам кибернетических войн (научные материалы НИЦ). Бюллетень «Проблемы безопасности» №3 Научно-исследовательского центра «Наука-XXI»

маневр) в информационно-интеллектуальную и информационно-техническую сферы, то есть туда, где подготавливаются, принимаются и реализуются военные и политические решения. Будущая война может быть спровоцирована в информационной сфере, которая будет охватывать политическую, экономическую, техническую и военную области»[169].

Впервые о возможности войны в информационной сфере заговорили в середине 90-х г. XX века. В конце 1996 года на одном из симпозиумов представитель МО США Роберт Банкер представил доклад, посвященный новой военной доктрине вооружённых сил США XXI столетия (концепции «Force XXI»). Ключевым моментом в ней является разделение всего театра военных действий на две составляющих – традиционное пространство и киберпространство, причем последнее имеет более важное значение. Банкер предложил доктрину «киберманевра», которая должна стать естественным дополнением существующих военных концепций, преследующих цель нейтрализации или подавления вооружённых сил противника.

В число сфер ведения боевых действий помимо земли, моря, воздуха и космоса было предложено включить и ионофосферу. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психология противника (появился даже термин «human network»/человеческие сети)[170].

«Под информационным противоборством (Information Warfare, IW) понимается комплексное воздействие на систему государственного и военного управления противоборствующей стороны, на её военно-политическое руководство, а также защита своих информационных объектов от подобного воздействия. В принципе это воздействие должно ещё в мирное время способствовать принятию благоприятных для стороны – инициатора информационного давления решений, а в ходе конфликта полностью парализовать функционирование инфраструктуры управления противника.

Основными руководящими документами США в области организации и ведения информационного противоборства являются:

– Национальная стратегия по физической защите критической инфраструктуры и объектов национального достояния (2003), в которой сформулированы цели и принципы обеспечения безопасности национальной инфраструктуры США, а также определены условия объединения усилий различных государственных и частных структур по повышению степени их защищенности.

---

169 Защита информации и информационная безопасность: учебник/Соловьев А.А., Метелев С.Е., Зырянова С.А. – Омск: Изд-во Омского института (филиала) РГТЭУ, 2011.

170 Горбачев Ю.Е., Тюрин В.М. – К вопросу о «войне в четвертой сфере». Независимое военное обозрение. 20 апреля 2001

– Национальная стратегия по защите киберпространства (2003) охватывает область обеспечения защиты технических и программных средств, объединенных в компьютерные сети, и систем решения задач управления и информационного обеспечения на различных уровнях государственных, общественных и частных структур, в том числе в различных сферах национальной экономики. Главная цель этой стратегии – предотвращение компьютерных атак против объектов критической инфраструктуры, снижение их эффективности, а также максимальное сокращение периода ликвидации последствий нападения на компьютерные сети.

– Национальная военная стратегия по проведению кибероперациий (2006), где определяются основные направления и сферы действий киберсообщества США в киберпространстве.

– Доктрина информационных операциё (2006), в которой представлены взгляды военного руководства США на подготовку и ведение такого рода операций вооружёнными силами, уточнены цели, задачи и основные принципы информационного противоборства, а также обязанности должностных лиц по подготовке и проведению информационных операций как в мирное, так и в военное время. В соответствии с новыми взглядами информационные операции представляют собой комплекс мероприятий, проводимых ВС США по воздействию на людские и материальные ресурсы противника с целью затруднить или сделать невозможным принятие им верных решений с одновременной защитой своих информационных систем.

В данном документе впервые официально упоминаются «сетевые операции», которые включают в себя компьютерные сетевые атаки/Computer Network Attacks, сетевую защиту/Computer Network Defense, использование компьютерных сетей противника в своих целях/Computer Network Exploitation[171].

Информационное противоборство предполагает проведение мероприятий, направленных против систем управления и принятия решений/Command & Control Warfare, C2W, а также против компьютерных и информационных сетей и систем/Computer Network Attacks, CNA.

Деструктивное воздействие на эти системы достигается с помощью: психологических операций/Psychological Operations, PSYOP, направленных против персонала и лиц, принимающих решения; радиоэлектронной борьбы/Electronic Warfare, EW – против средств управления, связи и радиотехнического обеспечения; сетевых операций/Computer Network Operations, CNO; мероприятий по оперативной маскировке/Military Deception и по обеспечению безопасности собственных сил и средств/Operations Security.

---

171 Костюхин А. А., Горбунов Г. С., Сажин А. А. – Информационные операции в планах командования ВС США. Информационный сборник ГШ ВС РФ по зарубежным странам и армиям Центра зарубежной военной информации и коммуникации. 2006, №3 (160), с. с. 5,6

Вспомогательными элементами информационных операций, по взглядам военно-политического руководства США, являются: обеспечение безопасности информации/Information Assurance; физическое уничтожение/Physical Attacks критически важных информационных структур противника и контрразведка/Counterintelligence.

Концепциями информационного противоборства предусматриваются, прежде всего,, несанкционированные воздействия (НСВ) в виде подавления (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления), а также осуществление несанкционированного доступа (НСД) к информационным ресурсам (благодаря использованию программно-аппаратных средств прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением или хищением либо нарушение нормального функционирования этих систем. Кроме того, предполагается: электромагнитное воздействие на элементы информационных и телекоммуникационных систем (радиоэлектронная борьба); получение разведывательных данных в результате перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счёт специального внедрения технических средств перехвата информации и другие мероприятия.

Во «Всестороннем обзоре состояния и перспектив развития ВС США», который был представлен министром обороны США 06.02.2006 президенту и конгрессу в разделе «Силы стратегического сдерживания скорректированного состава – новая триада» в контексте организации информационного противодействия на Объединённое стратегическое командование (ОСК) ВС США возложено проведение глобальных операций в компьютерных сетях. Для качественного их выполнения намечено:
– выделить дополнительные инвестиции на развитие средств обеспечения защиты информации и защиты компьютерных сетей МО США;

– усилить координацию действий различных сил и средств министерства обороны при проведении ими наступательных и оборонительных компьютерных операций;

– на основе опыта отражения компьютерных атак при эксплуатации компьютерных сетей повысить уровень их защищенности и реализовать принцип эшелонирования при планировании мероприятий по защите информации.

Планирование и реализация операций в глобальных компьютерных сетях осуществляются в соответствии с концепцией «Сетецентрические операции»/«Net-Centric Operations» (Сетецентричность определяется как возможность использования преимуществ информационного взаимодействия).

Основой для сетецентричных операций является глобальная информационно-управленческая сеть (ГИУС) Гиг/Global Information Grid, представляющая собой набор взаимосвязанных высокозащищенных локальных информационных сетей. ГИУС оптимизирует процессы сбора, обработки, хранения, распределения информации и управления ею, а также доведение её до потребителей внутри министерства обороны и за его пределами. С её помощью осуществляются как административное, так и оперативное управления вооружёнными силами США. Головным ведомством, отвечающим за работоспособность и защиту Глобальной информационной сети министерства обороны назначено Объединённое стратегическое командование (ОСК) ВС США.

Элементы ГИУС развёртываются на земле, в воздухе, космосе и на море. Подсистемами ГИУС являются автоматизированные системы управления, построенные на базе глобальных и локальных информационных сетей аппарата министра обороны, Комитета начальников штабов (КНШ), разведывательного сообщества США, видов вооруженных сил, объединенных командований и других структурных подразделений министерства обороны. ГИУС «Гиг» имеет открытую архитектуру, единый комплекс стандартов представления данных и обмена ими, унифицированное программное обеспечение и аппаратные средства, что позволяет осуществлять её дальнейшее наращивание и обеспечивает общий доступ к базам данных различной принадлежности (рисунок).

Важнейшими компонентами ГИУС «Гиг» являются глобальная система оптоволоконных линий связи, система космической связи и сеть наземных ретрансляторов (телепортов), объединяющих эти две системы. В глобальной

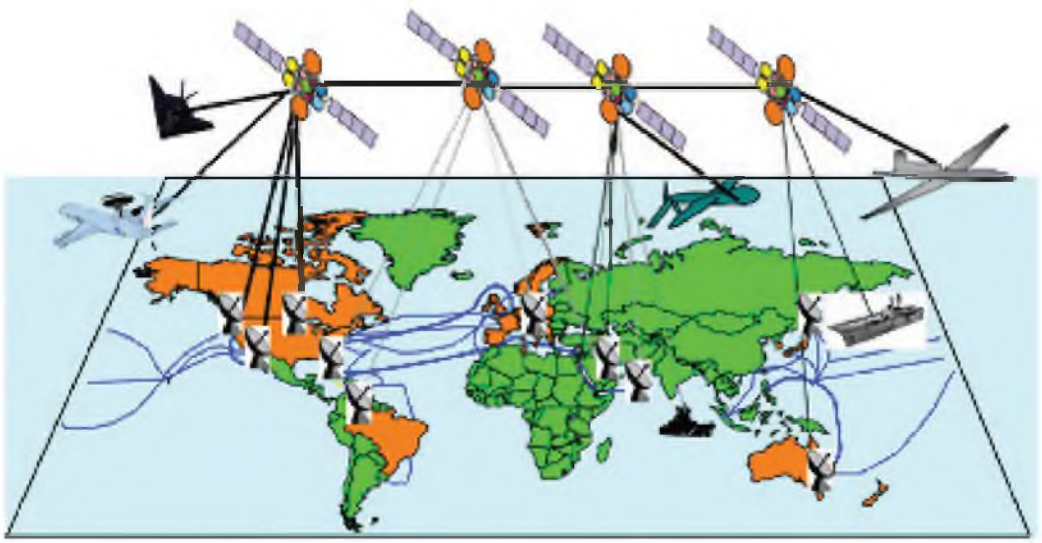


Рисунок. *Концепция построения ГИУС ВС США «Гиг»*

информационно-управленческой сети используются унифицированные средства радиосвязи, для чего привлекаются спутниковые системы, авиация, беспилотные летательные аппараты и надводные аппараты, а также действует единая система обеспечения информационной безопасности.


Источник: investigator.org.ua

Сулейман Анил

Американской программой FCS/Future Combat System предусматривается поступление в войска уже в ближайшие годы индивидуальных боевых комплектов, которые будут подключаться к ГИУС. Их основу составят компьютеры, позволяющие солдатам вести наблюдение за полем боя, поддерживать связь с командирами и своими боевыми товарищами, управлять огнём из наличных боевых средств. Удар по компьютерным сетям нарушит связь между командирами и подчиненными, то есть подорвет боеспособность американской армии на самом её низшем уровне. И это лишь одно из последствий возможных сетевых компьютерных атак (кибератак) по управленческим сетям вооружённых сил противника.

Исходя из этих факторов, можно сделать вывод, что целенаправленная и массированная кибератака может быть проведена за минуты, секунды и даже тысячные доли секунды, в то время как современным системам вооружений требуются недели, а то и месяцы подготовки. Более того, её (т. е. спланированную кибератаку), по мнению руководителя координационного центра реагирования на компьютерные инциденты НАТО Сулеймана Анила, практически невозможно пресечь. «Кибернетическая война может быть весьма эффективной, потому что не сопряжена с большим риском для тех, кто нападает, не требует больших затрат, её поражающий эффект велик, а «оружие» можно быстро и легко разместить в любом месте планеты. Это почти идеальное оружие, которое нельзя игнорировать», – сказал Анил.

Таким образом, решение задач управления вооружёнными силами США в современных условиях осуществляется в рамках сложившейся ещё в конце XX века, активно усовершенствуемой и достаточно эффективно функционирующей в настоящее время системы стратегического руководства. Она имеет чёткие организационно-функциональные разграничения структурных компонентов и принципов управления (административного и оперативного) и представляет собой единство высших государственных (гражданских) и военных органов, различных технических систем и средств, обеспечивающих деятельность Национального военного руководства США по управлению вооружёнными силами,

как в мирное, так и в военное время. Однако её слабым элементом является открытая архитектура, что открывает возможности внешних воздействий.

Каким же образом предполагается осуществлять защиту в компьютерных сетях?

В начале 2008 года президент США Дж. Буш подписал две секретные директивы №54 (Директива президента по национальной безопасности) и №23 (Директива президента по внутренней безопасности). В этих документах спецслужбам США и, прежде всего, Министерству внутренней безопасности (МВБ), а также Агентству национальной безопасности (АНБ) даются указания по усилению контроля компьютерных сетей, используемых американскими федеральными структурами. Кроме того, заокеанские разведчики и контрразведчики должны расширить сферы мониторинга информации, поступающей в сети правительственных ведомств Соединённых Штатов через Интернет[172].

После подписания Бушем новых директив, под руководством директора национальной разведки США была создана специальная структура, которой предписано осуществлять координацию усилий американских спецслужб по вскрытию источников кибернетических атак на федеральные информационные системы. МВБ будет обеспечивать защиту этих систем. А Пентагону (ОСК ВС США) надлежит разработать стратегию противодействия всем попыткам извлечения данных, потеря которых может повредить национальной безопасности страны.

За последние полтора года сети Государственного департамента, Министерства торговли, Минобороны и МВБ США неоднократно подвергались атакам хакеров и зарубежных спецслужб. Чиновники в Вашингтоне и специалисты по компьютерной безопасности утверждают, что крупнейшие атаки на эти ведомства, включая базы данных некоторых лабораторий, занимающихся ядерными разработками, и крупных подрядчиков МО, были предприняты Китаем.

Новыми директивами Буша Пентагону разрешается разрабатывать планы проведения кибернетических контратак на информационные сети противников США. В тех случаях, когда АНБ будет установлен конкретный факт нападения и выявлен сервер иностранного государства, с которого была осуществлена атака, специалисты Минобороны нанесут по нему ответный удар, чтобы прекратить новые атаки на информационные сети американского правительства[173]. Такие же меры будут приниматься и в тех случаях, когда атакам будут подвергаться сети частных фирм.

В начале марта 2008 года в США состоялись учения под кодовым назва-

---

172 Иванов В. – Контрразведывательные операции в киберпространстве. Независимое военное обозрение, 8 февраля 2008

173 Пентагону в случае обнаружения угрозы поручено контратаковать и выводить из строя сервер-нарушитель. Готовясь к выполнению этой задачи, министерство обороны США создало на базе ВВС в Барксдейле (штат Луизиана) новое командование, предназначенное для ведения кибервойны

нием «Кибернетический ураган-2». Их проводило МВБ с участием 18 федеральных ведомств, в том числе ЦРУ, ФБР, МО (ОСК ВС США) и АНБ, представителей девяти американских штатов и свыше трёх десятков частных компаний, а также соответствующих служб Австралии, Великобритании, Канады и Новой Зеландии. Командный пункт учений располагался, как сообщается, в штаб-квартире секретной службы США, которая отвечает за безопасность главы государства и структурно входит в состав МВБ. «Вероятный противник» не обозначался, однако считалось, что он преследует политические и экономические цели и для их достижения предпринял мощную кибератаку против компьютерной инфраструктуры страны. В ходе учений участники отрабатывали совместные действия, призванные дать отпор этому нападению.

Учения «Кибернетический ураган-2» стали ещё одним свидетельством разворачивающейся в США подготовки к ведению кибервойн. Об опасности их развязывания в будущем утверждали <…> на Западе уже давно. Однако, то, что эта война не такая уж виртуальная, а главное, что её последствия могут быть не менее катастрофическими, чем от ракетной, заговорили в США и НАТО со всей серьёзностью[174]. Активному воздействию в этот период подвергались информационные сети Эстонии, США, Германии, Франции, Великобритании и Южной Кореи»[175].

На сайте Washington Profile сообщается, что сегодня в мире еженедельно регистрируются более 55 миллионов акций компьютерных хакеров как успешных, так и безуспешных. Ущерб от них составляет более 15 миллиардов долларов ежегодно и продолжает быстро расти. Наиболее распространенный способ действия хакеров – блокировка корпоративной сети или интернет-ресурса избранного объекта с помощью DDoS-атаки (Distributive Denial of Service/отказ в обслуживании).

«Суть его состоит в том, что в необходимый момент хакеры по команде начинают забрасывать выбранный ресурс тысячами ложных запросов (спамов) в секунду. Это приводит или к выходу из строя сервера, подвергшегося атаке, или к прекращению доступа к нему другим пользователям.

Скоординированная рассылка американскими хакерами в течение нескольких дней более 500 тысяч писем привела к полному выводу из строя правительственного сайта Югославии. В то же время представитель НАТО Джими IIIи отмечал, что их почтовый сервер длительное время получал ежедневно более 2 тысяч посланий только от одного отправителя[176].

---

174 Сидоров В. – Кибервойны: от дождя к урагану. Красная Звезда. 26 марта 2008

175 Защита информации и информационная безопасность: Соловьев А.А., Метелев С.Е., Зырянова С.А. – Омск: Изд-во Омского института (филиала) РГТЭУ, 2011.

176 Польских А. – О применении глобальной компьютерной сети Интернет в интересах компьютерного противоборства. Зарубежное военное обозрение. 2005, № 7, с. с. 2,3

Хакеры в своих атаках на киберпространство используют также рассылку ложных писем, направляющих пользователя на поддельный ресурс, внешне напоминающий оригинальный, и внедрение крадущих информацию вирусов – «троянов». Последние, получившие своё название от «троянского коня», обычно перехватывают нажатия клавиш, могут делать копии экрана пользователя или копировать данные, посылаемые пользователем через сеть, затем полученная информация направляется по нужным адресам.

Информационный конфликт как форма взаимодействия информационных систем применительно к вычислительным сетям характеризуется преднамеренным характером воздействий нарушителя.

При этом его объектами становятся как информация, хранимая, обрабатываемая и передаваемая в интересах решения прикладных задач пользователей, так и сами вычислительные сети, т. е. все доступные для воздействия ресурсы.

Обеспечение безопасного функционирования вычислительных сетей в таких условиях связано с защитой от более широкого спектра угроз безопасности информации и со специфичным распределением таких угроз по элементам вычислительной сети. В качестве основной формы воздействия на вычислительные сети со стороны нарушителя выступают компьютерные атаки (КА), защита от которых для обычных условий функционирования вычислительных сетей, как правило, не рассматривается или рассматривается как второстепенная задача по защите от вирусов.

Следовательно, специфика условий информационного конфликта определяет необходимость контроля реальной защищенности вычислительных сетей от КА и поиска эффективных решений для защиты от них.

Объективной реальностью в развитии теории и практики защиты информации в вычислительных сетях стало появление нового вида глобальных угроз безопасности их функционирования – информационного оружия, с помощью которого реализуются задачи информационного противоборства.

В общем случае под информационным оружием понимается совокупность средств и способов воздействия на информацию, информационно-психологические, информационно-технические объекты и информационный ресурс в целях решения задач воздействующей стороны[177].

Другими словами, это сплав специально организованной информации и информационных технологий, позволяющий целенаправленно преодолевать систему защиты, воздействовать на информацию или нарушать нормальное функционирование информационно-вычислительных систем.

---

177 Словарь терминов и определений в области информационной безопасности. НИЦ «Информационной безопасности» ВА ГШ ВС РФ. М., 2008, с. с. 47, 48

Применительно к вычислительным сетям информационная борьба представляет собой особую форму конфликта с активным воздействием нарушителя и пассивным поведением системы защиты вычислительной сети. В подобных условиях, называемых далее условиями информационного конфликта, обеспечение безопасности функционирования вычислительной сети предполагает защиту обрабатываемой в вычислительной сети информации от НСД со стороны нарушителя, а также защиту самой вычислительной сети от НСВ со стороны нарушителя, направленных на нарушение её функционирования. Применительно к условиям информационного противоборства термин «защита информации от НСД» [178]включает в себя все аспекты обеспечения безопасности информации:

– конфиденциальность (защита от несанкционированного чтения или копирования);

– целостность (защита от несанкционированного изменения или удаления);

– доступность (защита от несанкционированного блокирования).

Основной формой информационного воздействия нарушителя на ресурсы вычислительной сети являются КА, представляющие собой упорядоченные во времени действия по преодолению системы защиты и нарушению безопасности информации, реализуемые посредством программ с потенциально опасными (деструктивными) функциями. К числу таких функций относятся:

– сокрытие признаков своего присутствия в программно-аппаратной или вычислительной среде;

– осуществление сбора данных о параметрах вычислительной сети и о системе ее защиты;

– самодублирование или перенос своих фрагментов в другие области оперативной или внешней памяти;

– ассоциирование с другими программами в вычислительном окружении;

– искажение или разрушение кода программ в оперативной памяти;
– сохранение фрагментов информации из оперативной памяти в некоторой области внешней памяти (локальной или удаленной);

– искажение, блокирование или подмена выводимого во внешнюю память или в канал связи массива информации, образующейся при выполнении прикладных программ;

– подавление информационного обмена в телекоммуникационных сетях;

– искажение или фальсификация информации при обмене по каналам телекоммуникационных сетей;

---

178 Несанкционированный доступ – первичное действие в ходе компьютерной атаки, так как без него невозможна организация несанкционированного воздействия

– нейтрализация или нарушение работы тестовых программ и системы защиты.

В случае успеха КА реализуются одна или несколько угроз безопасности функционирования вычислительной сети, то есть потенциально возможное событие, процесс или явление, которые посредством воздействия на информацию или другие компоненты вычислительной сети могут прямо или косвенно привести к нарушению безопасности информации.

В зависимости от принадлежности источника угрозы выделяют внутренние и внешние угрозы безопасности функционирования вычислительной сети. Основным источником внутренних угроз являются высококвалифицированные специалисты в области разработки и эксплуатации программного обеспечения (ПО) и технических средств, знакомые со спецификой решаемых в автоматизированной системе (АС) задач, структурой, основными функциями и принципами работы программно-аппаратных средств защиты информации, имеющие возможность использования штатного оборудования и технических средств сети.

В зависимости от конкретных условий функционирования и особенностей вычислительной сети в качестве источника внутренних угроз могут выступать:

Взаимодействие органов информационной борьбы США

– авторизованные субъекты доступа – администратор вычислительной сети, администратор баз данных, администратор безопасности, пользователи, программисты, разработчики;

– вспомогательный технический и обслуживающий персонал – служба охраны, жизнеобеспечения и другие.

Источниками внешних угроз для вычислительных сетей являются:

– представители криминальных структур и террористических организаций, заинтересованные в хищении информации, составляющей государственную или коммерческую тайну, или причинении ущерба инфраструктуре организации;

– хакеры или недобросовестные поставщики телекоммуникационных услуг;

– подразделения и службы технической разведки иностранных государств.

Основным классификационным признаком угроз безопасности выступает их направленность. В соответствии с этим выделяют угрозы нарушения конфиденциальности, целостности или доступности информации. При этом в качестве объекта угрозы рассматривается как оперативная информация, обрабатываемая в интересах конечных пользователей вычислительной сети, так и технологическая, используемая для организации функционирования комплекса средств обработки информации и комплекса средств защиты информации.

К угрозам нарушения конфиденциальности информации в вычислительных сетях относятся:

– несанкционированное чтение или копирование информации, в том числе остаточной или технологической, на любом из этапов ее обработки;

– несанкционированный импорт или экспорт конфиденциальной информации;

– передача информации между элементами вычислительной сети, относящимися к разным классам защищенности.

Угрозами нарушения целостности являются:

– несанкционированная модификация либо удаление программ или данных;

– вставка, изменение или удаление данных в элементах протокола в процессе обмена между абонентами вычислительной сети;

– потеря данных в результате сбоев, нарушения работоспособности элементов вычислительной сети или некомпетентных действий субъектов доступа.

К угрозам нарушения доступности относятся:

– повторение или замедление элементов протокола;

– подавление обмена в телекоммуникационных сетях;

– моделирование ложной тождественности узла вычислительной сети или связи для передачи данных;

– использование ошибок или недокументированных возможностей служб и протоколов передачи данных для инициирования отказа в обслуживании;

– перерасход вычислительных или телекоммуникационных ресурсов.

В отдельный класс угроз следует выделить события, которые в зависимости от условий могут нарушить любую из составляющих безопасности информации:

– проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

– несанкционированное включение в состав комплексов средств обработки информации и средств защиты информации новых элементов или изменение режимов их работы;

– доступ к ресурсам вычислительной сети без использования штатных средств вычислительной техники (СВТ) или выполнение программ или действий в обход системы защиты;

– подбор, перехват или разглашение (компрометация) параметров аутентификации или ключей шифрования (дешифрования);

– несанкционированный запуск программ;

– использование нестойких параметров аутентификации или ключей шифрования либо их несвоевременная смена;

– навязывание ранее переданного или ложного сообщения, отрицание факта его передачи или приёма;

– некомпетентное использование, настройка или администрирование комплексов средств обработки информации и средств защиты информации;

– сбои и отказы в работе комплексов средств обработки информации и средств защиты информации.

Анализ угроз безопасности функционирования вычислительных сетей в условиях информационного конфликта позволяет сделать вывод, что в зависимости от текущего уровня защищенности информации от НСД стратегии нарушителя по преодолению системы защиты будут изменяться.

Конечное число видов информационных воздействий определяет конечное число видов стратегий воздействий нарушителя. В зависимости от возможностей нарушителя по воздействию на определенные свойства защищаемой информации выделяются следующие типы стратегий:

Нарушение доступности информации. Используется в случае, если нарушитель не может получить непосредственный доступ к защищаемой

информации и вынужден воздействовать на него опосредованно, путем изменения структуры, параметров, режимов работы или нарушения (снижения) качества функционирования комплексов средств обработки информации и средств защиты информации.

Нарушение конфиденциальности информации. Применяется в случае существования канала НСД или возможности дешифрования информации в приемлемые для нарушителя сроки.

3. Нарушение целостности информации. Используется в случае, если несанкционированное чтение или копирование информации невозможно или нецелесообразно.

4. Навязывание ложной информации. Применяется для воздействия на подсистему организационного управления в целях принятия атакуемой стороной решений, не адекватных ситуациям.

Для предотвращения такого рода угроз в ВВС США осенью 2007 года создано специальное командование ВВС – киберкомандование (AF Cyber Command). Идея создания единого органа МО США по противодействию кибернетическим угрозам обсуждается в высших органах США с начала XXI века. В 2006 году её озвучил заместитель начальника управления стратегического планирования и политики объединенного центрального командования вооруженных сил США бригадный генерал Марк Киммит: «Террористы уже давно создали группу, которая ведет активную работу в Интернете, и Пентагону следует создать мощное подразделение, которое будет противостоять этому»[179].

Организационные мероприятия по формированию новой структуры прошли на авиабазе Барксдейл (штат. Луизиана). На пресс-конференции 2 ноября 2007 года министр ВВС США Майкл Вин (Michael W. Wynne) сообщил, что новое киберкомандование будет активно привлекать силы и средства 8 ВА. По словам генерал-лейтенанта Роберта Елдера (Robert J. Elder), командующего 8 ВА (Барксдейл), «ВВС заинтересованы в возможности многосторонних атак на ВС противника, а также защиты национальной инфраструктуры. Однако увеличение военного присутствия США в киберпространстве имеет и отрицательную сторону. ВС США становятся сильно зависимыми от Интернета, компьютерных систем связи, что делает их уязвимыми и создает предпосылки для массированных кибер-атак со стороны противника».

Таким образом, задачами AF Cyber Command ВВС США в настоящее время являются: подготовка и представление правительству вариантов решения вопросов по защите целостности США и их глобальных интересов, обе-

179 Иващенко А. – Борьба Пентагона с террористами в Интернете. Зарубежное военное обозрение. 2006, №5, с. 65

спечение боевых вылетов авиации и ведение боевых действий в воздухе, космосе и киберпространстве. Начальником AFCBYER ВВС США назначен генерал-майор Вильям Т. Лорд (William T. Lord)[180].

Создание нового командования обусловлено необходимостью сосредоточения усилий по успешному противодействию атакам противника в киберпространстве, повышение степени защищенности как военных систем, так и гражданского сектора, а также организации собственных акций атакующего характера в целях завоевания инициативы и превосходства на кибернетическом ТВД[181]. По словам генерала Майкла Мосли – начальника штаба ВВС, «игнорирование киберпространства, как ключевого ТВД, ставит под угрозу успешность проведения операций в остальных ТВД».

Предполагается, что новое командование организует процесс формирования глобальных маневренных сил, способных действовать как в воздухе

Основные компетенции AF Cyber Command

180 Закончил академию ВВС США, имеет степень бакалавра по биологическим наукам, MBA и магистра по стратегии национальных ресурсов. Ранее занимал пост начальника отдела МО США по кибертрансформации и стратегии. Звание генерал-майора получил в 2006 году

181 США оценивает киберпространство как полноценное поле сражения, как и любое другое (воздух, земля, море и космос). Превосходство в киберпространстве дает свободу действий на других ТВД (и осложняет действия противников) и тесно связано со всеми военными операциями

и космосе, так и в киберпространстве, для чего будут задействоваться базы данных и других структурных элементов информационной борьбы (рисунок). Необходимость создания таких сил вытекает из концепции «Global vigilance, global reach and global power»[182], согласно которой США ставит перед собой задачи глобального контроля намерений и упреждения действий противника, осуществления моментального ответного удара с максимальной скоростью и точностью, а также поражения любой цели. AFCBYER станет динамичной военной организацией, объединяющей возможности страны, системы управления и персонал для достижения превосходства на всех ТВД.

Основное внимание нового командования будет сосредоточено на проведении операций:

– в электромагнитном спектре (РЭБ);

– в системах связи (радиоэлектронные системы);

– в компьютерных сетях.

В настоящее время в состав командования включены следующие структурные элементы:

– оперативный информационный центр ВВС (AFIOC), являющийся элементом командования связи ВВС (AFCA) (авб. Скотт, шт. Иллинойс);

– центр глобальных киберинноваций (авб. Лэнглей, шт. Вирджиния);

– 38 группа инжиниринга киберпространства (авб. Тинкер, шт. Оклахома);

– 688 крыло информационных операций (авб. Локленд, шт. Техас);

– 450 крыло РЭБ (авб. Девис-Монтан, шт. Аризона);

– 68 крыло РЭБ (авб. Эглин, шт. Флорида);

– 689 киберкрыло (авб. Тинкер, шт. Оклахома);

– 750 космическая группа (авб. Петерсон, шт. Колорадо);

– 67 крыло сетевых войн (Локленд, шт. Техас).

На дежурстве:

– 3 группа боевых коммуникаций (авб. Тинкер, шт. Оклахома);

– 5 группа боевых коммуникаций (авб. Джорджия, шт Джорджия);

– 85 отряд инженеринга и сооружений (авб. Кислер, шт. Миссури);

– 84 отряд оценки радаров (ав. Хилл, шт. Юта).

К работе в AFCYBER ВВС США будет привлечено 20000 военнослужащих и лиц гражданского персонала, в том числе лётный состав и специалисты по авиационной электронике, а также авиация следующих типов: U-2 – стратегический разведывательный самолет, ЕС-130Е – самолет разведки, радио и телевещания, ЕС-130Н – самолет РЭБ. Ожидается, что Киберкомандование ВВС США будет способно решать зада-

182 Концепция реализуется в ВВС с ноября 2000 года

чи координирования деятельности специальных органов МО США по противодействию угрозам кибервойны в полном объеме с начала 2009 года»[183].

«В Японии – в штабах видов и объединений вооружённых сил создаются специальные отделы по информационному противоборству, разработаны программы использования компьютерных технологий и подготовки войск к ведению информационного противоборства.

Готовность к ведению кибервойны демонстрируют не только отдельные страны, но и в целом Североатлантический альянс, где её ставят в один ряд с противоракетной обороной и борьбой против международного терроризма. Ещё пять лет назад на саммите в Праге (2003) атлантисты приняли решение разработать программу по защите от атак в киберпространстве. Тогда же была создана специальная служба NATO Computer Incidents Response Capabilities Centre, специалисты которой готовы приступить к защите компьютерных сетей в любое время дня и ночи. На сегодняшний день НАТО имеет уже три линии кибероборонь: кроме указанной службы, существуют ещё Гаагский исследовательский центр проверки действующих систем и выработки новых стандартов защиты, а также программа разработки защищённых систем связи.

Однако в Брюсселе считают, что этого недостаточно. Как заявил представитель НАТО генерал-майор Джордж д'Олландер, сейчас разрабатывается специальная структура для защиты стран – членов альянса от кибератак. Она будет заниматься сбором разведывательных данных и координировать действия членов НАТО в борьбе против киберпреступности. Создание отдельной структуры по предотвращению кибератак возможно будет одобрено руководством стран – участниц НАТО на одном из ближайших саммитов. Там же будет заложено отдельное направление работы альянса под названием «политика кибернетической обороны»[184].

Позитивный опыт информационной войны стимулировал переход США к современным методам и средствам информационного противостояния в самых агрессивных формах, предназначенных на добивание России (Германия на очереди) как основного препятствия для достижения глобального доминирования.

Довольно быстро в США произошло решительное расширение структур, ответственных за ведение информационной войны и их переоснащение самыми современными техническими средствами. Была осовременена и идеологическая основа информационной войны в виде доктрины «исторической миссии» по распространению и защите «американской модели демократии во всём мире».

---

183 Защита информации и информационная безопасность: Соловьев А.А., Метелев С.Е., Зырянова С.А. – Омск: Изд-во Омского института (филиала) РГТЭУ, 2011.

184 Защита информации и информационная безопасность: Соловьев А.А., Метелев С.Е., Зырянова С.А. – Омск: Изд-во Омского института (филиала) РГТЭУ, 2011.

Для понимания масштабов развития методов и средств информационной войны Соединёнными штатами Америки и учёта последствий этих мероприятий Российской Федерацией в её практической деятельности по обеспечению собственной информационной безопасности рассмотрим конкретные мероприятия США по перестройке структуры вооружённых сил в части структур, назначенных на обеспечение ведения такой войны.

Освоение кибернетического пространства военными уже привело к переоценке многих постулатов военной науки прошлого, и даже представлений о характере обеспечения глобального доминирования. Появились новые теоретики военного дела и новые теории.

Доктрина геоцентрического театра военных действий.

«Наиболее интересным текущим результатом этого процесса (он явно только начался, и ещё преподнесёт сюрпризы) является, вероятно, доктрина «Геоцентрического ТВД», выдвинутая командующим космическими войсками ВВС США генералом Робертом Келером. В её основе – представление о фундаментальной взаимосвязи кибернетического и космического пространств. Стоит обсудить недолгую, но богатую событиями историю признания доктрины геоцентрического ТВД, хотя бы обозначить здесь основные её постулаты и попытаться понять её смысл.

На 25 космическом симпозиуме 31 марта 2009 года генерал Келер неожиданно употребил новый термин – ***«геоцентрический театр военных действий (ТВД)»*** (Spherical Battlespace) и в нескольких фразах описал его. Новый театр военных действий простирается сверху вниз от уровня геостационарной орбиты (36 тыс. км над Землёй) до её поверхности, постепенно вбирая в себя все прежние арены (домены в американской терминологии) военного противоборства – космос, атмосферу, сушу, море, а также новый домен – киберпространство»[185]. Заметим, что такое утверждение было и до сих пор остаётся справедливым только до перемещения на Луну, а в дальнейшем и на Марс (и /или на Фобос) военных информационных и энергетических установок. В последнем случае придётся рассматривать уже не геоцентрический ТВД, а говорить о гелиоцентрическом ТВД, тем не менее, даже геоцентрический ТВД переводит военное противостояние на принципиально иной уровень. На этом уровне противостояния столь же принципиально должны измениться и уже изменяются все методы и средства ведения военных действий.

Сразу вслед за этим, в апреле 2009 года, генерал Келер настоял на, казалось бы, совершенно бессмысленном и алогичном решении – подчинении

185 Война в киберэпоху: концепция геоцентрического ТВД http://habrahabr.ru/post/108701/

Эмблема Космического командования ВВС США.

Эмблема Стратегического командования ВС США.

кибервойск командованию космическими войсками (AFSPC). «Казалось бы, сущая нелепица – кибервойска и космические войска действуют в совершенно различных средах, различными методами, решают различные задачи. Всё равно, что подчинить моряков пехоте, или пехоту авиации.

Однако уже в мае того же года Сенат США выслушал и одобрил предложения генерала. Кибернетические войска было решено подчинить космическим.

Год спустя, 21 мая 2010 года кибернетическое командование USCYBERCOM достигло статуса ограниченной боеспособности (Initial Operational Capability, IOC). При этом оно было подчинено не командованию космическими войсками ВВС США, как настаивал Келер, но непосредственно стратегическому командованию USSTRATCOM.

«Казалось бы, противоречие – схема Келера отвергнута? Нет. Ещё на исходе лета стало известно, что президент Обама номинировал генерала на должность командующего стратегическим командованием. Такое кадровое решение выглядит как раз вполне логичным – на новом посту генералу легче будет реализовать новую доктрину.

Руководящий документ AFDD3–12 Киберкосмические операции/Cyberspace Operations, утверждённый 15 июля, был впервые опубликован 14 октября 2010 года. В нём было отмечено, что киберпространство – **первая в истории искусственная арена боевых действий**. До её появления войны велись только в естественных доменах, то есть на суше, на море, в воздухе и в космосе.

Киберкомандование достигло статуса полной боеспособности/FOC, Full Operational Capability 3 ноября. Заместитель министра обороны США

Уильям Линн охарактеризовал киберпространство уже не просто как новый и не просто как исключительный домен, но назвал его последним (latest) мыслимым доменом вообще. Вне зависимости от его правоты или неправоты ясно, что прозвучала официальная точка зрения. А раз киберпространство – домен самый последний, то и бой за него будет «последним и решительным», когда все средства хороши.» [186]


Источник: www.tadviser.ru

Уильям Линн

В этом послании военного чиновника проявилось либо политическое семантическое лукавство, либо плохое понимание теории информации: «latest» имеет смысл «последний на временной шкале, за которым не существует продолжения, например, фраза из песни «это есть наш последний и решительный бой», но также это слово имеет смысл как последний в ряду, имеющем продолжение, следующий за предыдущим известным). Такое лукавство или имитация незнания, тем не менее, имеет очевидную цель оправдания утверждения о том, что «все средства хороши», что, к сожалению, стало частью американской военной политики.

«В чём смысл концепции геоцентрического ТВД? В кратком изложении это сделать трудно, тем более, что ее систематизированный и целостный вариант, вероятно, не опубликован. Да и сама концепция не является догмой, а потому имеет свойство к трансформации и развитию. Но то, что она стремительно реализовывается – факт безусловный. Каковы же основные положения Келеровской военной концепции? Несколько слов о них и выводах, которые следуют из изучения доктрины.

1. Ареной военного противоборства теперь будет служить всё геоцентрическое пространство. Термин «ноосфера» в полной мере подходит для обозначения пространства геоцентрического ТВД. С нашей точки зрения этот, обозначающий «новое, искусственное пространство» термин вполне применим к виртуальному пространству, хотя в реальном земном пространстве он привёл к глубокой деформации миропонимания нескольких поколений. В частности, абсолютно безответственная концепция глобального геоинжениринга, проталкиваемая помощником президента Б. Обамы по науке, бывшим журналистом Джоном П. Холдреном, основывается на теории ноосферы Вернадского.

---

186 Война в киберэпоху: концепция геоцентрического ТВД http://habrahabr.ru/post/108701/

2. Главную действующую силу на геоцентрическом ТВД представляют космические и кибернетические войска, которые выступают фактически единым целым и действуют под единым командованием. Понятно, что методологической основой функционирования киберкосмических войск станут базовые концепции информационной войны, а дополнительными средствами силовой реализации – весь комплекс вооружений геоцентрического ТВД.
3. Два фактора определяют необходимость объединения кибер и космических войск. Это скорость проведения операций и их быстротечность. И минимальное или фактическое отсутствие различия между стратегическим и тактическим уровнями управления. Нужно особо отметить это революционное утверждение, тем более, сформулированное карьерным генералом.
4. В новый условиях информация, с помощью которой управляют ведением боевых операций, уже не будет делиться на тактическую (детальную и локальную) и стратегическую (глобальную, но не столь детальную), как это было прежде. На всех уровнях системы управления войсками информационный образ обстановки должен быть одним и тем же – фактически, он должен стать «резиновым», загрубления (генерализация) невозможны и недопустимы. Это положение известно как принцип «Ситуационной осведомлённости»/Situational Awareness.
5. Естественно, информация при этом должна быть и трёхмерной, и динамической. Любое событие, объект, процесс должны быть локализованы и в пространстве, и во времени. На практике это обозначает очередной качественный скачок в теории войны – переход от трёхмерных к четырёхмерным представлениям о ведении и обеспечении боевых действий, что потребует переподготовки операторов всех уровней.
6. В этой ситуации киберпространство становится не просто средой, в которой противники крушат сети друг друга, но ещё и носителем информационного образа геоцентрического пространства – важнейшего условия победы в войне, особой «геоинформационной системой». Без наличия информационного образа текущей обстановки победа в войне невозможна, а с ним – становится предопределённой. Потому что победа достигается через заблаговременное выявление угроз и нейтрализации их с помощью концентрации ресурсов – там и тогда, где и когда это необходимо. Доминировать везде и всегда уже не получится – об этом прямо говорится в разделе «Космические операции»/Cyberspace Operations.

Однако это приводит к ситуации, когда становятся очевидными и факторы собственной уязвимости, которые, как правило, связаны с критически важными объектами на собственной территории. Обязательная усиленная защита таких объектов создаёт статичные узлы в динамической системе ТВД, отвлекающие и таким образом распыляющие задействованные силы, делая победу далеко не предопределённой.

7. Победа станет возможной не истощением противоборствующей стороны, но через «обескураживание» его действиями, которые так быстро изменяют обстановку, что противник не в состоянии не только что-либо предпринять, но и воспринять – так выглядит доведенная до логического завершения концепция «Маневренной войны»/Maneuver Warfare.

В этом положении в неявном виде заключена реминисценция идеологии войны на истощение/war of attrition, в которой в условиях преимущественно двумерной борьбы операции разделяются на тактические и стратегические, где только тактические операции маневренной войны подразумевают элемент неожиданности. Кроме того, это положение подразумевает необходимость восприятия противником атакующего стратегического действия в расчёте на опоздание противника в его оценке и, что ещё хуже, наличие ответного действия.

На самом деле, порочность, способная привести к поражению, заключена уже в самой заданности такого предположения. Никто не доказал, что противник должен отвечать на какое бы то ни было действие или даже размышлять об этом, кроме самого факта начала войны. Противник волен как хороший шахматист пожертвовать объектами атаки и нанести удары по агрессору по собственному плану, исходя из собственных боевых возможностей.

Рассмотрим весьма нежелательную, но геополитически вероятную ситуацию войны между США и ИРИ.

Исходные данные:
США:

задействованы сразу в нескольких «горячих» конфликтах (два крупных трёхмерных без явного применения ОМУ, связывающих значительные контингенты современных вооружённых сил, истощающих финансовые ресурсы и вызывающих заметную социальную напряжённость в собственной стране);

располагают всеми СМП, в том числе порядка 2500 ядерных боеголовок, и некоторым количеством вооружений, назначенных на ведение действий

Реза Кахлили

на геоцентрическом ТВД, в том числе прошедших натурные испытания, оказавшие разрушительные воздействия на природные и промышленные объекты на территории Ирана;

имеют обширный опыт ведения глобальной информационной войны;

обладают ограниченным контингентом полностью боеготовых сухопутных воинских подразделений весьма средней боеспособности, но располагающих избыточными возможностями получения поддержки со стороны ВВС и ВМФ;

имеют конфликтующих между собой союзников в регионе: Израиль с 800-1000 боеголовками в ядерной триаде, в том числе 2-3 мощностью более 1 мегатонны; Турция с сильной традиционной армией, которая в настоящая время ослаблена конфликтом с политической властью; Грузия и Азербайджан, не имеющие самостоятельного военного значения, но полезные как угрожающий плацдарм для сил наземного вторжения; Саудовская Аравия и Катар, не имеющие значимых вооружённых сил, но финансирующие и контролирующие исламских экстремистов, наёмников и террористов, включая боевиков Аль Каеды, готовых вести и ведущих подрывные действия в странах региона.

ИРИ:

после Ирано-Иракской войны не участвует в военных конфликтах, за исключением военно-морских операций против пиратов в Йеменском заливе.

Располагает ограниченным потенциалом СМП, в том числе предположительно имеет до 10 ядерных боеголовок мощностью до 5 килотонн и до 30 ядерных зарядов малой мощности, назначенных на применение в условиях традиционной и в меньшей мере в условиях современной трёхмерной войны, располагает ракетными средствами доставки – всего более 6000 единиц, в том числе до 1000 ракет средней и большей дальности, предположительно, со значительными ограничениями по точности; оценка ядерного потенциала получена сравнительным анализом данных, имеющихся в распоряжении авторов, и данных агента ЦРУ, опубликованных в Вашингтон Пост.

«Давление, которое Соединенные Штаты и Запад в целом применяют в отношении Ирана с целью удержать его от обретения ядерного оружия, осуществляется абсолютно напрасно. У Исламской Республики уже имеется не только ядерное оружие от бывшего Советского Союза, но и достаточное количество обогащенного урана для производства нового оружия. И что ещё хуже, у Ирана есть средства доставки.

Источник: ru.wikipedia.org

Мохсен Резэй

Источник: www.svoboda.org

Аятолла Хомейни

Источник: www.newspakistan.pk

Абдул Кадир Хан

Запад в течение примерно десятилетия проявлял беспокойство в связи с расширением технических возможностей Ирана в плане производства урана, будучи уверенным, что Иран работает над созданием ядерной бомбы, хотя правительство продолжает настаивать, что его программа по обогащению урана носит исключительно мирный характер.

Когда Иран начал свою ядерную программу в середине 1980-х годов, я работал в качестве шпиона ЦРУ внутри Корпуса стражей исламской революции (КСИР)[187]. Разведка стражей в то время узнала о попытке Саддама Хусейна приобрести ядерную бомбу для Ирака. Командование корпуса пришло к выводу, что им нужна ядерная бомба, потому что если она будет у Саддама, он использует её против Ирана. В то время две страны находились в состоянии войны».

Иранское ядерное оружие в новом веке

Мохсен Резэй (Mohsen Rezaei), тогдашний командир Стражей, получил разрешение от аятоллы Рухоллы Хомейни (Ruhollah Khomeini) начать скрытую программу по приобретению ядерного оружия. С этой целью Стражи вступили в контакт с пакистанскими генералами и пакистанским учёным-ядерщиком Абдулом Кадир Ханом (Abdul Qadeer Khan)[188].

Командующий Али Шамхани (Ali Shamkhani) ездил в Пакистан, предлагая миллиарды долларов за бомбу, но все переговоры закончились вместо этого лишь чертежами и центрифугами. Первая центрифуга была доставлена в Иран на личном самолете Хомейни [189].

---

187 Халили ...

188 ***Проф. Абдул Кадир Хан,*** *Abdul Qadeer Khan (Urdu: ڈاکٹر عبد القدیر خان; b. 1 April 1936) Широко известен как Д-р А. К. Хан, пакистанский учёный – ядерщик (долгое время содержался под домашним арестом по подозрению в распространении ядерных технологий)*

189 ***Аятолла Рухолла Мусави Хомейни*** *(перс. روح الله موسوی خمینی) 17 мая 1900-3 июня 1989 Высший руководитель Ирана с 1979 по 1989.*

Источник: news.rambler.ru

Али Шамхани

Источник: gyrosco;ye-v.narod.ru

Виктор Иванович Самойлов

В рамках второй, но осуществляемой параллельно попытки заполучить ядерное оружие, Иран обратился к бывшим советским республикам. Когда Советский Союз распался в 1990 году (ошибка! – формально распад СССР произошёл в 1991 году), Иран страстно желал получить тысячи единиц тактического ядерного оружия, которые были распылены по бывшим республикам Союза.

«В начале 1990-х годов ЦРУ попросило меня найти иранского ученого, который засвидетельствовал бы, что у Ирана есть бомба. ЦРУ узнало, что агенты иранской разведки ездили на ядерные объекты по всему бывшему Советскому Союзу, и при этом проявляли особый интерес к Казахстану [190]. Мусульманский Иран активно обхаживал Казахстан, на долю которого приходилась значительная часть советского арсенала, и который при этом являлся преимущественно мусульманским, и Тегеран предлагал ему сотни миллионов долларов за бомбу. Вскоре появились сообщения о том, что три ядерные боеголовки пропали. Это подтвердил и российский генерал Виктор Самойлов, который занимался вопросами разоружения для Генерального штаба. Он признал, что из Казахстана исчезли три ядерных боеголовки.

Между тем, Пол Мюнстерманн (Paul Muenstermann), тогдашний вице-президент германской федеральной службы разведки, заявил, что Иран получил две из трёх ядерных боеголовок, а также средства доставки ядерного оружия средней дальности из Казахстана. Он также сообщил, что Иран приобрел четыре 152-миллиметровых ядерных боеприпаса из бывшего Советского Союза, которые, по сообщениям, были украдены и проданы бывшими офицерами Красной армии.

«Что ещё хуже, несколькими годами спустя российские официальные лица заявили, что при сравнении документов о передаче ядерного оружия из Украины в Россию, обнаружилось расхождение ни много, ни мало в 250 ядерных боеголовок»[191].

В приводимой здесь цифре есть некоторая двусмысленность: в соответствии с Четырёхсторонним соглашением Украина имела право сохранить

190 Кахлили ...

191 Кахлили

у себя 200 устаревших урановых тактических боеголовок для последующего блендинга на собственных предприятиях, и если эти 200 единиц входят в число (250) указанных в передаточном протоколе, то количество неучтённых боеприпасов составляет примерно 50 единиц, включая мины, артиллерийские снаряды и т. п., что, в общем-то, соответствует существующей оценке ядерных боеприпасов, вероятно проданных Украиной Ирану в начале 90-х годов, в том числе в комплектации ДЭПЛ проекта 877ЭКМ торпедами и ракетами средней дальности с ядерными боеголовками.

Источник: www.iwp.edu

Тони Шаффер

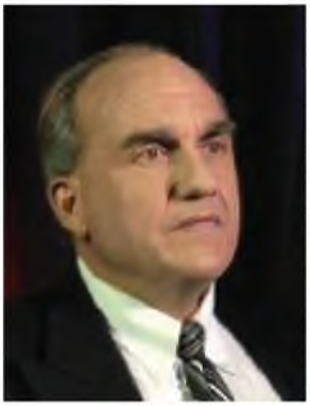
«На прошлой неделе Мэтью Насути (Mathew Nasuti), бывший капитан ВВС США, который в какой-то момент был нанят Госдепартаментом в качестве советника для одной из провинциальных групп по восстановлению в Ираке, рассказал, что в марте 2008 года, во время брифинга по Ирану в Госдепартаменте, эксперт департамента по Ближнему Востоку сказал группе собравшихся как о «общеизвестном факте», что Иран приобрел тактическое ядерное оружие у одной или нескольких бывших советских республик.

«Подполковник Тони Шаффер (Tony Shaffer), опытный офицер разведки, награжденный «Бронзовой звездой» (военная медаль, американская военная награда за отвагу, четвертая по значимости награда в ВС США, учреждена в феврале 1944 года – прим. перев.), рассказал мне, что его источники сообщают, что у Ирана сейчас имеется две рабочие ядерные боеголовки[192]».

Редакционная статья в иранской газете Кайхан/Kayhan, газете, которая находится под прямым наблюдением аппарата духовного лидера Ирана, предупреждала, что если Иран будет атакован, то последуют ядерные взрывы в американских городах.

«Несмотря на твёрдое знание того, что иранские лидеры стремятся обрести ядерное оружие, западные лидеры выбрали путь переговоров и умиротворения, в надежде найти решение иранского вопроса. Прошло примерно три года работы администрации Обамы, и мы должны признать, что политика сначала пряника в виде доброй воли и сотрудничества, а потом кнута в виде санкций не смогла убедить иранцев отказаться от ядерной программы, и не смогла сдержать их агрессивное позиционирование. Сегодня иранские лидеры, несмотря на четыре набора санкций ООН, продолжают реализацию и своей ракетной программы, и программы в области ядерного обогащения, и у них достаточное количество обогащенного урана для создания шести

192 Кахлили



Источник: www.groundzeromedia.org

Питер Винсент Прай

ядерных бомб, согласно данным последнего отчета Международного агентства по атомной энергии (МАГАТЭ)[193]».

Если Иран станет обладателем ядерного оружия, его создаст и Саудовская Аравия

У Корпуса стражей исламской революции сейчас имеется более тысячи баллистических ракет, многие из которых нацелены на американские военные базы на Ближнем Востоке и в Европе. Стражи также добились больших успехов в разработке своих межконтинентальных средств доставки ракет, под прикрытием своей космической программы. «Как я говорил ранее, боеголовки, способные нести ядерные заряды, были доставлены стражам, и духовный лидер Ирана приказал им установить на ракеты ядерные боезаряды»[194]. Иранский флот уже вооружил свои корабли ракетами «земля-земля» дальнего радиуса действия, и вскоре расширит зону охвата своей миссии на Атлантический океан и Мексиканский залив» [195] (см. приводимую информацию о составе и перспективах модернизации Иранского флота).

«История заставляет предполагать, что может быть уже слишком поздно с нашей стороны пытаться остановить Иран в его ядерных амбициях. Почему мы предполагаем, что за 20 лет попыток Иран не смог достичь результата – имея доступ к огромным количествам незасекреченных данных о конструкциях ядерного оружия, и вооруженный технологиями 21-го века – которого США достигли за три года во время реализации Манхэттенского проекта в 1940-е годы?», – задается вопросом эксперт по ядерному оружию Питер Винсент Прай (Peter Vincent Pry), который работал в ЦРУ и в комиссии EMP (Комиссия по оценке угрозы Соединённым Штатам от атаки при помощи электромагнитного импульса (возникающего при ядерном взрыве) – Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) attack – EMP Commission), а сейчас является президентом EMPact America.

Г-н Прай приходит к выводу, что Ирану нужна лишь одна единица ядерного оружия, чтобы уничтожить Соединённые Штаты. «Ядерный электромагнитный импульс способен уничтожить национальную энергосеть и дру-

---

193 Кахлили

194 Кахлили

195 У Ирана уже есть ядерное оружие («The Washington Times», США) http://inosmi.ru/asia/20111028/176730988.html#ixzz2olS6nPaZ

гие критически важные инфраструктуры, которые поддерживают жизнь 310 миллионов американцев»[196].

Этот вывод – скорее всего, измышление провокатора или, что менее вероятно, некомпетентный бред параноика. Иран не имеет ядерного боеприпаса мощностью ~ 1 Мегатонна и, тем более, возможностью доставить его на высоту 1,0-1,5 км над территорией США.

«Готовы ли мы окончательно понять, каковы цели и идеология джихадистов в Тегеране, и предпринять соответствующие действия против них? Сам иранский народ, который выступает против мулл с диктаторскими замашками, годами просил нас сделать это. Тысячи людей отдали свои жизни, чтобы показать нам настоящую природу этого режима. Мы должны действовать, пока не стало слишком поздно»[197].

Иран

имеет приличные, хорошо защищённые системы ПВО и значительный опыт информационного противоборства с США и их союзниками;

обладает значительным контингентом религиозно индоктринированных боеготовых частей, в том числе частей с очень высокой боеспособностью, а также – примерно 6000 добровольцев-смертников;

ВВС:

располагает несколько устаревшими, но развивающимися и модернизируемыми военно-воздушными силами.

На начало 2000-х годов численность ВВС Ирана оценивалась разными изданиями от 30000 человек. Имелось 12 авиабаз, включая 10 истребительных и 2 транспортные. В своём составе ВВС имели до 25 боевых эскадрилий, 12 транспортных, 2 вертолётные, 10 отрядов связи и управления, 10 поисково-спасательных отрядов [3]. За истёкшее время построены две новые авиабазы.

Кроме того, на вооружении частей иранской армии стоит около 200 легких гидросамолетов Bavar 2 иранского производства.

Иран располагает лучшим флотом среди стран Персидского залива

На сегодняшний день корабельный состав ВМС Ирана выглядит следующим образом:

---

196 У Ирана уже есть ядерное оружие («The Washington Times», США) http://inosmi.ru/asia/20111028/176730988.html#ixzz2olS6nPaZ

197 Кахлили

Техника и вооружение

Тип	Назначение	Кол-во	Примечания	Изображение
Истребительная авиация				
HESA Saeqeh	Фронтовой истребитель	24 [4]	Разработан и построен силами Ирана	
HESA Azarakhsh		30 [5]		
F-14 Tomcat	Истребитель-перехватчик	44 [6]	Построены в 1974-1979, 25 используются. 1 потерян в 2012. Иран самостоятельно наладил производство запчастей для F-14.	
МиГ-29	Фронтовой истребитель	35	Перегнано в 1991 из Ирака [7]	
Dassault Mirage F1		10	Построены в 1991. Перегнаны из Ирака во время войны в Персидском заливе в 1991 году [7]	
Northrop F-5		20	Поставлялись с 1960 по 1970-е	
F-7M		24	Поставлялись с 1960 по 1970-е	
Су-25	Штурмовик	13	Перегнано в 1991 из Ирака. [7]	

Тип	Назначение	Кол-во	Примечания	Изображение
Dorna/Tazarv	Учебно-тренировочный самолет/лёгкий штурмовик/лёгкий истребитель	25 [8]	Разработан и построен силами Ирана	
Бомбардировщики				
Су-24МК	Фронтовой бомбардировщик	30	24 перегнаны из Ирака в 1991 [7]	
Mc Donnell Douglas F-4 Phantom II		65	Постройки 1960-х	
Northrop F-5	Истребитель-бомбардировщик	60	Поставлялись с 1960 по 1970-е	
Транспортная авиация				
Boeing 707	Транспортный	4		
Boeing 747		5		
Boeing 727		1		
Lockheed C-130 Hercules		19		
Ил-76		12		
Ан-24		14		
Fokker F27		10		
Dassault Falcon 20		1		
Y-12		9		
Ан-72		11		
HESA IrAn-140	Транспортный АВАКС	15		

Тип	Назначение	Кол-во	Примечания	Изображение
Вертолёты				
HESA Shahed 285	Ударный	50	Современный ударный вертолет полностью иранского производства, разработан на основе вертолетов Bell 206 и Panha Shabaviz 2061 по сумме боевых показателей не уступает таким ударным вертолетам как McDonnell Douglas AH-64 Apache, Bell AH-1Z Viper, Mu-28, CAIC WZ-10. Количество изготовленных машин держится в тайне но по примерным подсчетам около 50 образцов.	
Bell AH-1 Cobra		100	Модернизированы с использованием авионики для HESA Shahed 285, в том числе установлен бортовой компьютер, радар, инфракрасный сканер.	
Bell-205 Bell-206		~100	Вертолет полностью иранского производства.	
Shabaviz 2-75		25		
Беспилотные ЛА				
Karrar	Ударный БПЛА	Большое количество	Тяжёлый атакующий БПЛА максимальная полезная нагрузка 1 тона. Является основным атакующим БПЛА Иранской армии.	
Ababil			Средний («миди») БПЛА для разведки и атаки целей.	
Sofreh Mahi		По крайней мере, 1 летающий прототип	Разрабатывающийся в Иране тяжёлый атакующий БПЛА. Использует стелс технологию. Разрабатывался с применением технологий захваченных на своей территории иностранных БПЛА, в том числе технологии RQ-170 Sentinel.	

Тип	Назначение	Кол-во	Примечания	Изображение
Mohajer 1,2,3,4	БПЛА	Большое количество	Серия средних («миди») БПЛА Mohajer предназначена для разведки и наведения лазерных боеприпасов на цели. Mohajer 1 это первый БПЛА разработанный в Иране. Разработан и поступил на вооружение в 1985 году.	
Zohal			Микро БПЛА вертикального взлета для тактической разведки.	
A1		Значительное количество	Перспективный средний разведывательный БПЛА.	
Shaparak			Перспективный средний разведывательный БПЛА.	
Ra'd			Перспективный средний разведывательный БПЛА.	
Saeghe	Мишень БПЛА	Большое количество	Средний («миди») БПЛА предназначен для использования в качестве мишени и в качестве ложной цели для противника.	
ПВО				
Panipa	ЗРК	30		
Crotale (ЗРК)		30		
МІМ-23		150+ ПУ		
Хок С-75		45 ПУ		
Сайяд-1		20 ПУ	Глубокая модернизация С-75.	
Сайяд-2		50+ ПУ	Глубокая модернизация С-75, дальность полета увеличена до 110 км.	
С-200		200+ ПУ		
Фаджр-8		30+ ПУ	Произведенная в Иране копия С-200.	
Бауэр – 373			Произведенная в Иране копия С-300. [9]	
Тор-М1		29	Используются для защиты самых важных объектов ядерной промышленности.	
Панцирь – С1		10 ПУ	Используются для защиты самых важных объектов ядерной промышленности.	

Тип	Назначение	Кол-во	Примечания	Изображение
Mersad	*ЗРК*	*200+ ПУ*	*Разработан и построен силами Ирана, является глубокой модернизацией MIM-23 Хок использует для наведения фазированную РЛС.*	
Месбах 1	*ЗУ*	*300+*	*Зенитное артиллерийское орудие на основе ЗУ-23-2 использует для наведения РЛС и системы оптического наведения.*	
Sa'ir (Saeer)		*100+*	*Зенитное артиллерийское орудие на основе КС-19 использует для наведения РЛС и системы оптического наведения.*	

В декабре 2009 года Разведывательное управление ВМС США опубликовало доклад «ВМС Ирана: от партизанской войны к современной военно-морской стратегии», в котором впервые официально заявило, что Иран приобрел у КНДР небольшое количество полупогружных подводных лодок классов **Kajami (Taedong-B)** и **Gahjae (Taedong-C)** [160].

десантные корабли

- танкодесантные корабли типа Hengam
- 51 Hengam
- 52 Larak
- 53 Lavan
- 54 Tonb
- десантные корабли типа Iran Ajr
- Iran Ajr
- Iran Ghadr
- десантные корабли типа Iran Hormuz-24
- малые десантные корабли типа Iran Hormuz-21
- малые десантные корабли типа Chavoush
- 102 Chavoush
- 103 Chalak
- малые десантные корабли типа Fouque (MIG-S-3700)
- катера на воздушной подушке типа Wellington (BH-7)
- катера на воздушной подушке типа Юнис-6[161]

минно-тральные корабли

- морской тральщик типа Riazi 312 Riazi

160 Иран получает от КНДР подлодки и технологии.

161 Военно-морские силы Ирана спустят на воду две подводные лодки типа «Аль-Гадир»

вспомогательные суда

- 1 танкер (судно снабжения) типа Kharg
- 2 танкера (судно снабжения) типа Bandar Abbas
- 2 танкера типа Kangan
- 7 судов снабжения типа Delvar
- 12 (13 по др. источнику) вспомогательных судов типа Bakhtaran (Hendijan, MIG-S-4700)
- 10 судов типа Damen 1550

Тип	***Производитель***	***Название***	***№***	***Примечания***	***Изображение***
Подводные лодки					
ДЭПЛ проекта 877ЭКМ		*Tareq*	*901*	*Поступила в 1992, отремонтирована в 2012 году.*	
		Noor	*902*	*На вооружении с 1993*	
		Yunes	*903*	*На вооружении с 1997*	
Подводные лодки проекта Al-Ghadir		*Ghadir 942*	*942*	*Головная мини подлодка. На вооружении с 2007. Водоизмещение 120т, длина 29м, ширина 3м, высота 2,5 м, скорость 11 узлов, экипаж 18 человек, 2 ТА для торпед и мин*	
		Ghadir 944	*944*		
		Ghadir 945	*945*		
		Ghadir 946	*946*		
		Ghadir 947	*947*		
		Ghadir 948	*948*		
		Ghadir 949	*949*		
		Ghadir 950	*950*		
		Ghadir 951	*951*		
		Ghadir 952	*952*		
		Ghadir 953	*953*		
		Ghadir 954	*954*		
		Ghadir 955	*955*		
		Ghadir 956	*956*		
		Ghadir 957	*957*		
		Ghadir 958	*958*		

Тип	Производитель	Название	№	Примечания	Изображение
		Ghadir 959	959		
		Ghadir 960	960	Вступила в строй в феврале 2012	
Подводные лодки проекта Al-Sabehat		Al-Sabehat		Мини подлодка	
Подводные лодки проекта Qaaem		Qaaem		Строится	
Подводные лодки проекта Fateh		Fateh		С 2011	
Подводные лодки проекта Nahang		Nahang		с 2006	
Подводные лодки проекта Nahang		Nahang		с 2006	
Подводные лодки проекта Yugo				Переданы за долги	
Эсминцы					
Эсминцы типа Damavand		Damavand	D5	Бывший корабль Великобритании, не активен	
Эсминцы типа Babr		Babr	D7		
Эсминцы типа Babr		Palang	D9	Бывший корабль Великобритании, не активен	

Тип	Производитель	Название	№	Примечания	Изображение
Фрегаты					
Фрегаты типа «Алванд»		Alvand	71	с ПКР YJ-82	
Фрегаты типа «Алванд»		Alborz	72	с ПКР YJ-82	
Фрегаты типа «Алванд»		Sabalan	73	с ПКР YJ-82	
Фрегаты типа Moudge		Jamaran	76	На вооружении с 2010, с ПКР YJ-82	
Фрегаты типа Moudge		Velayat	77	Заложен в 2007, ввод в строй 2012(план), с ПКР YJ-82	
Корветы					
Корветы типа Bayandor		Bayandor	81	с ПКР YJ-82	
		Admiral Naghdi	82	с ПКР YJ-82	
Корветы типа Hamzeh		Hamzeh	802	Построен в 1960-х, с ПКР YJ-82	

Тип	Производитель	Название	№	Примечания	Изображение
Ракетные катера					
Ракетные катера типа Houdong		Fath	P313-2		Построены в 1994-1996, с ПКР YJ-82
		Nasr	P313-2		
		Saf	P313-3		
		Ra'ad	P313-4		
		Fajr	P313-5		
		Shams	P313-6		
		Me'raj	P313-7		
		Falaq	P313-8		
		Hadid	P313-9		
		Qadir	P313-10		
Ракетные катера типа Kaman		Kaman	P221		Построены в 1977-1981
		Xoubin	P222		
		Khadang	P223		
		Falakhon	P226		
		Shamshir	P227		
		Gorz	P228		
		Gardouneh	P229		
		Khanjar	P230		
		Neyzeh	P231		
		Tabarzin	P232		
Ракетные катера типа Sina		Paykan	P224		Построены с 2003 года, с 4хПКР YJ-82
		Joshan	P225		2006
		Derafsh	P233		2008
		Kalat	P234		2008
Малые сторожевые катера типа Parvin		Parvin	211		
		Bahram	212		
		Nahid	213		

Перспективы развития

2008 год – в октябре иранские военные объявили о введении в строй новой военно-морской базы в ключевой точке морского пути транспортировки ближневосточных углеводородов в Ормузском проливе, в портовом городе Джаск.

2009 год – в сентябре при участии министра обороны Ирана Ахмада Вахиди, командующего военно-морскими силами (ВМС) Хабиболлы Сайяри и других официальных лиц был спущен на воду новый ракетный фрегат типа «Sina». Как указывали иранские военные, на нём были установлены более ста образцов военной техники – ракет с радарами, артиллерии и систем связи, а также что судно может противостоять высоким волнам. [162] (Однако еще в 2002 г. тогдашний командующий ВМС Ирана контр-адмирал Аббас Мохтадж упоминал под тем же названием разработанный Ираном ракетный катер «Сина-1» и упоминал о том, что в стадии разработки находятся катера «Сина-2» и «Сина-3») [163].

2009 год – в ноябре, ко Дню военно-морских сил Ирана, по заявлению командующего морскими силами адмирала Хабиболлы Сайяри, на воду будут спущены два корабля с ракетным вооружением «Калат» и «Дерафш», а также легкая подводная лодка[164].

2009 год – в ноябре командование ВМС Ирана заявило о строительстве «современнейшего многоцелевого боевого корабля». Класс корабля и его характеристики не назывались, но, по словам представителя ВМФ, новый корабль «расширит государственные «возможности сдерживания», а благодаря большому водоизмещению он сможет действовать вдали от берегов» [165]. Есть основания предположить, что это будет крейсер.

2010 год, 8 августа – Военно-морские силы Ирана 8 августа 2010 года приняли на вооружение четыре новых подводных лодки класса Ghadir.

Участие в вооружённых конфликтах
Борьба с сомалийскими пиратами

Корабли иранских ВМС ведут патрулирование вод Аденского залива с ноября 2008 года, когда сомалийские пираты у побережья Йемена захватили иранское грузовое судно «Delight» [166]. В настоящее время, несмотря на то,

---

162 ВМС Ирана спустили на воду новый ракетный фрегат «Sina»

163 Аббас Мохтадж (Главком ВМС Ирана) — Мы никому не позволим использовать свои территориальные воды

164 Военно-морские силы Ирана пополнятся двумя ракетоносцами и подводной лодкой.

165 Иран строит современнейший корабль.

166 Пираты назвали условия освобождения иранского судна.

что многие страны мира объединились в коалицию под командованием США в Аденском заливе, корабли ВМС армии ИРИ несут боевое дежурство в этом заливе самостоятельно, опираясь исключительно на свои силы.

- ***май 2009 года***. – в Аденский залив с целью защиты иранских торговых судов и нефтяных танкеров от атак сомалийских пиратов были направлены два иранских военных корабля сроком на пять месяцев. В конце июня им удалось предотвратить захват иранского нефтяного танкера «Hadi». [167]
- ***июль 2009 года*** – Иран направил еще два своих боевых корабля в Аденский залив для защиты судоходства.
- ***сентябрь 2009 года*** – кораблям ВМС Ирана удалось отбить у берегов Сомали атаку пиратов, которые пытались захватить три иранских торговых судна [168].
- ***январь 2010 года*** – 5 оперативная группа боевых кораблей ВМС армии ИРИ в составе двух эсминцев – «Лаван» и «Чиру» – отправилась из Бандар-Аббаса.

Иран имеет консолидированных союзников в регионе: движение «Хэзбола» (Ливан), шиитские движения и организации в Ираке, движение «Хамаз» в секторе Газа (Палестинская автономия), Сирия, а также может рассчитывать на поддержку России и Китая в СБ ООН и на отмену ими ограничений в случае военной агрессии против ИРИ (например, может быть осуществлена поставка торпед «Шквал» и современных систем ПВО в случае несанкционированной СБ ООН военной акции США или коалиции, возглавляемой США, против Ирана).

Сопоставление потенциалов пригодных к задействованию вооружений, в том числе оружия геоцентрического ТВД и СМП, однозначно указывает на более высокую вероятность достижения военной победы Соединёнными штатами Америки. Однако, как уже не раз случалось в истории и как показывает современная военная наука, даже подавляющее преимущество в вооружениях далеко не всегда обеспечивает конечную победу.

Рассмотрим веер возможностей развёртывания вероятного конфликта для обеих противостоящих сторон. В 2007 году намерения США выглядели следующим образом[169].

Администрация президента США Джорджа Буша активно обсуждала планы возможного бомбового удара по Ирану, передает американский телеканал Fox-News со ссылкой на собственные источники в Белом доме.

По данным «хорошо осведомлённого источника» телеканала, «все в городе (Вашингтоне)» <…> активно участвуют в широких дискуссиях

167 Иран увеличил число кораблей, защищающих суда от морских пиратов в Аденском заливе.

168 ВМС Ирана отбили у берегов Сомали атаку пиратов.

169 Спектор В.Н. – Аналитическая записка по Ирану от 26.11.07. Труды МАН ПНБ. М., 2010, том 2, вып. 5

о цене и выгоде военной операции против Ирана, наиболее вероятными сроками которой будут следующие восемь-десять месяцев – после того, как итоги предварительных президентских выборов будут уже определены, но ещё останется достаточно времени до финального тура 2008 года.

Обсуждение ведётся по двум основным направлениям: вторжение минимальными силами, результатом чего станет блокада иранского экспорта нефти и газа (мера, призванная негативно повлиять на жизнь простых иранцев, но не правительства), а также тотальная бомбардировка страны[170].

Слухи о планах нападения США на Иран появились в начале 2007 г. Первая информация об этом была распространена кувейтскими СМИ. Журналисты сообщали, что Белый дом планирует нанести удар по ядерным объектам Ирана до апреля 2007 года. По их словам, такое решение было принято на совещании президента США с участием вице-президента Дика Чейни, министра обороны Роберта Гейтса, госсекретаря Кондолизы Райс и ряда военных советников американской администрации. По этому плану удар должен был быть нанесён с моря подразделениями ВВС и ВМФ. Такая тактика позволяет избежать человеческих жертв со стороны американских войск.

В конце мая 2007 года ВМФ США в составе 9 военных кораблей, в том числе двух авианосцев, провёл учения в Персидском заливе. После ввода военных кораблей появилась информация, что ЦРУ тайно готовится заняться дестабилизацией иранского режима (информационная война). По неофициальным данным, соответствующее секретное постановление издал президент США Джордж Буш. В соответствии с документом, ЦРУ будет осуществлять координированную кампанию по проведению пропаганды в стране, по дезинформации иранских властей, а также по манипуляции национальной валютой Ирана и международными финансовыми операциями.

Финальная диспозиция.

Существенным, но недекларируемым основанием для отыскания Соединёнными штатами повода для агрессии против Ирана и очередной силовой смены режима, как уже было в 1953 году в отношении правительства Моссадека, вознамерившегося осуществить национализацию нефтяных богатств Ирана, стало достижение их монопольного контроля Соединёнными штатами в полном соответствии с мондиалистской концепцией неоконсерваторов.

Для публичного обоснования намерений проведения военной операции против Ирана, как для внутренней потребы, так и на международном уровне, в том числе и для сколачивания коалиции, естественно, выдвигается вероят-

170 Американские СМИ: США планируют бомбардировку Ирана. 2007. Интернет

Источник: fakti.org

Ахмад Вахиди

Источник: flot.com

Хабиболла Сайяри

ность создания Ираном ядерного оружия и совершенствования средств его доставки. Подтверждением этого публичного намерения стала широко разрекламированная как в СМИ, так и при протаскивании санкций в СБ ООН в рамках информационной борьбы, кампания по объективно неподтверждённой и неподтверждаемой навязчивой идее об опасности разработки Ираном национальной ядерной технологии.

В рамках широко развернувшейся кампании дезинформации освоение Ираном энергетических ядерных технологий активно выдавалось за этапы в разработке оружейных технологий. В исчерпывающем анализе действительного состояния дел в ядерных программах Ирана[171], признаётся высокая вероятность, граничащая с объективно подтверждённой информацией о наличии у Ирана достаточного для решения задачи сдерживания количества высоко обогащённых (оружейных) делящихся материалов и ядерных устройств (боеголовок средней мощности, артиллерийских снарядов, мин и т. п.), полученных им по разным каналам из-за рубежа, но убедительно отрицается, как разработка Ираном военных ядерных технологий, так и осмысленность таких разработок[172]. В комментариях по этим докладам, опубликованным в газете «Вашингтон Пост», не опровергается аргументация автора, но, как это было при подготовка к вторжению в Ирак, высказывается цепь сослагательных предположений: а вдруг Иран всё-таки разрабатывает национальные технологии обогащения до оружейного уровня и готовится к производству собственных ядерных вооружений.

Такая ментальность самообмана определяет практически однозначно стратегическую концепцию планирования, а в случае имплементации планов стратегию и тактику военной операции. Во-первых, со стороны аэрокосмических сил США не следует ожидать разрушительных ударов по структурам нефте- и газодобывающего комплекса Ирана, трубопроводам и терминалам, – мондиалисты не допустят.

---

171 Spector V.N. – The Russian Perspective on Nuclear and Radiological Terrorism. Доклад на семинаре Департамента по информации и разведке Госдепа США и публичный доклад в Кеннановском Институте. Вашингтон. Дистрикт Колумбия, США, 2006

172 Spector V.N. – The Russian ...

Планировавшиеся направления ударов, 2007.

Иран в окружении американских военных баз.

Финальная диспозиция.

Считая, что у руководства США сохранились остатки здравого смысла и морали, можно предположить воздержание от бомбёжек и ракетно-артиллерийских ударов по святыням мусульман-шиитов – городов Кум и Мешхед. В аятолл всё равно не попадут, а всемирно известный храм Непорочной Фатимы и комплекс Гробницы Имама Резы могут быть разрушены. Однако после разрушения знаменитой шиитской Мечети в Самаре и множественных оскорблений религиозных чувств мусульман (в числе издевательств над заключёнными и убитыми) трудно надеяться на здравый смысл американской военщины, но можно быть твёрдо уверенным в росте враждебности со стороны мусульман, в первую очередь шиитов.

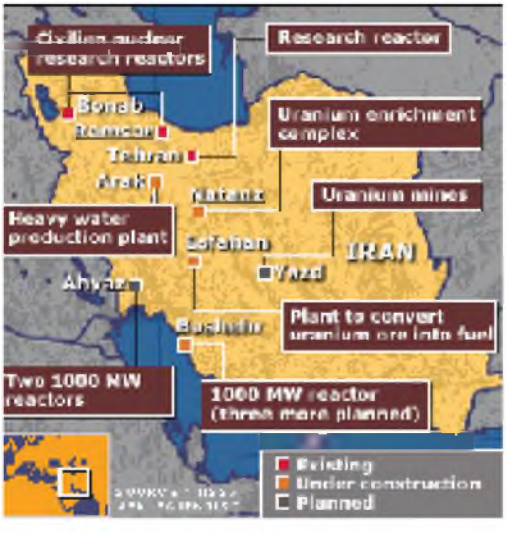
Для оправдания многолетней истеричной кампании по якобы разработке ядерного оружия Ираном основные ракетно-бомбовые удары, координируемые средствами геоцентрического ТВД, будут предсказуемо направлены

Основные Иранские нефтяные поля. *Направление стратегических ударов «нефтяной компоненты» плана операций 2007 и 2008-2009 годов.*

на ядерные объекты Ирана: Натанц (Ядерный центр по обогащению урана), Эрак (место планируемого возведения ядерного реактора на 40 МВт на тяжёлой воде, IR-40 и завод по производству тяжёлой воды/техническая возможность получения оружейного плутония), Фордо близ Кума в глубине горного массива (завод по обогащению урана), Парчин (сравнительно маломощное, но очень хорошо защищённое предприятие по обогащению урана, вызывающее гипертрофированный интерес МАГАТЭ, скорее всего потому, что туда настойчиво не допускают инспекторов МАГАТЭ) и Ардакан (производство ядерного топлива). Нужно надеяться, что Анарак (место захоронения ядерных отходов) не входит в планы бомбёжек по очевидной причине и едва ли включена обслуживаемая с участием российских специалистов Бушерская АЭС, если, конечно, в планы американских параноиков не входит использование Ирана как «спички» очередной мировой войны.

Даже эта первая фаза горячей войны для Стратегического командования США сопряжена со значительными трудностями. Персидский залив – не самое спокойное место для авианосцев США. Россия предупредила, что военные корабли США, в том числе оборудованные системами ПВО, и любой коалиции под эгидой США в соответствии с международным правом не могут заходить в Чёрное море, и не будут приветствоваться Российским Черноморским флотом. Пролёт американских летательных аппаратов над территориями суверенных государств Персидского залива за исключением Саудовской Аравии может представить серьёзную военно-дипломатическую проблему.

Кроме того, хорошо укомплектованы и укрыты характером ландшафта приграничные системы ПВО Ирана и ещё лучше укомплектованы системы ПВО ядерных объектов, включая современные комплексы, назначенные на ведение боевых действий в условиях трёхмерного ТВД. Таким образом, самая приблизительная оценка боевых потерь ВВС США при проведении военной операции против Ирана превысит 50% задействованных единиц техники.



ядерные объекты Ирана.

Как уже отмечалось Персидский залив и Чёрное море не могут рассматриваться как приемлемые акватории для действий ВМФ США. Оперативное пространство ВМФ будет ограничено Оманским зали-

вом и Средиземным морем, что диктует ограничения и предсказуемость направления десантных операций – южная хорошо защитимая граница Ирана (побережье Оманского залива) и, может быть, иранско-азербайджанская граница, но здесь Азербайджану есть, что терять в случае провала американской агрессии. Предсказуемость десантирования приводит к оценке чрезвычайно высоких (80-90%) потерь, как морских пехотинцев, так и самого флота, вынужденного находиться в пределах достижимости для иранских ракет средней и меньшей дальности.

Сухопутные операции ВС США на территории Ирана могут осуществляться за счёт авиационного десантирования, флотского десанта и сил вторжения с территории Афганистана. Авиационное десантирование в горной местности приемлемо лишь для проведения локальных диверсионных мероприятий и имеет крайне низкую вероятность успеха в иранской социальной среде. Организация вторжения с территории Афганистана неизбежно будет иметь самые острые внутриполитические последствия и будет связана с очень высокими потерями в боях с мотвированными, дисциплинированными и хорошо подготовленными соединениями стражей исламской революции.

Для возникновения дестабилизации внутреннего положения в США, вообще говоря, и судя по событиям времён Вьетнамской войны, хватило бы расширения вовлечённости США в военные конфликты во всём мире и осознания большинством граждан США возрастания антиамериканских настроений, в том числе и в странах – союзниках США по НАТО. Милитаризация внешней политики поглощает значительные материальные и финансовые ресурсы и как Молох перемалывает человеческие жизни. С ростом военных потерь связан значительный рост протестных настроений. Этому способствует и память о жертвах во Вьетнамской войне, и потрясающей художественной и моральной силы памятник жертвам Вьетнамской войны в Вашингтоне, который является перманентным напоминанием о событиях, унесших множество жизней американских солдат, о событиях, связанных с множеством военных преступлений и осуждённых американским обществом.

Однако, не только перманентное участие в вооружённых конфликтах, не только содержание бесчисленных военных баз, военных миссий по всему миру для реализации так называемого «Меморандума Вулфовица» (1992), который предусматривал постоянное военное присутствие США на всех шести континентах для сдерживания «потенциальных соперников, претендующих на роль регионального или глобального лидера» (на шестом континенте это, вероятно, пингвины), но и отсутствие согласия в американском обществе относительно будущего страны вызывает серьёзнейший социальный

кризис, разворачивающийся на фоне глубокого финансово-экономического кризиса. Политика сдерживания времён холодной войны заменилась новой амбициозной стратегией, предназначенной «установить и защитить новый миропорядок» в формате, продвигаемом неоконсерваторами, но неприемлемом для примерно половины американского общества.

Автор нашумевшей книги «Самоубийство сверхдержавы: доживёт ли Америка до 2025 года/«Suicide of a Superpower: Will America Survive to 2025?»», крайне правый консерватор, бывший кандидат в президенты США Патрик Д. Бьюкенен 24 марта 2003 года опубликовал в журнале «Американский консерватор» статью «Чья война?» с примечательным подзаголовком – «Неоконсервативная клика стремится завлечь нашу страну в серию войн, которые будут вестись не в американских интересах».

В ней автор утверждает, что «сегодня Америка стоит перед важным решением – начинать ли ей серию войн на Среднем Востоке, которые, скорее всего, приведут к национальной трагедии и катастрофе.

Раскрученный маховик войны нельзя будет остановить на каком-то определённом рубеже. Его можно будет только сломать. Вместе с самой Америкой, ставшей заложницей чуждого ей «неоконсерватизма»[173].

Он совершенно последовательно откликнулся и на сирийскую авантюру современного военно-политического руководства США[174]. В частности он обратился к истории американской традиции, той традиции, как её понимает Патрик и как её понимаем мы, той традиции, которая формировалась до времён оккупации США в XIX – начале XX века: «Пока в Европе не были урегулированы религиозные и этнические конфликты, там веками лилась кровь, и наши отцы учили нас держаться подальше от этих ссор, так как они – не наше дело. Тем более не наше дело Сирия в 2012 году».

Для него неприемлема логика Ричарда Пёрла, бывшего заместителя обороны США – Ричард Пёрл как-то обмолвился, что «Мубарак не такой уже и друг Америки. Можно найти ему и лучшую замену». Конечно можно, и замену, не обязательно лучшую, нашли за счёт тысяч загубленных жизней, разрушения экономики Египта и сдвига в сторону теократизации власти.

П. Бьюкенен обвиняет неоконсерваторов в том, что «нынешняя воинственная политика, полная высокомерия и самонадеянности, отталкивает от нас всех наших друзей и союзников, как в западном мире, так и в исламских странах». Этот новый «Pax Americana», предлагаемый неоконсерваторами, способен ввергнуть Америку в такие времена, когда, по словам Гарри Барнса (Harry Barnes), «будет идти перманентная война за перманентный мир». Бьюкенен пишет: «Разрушаются города, гибнет множество мирных

173 Бьюкенен Патрик Д. – Чья война? Американский консерватор. 24.03.2003

174 Бьюкенен Патрик Д. – Восстание в Сирии – не дело Америки. Американский консерватор. 08.06.2012

Источник: www.liveinternet.ru

Патрик (Пат) Джозеф Бьюкенен

жителей, в том числе стариков, женщин и детей. Идеологи Армагеддона, «Четвёртой мировой войны», сеющие зло и разрушение по всему миру, полагают, как и руководители Третьего Рейха, что сами они окажутся неуязвимыми для возмездия», будучи твёрдо уверенным, что им не удастся уйти от заслуженного возмездия.

Для него, также как и для нас, неприемлема бандитская логика неоконсерваторов: «Мы должны не просто разоружить, но и сокрушить режимы в Дамаске, Багдаде, Триполи, Тегеране и в секторе Газы таким образом, чтобы никто и не помышлял выступать против США или Израиля». Этот план был опубликован 1 января 2001 года, т. е. за девять месяцев до трагедии 11 сентября.

Выдавая теоретически вероятное за практически возможное, В. Истомин полагает, что уже в первой декаде XXI века «любой катаклизм может разодрать лоскутное одеяло США» и картинно представляет похороны этой державы, укладывая в гроб символ Свободы[175].

Хочется предупредить обескураженного читателя, что, во-первых, в глазах общественного мнения большинства стран мира, включая США[176], понятие свободы и демократии, символизируемое статуей Свободы, давно разошлось с восприятием социально-политической ситуации в США. Многие американцы осознали неприемлемость силовых методов насаждения демократии – «And that does not mean democracy enforced by a sword» [177].

Во-вторых, теоретически вероятное далеко не всегда становится практически возможным, и описываемые В. Истоминым вполне реальные предпосылки распада США, обусловленные вполне объективными интересами отдельных штатов или их более или менее аффинных кластеров, натыкаются, с одной стороны, на исторически сложившуюся экономическую взаимозависимость всех штатов и, с другой стороны, на отсутствие интереса к осуществлению такого события, как со стороны национальных олигархов, так и со стороны, что даже более важно, мирового банковско-финансового консорциума, использующего современные США в качестве геополитической площадки силового продвижения консорциума к завоеванию мирового господства. При этом подавляющее большинство населения США отдаёт себе отчёт в том, что три квартала в году оно кормится за счёт подачек со сто-

175 Истомин Всеволод – Разъединённые Штаты. Газета «Наше время». 19 августа 2007

176 Manning Jerry – We get what we deserve – we deserve what we get. Proc. IAS PNS. Moscow. 2007, vol. 2, issue 1

177 Manning Jerry – Helplessness or hopefulness – something you can do. Proc. IAS PNS. Moscow. 2007, vol. 2, issue 1

роны этого консорциума из средств, добываемых ограблением большинства народов мира[178].

Тем не менее, если заменить титул статьи В. Истомина с географического «Разъединённые штаты» на социальный – «Разделённая Америка» (книга американских авторов), то нужно отметить, что проблема разделения населения США по социальному признаку уже с начала 70-х годов прошлого века привлекает повышенное внимание и американских социологов, и американских писателей.

Источник: telegrafia.com

Ритуальные похороны статуи Свободы как знак развала США.

На фоне более чем семнадцатитриллионного государственного долга США более индикативна статья специалиста по Ближнему Востоку Линды Хёрд[179], в которой она утверждает, что к 2007 году «Соединённые Штаты просчитались во всём, и их просчёты привели к тому, что сегодня Америка слабее, чем когда бы то ни было», и приводит конкретные факты последствий стратегических ошибок администраций Клинтона и Буша, мл. во внешней политике. В заключение своей статьи она пишет: «Так, когда же американский народ прозреет? Их доллар потерял 25 процентов покупательной способности, их пенсии под угрозой, они не могут продавать свои дома, на горизонте маячит новая война, и идут разговоры о возвращении к призывной системе.

Ещё несколько лет назад неоконсерваторы со своей гегемонистской программой крайне меня тревожили. Теперь можно успокоиться». Ну, в этом Линда Хёрд явно погорячилась – успокаиваться вряд ли стоит, но её статья явно указывает на то, что поле возможностей ограбления других народов, ergo поле возможностей подкупа американского народа резко сужается. Это ведёт к накоплению латентных зон социальной напряжённости, что, естественно, повышает вероятность дестабилизации всего социума, его хаотизации с последующим переходом к новому устройству страны, скорее всего, на принципах этнической сегрегации[180].

---

178 Manning Jerry – Think about it. Proc. IAS PNS. Moscow. 2007, vol. 2, issue 1

179 Хёрд Линда – США больше не способны править миром. «Gulf Times», Арабская пресса. 14 августа 2007 года

180 Курепина Н. С., Спектор В. Н. – Факторы сегрегации и агрегации национально-государственных социумов. Труды МАН ПНБ. М., том 2, вып. 4, с. 8

Джерри Маннинг

В-третьих, несмотря на «во-вторых», далеко не любое потрясение может на практике привести к развалу США, хотя понукаемые и в значительной мере управляемые неоконсерваторами, последние 4-5 администраций США делали всё для того, чтобы он случился.

В настоящее время, проиграв президентскую гонку и не желая идти на компромисс по «бюджетному/налоговому обрыву» и по расширению пределов национального долга, 11 контролируемых демократами штатов, включая Техас (штат, вошедший в состав США как независимое государство), собрали достаточное количество подписей для получения независимости и выхода из США. Уже после написания этого раздела в прессе появилась информация, что сбор подписей о выходе из США начался ещё в 19 штатах[181].

Не следует думать, что план республиканцев в настоящее время состоит в развале страны. Скорее, эти плебисциты – оружие во внутригосударственной информационной войне, призванное стать рычагом влияния и получения преимуществ в переговорах с президентом. Дополнительным фактором, осложняющим положение администрации президента, является то, что для президента возникла ситуация цейтнота – его разногласия с Конгрессом должны быть урегулированы до конца декабря 2012 года.

Эта инициатива республиканцев указывает на то, что при определённых условиях теоретическая вероятность распада США может актуализироваться в практических действиях, и перейти из состояния информационной войны в войну гражданскую. Именно стремление южных штатов выйти из состава США и образовать независимую конфедерацию с целью сохранения там рабовладельческого уклада и торговли людьми привели в своё время, в начале истории США, к гражданской войне «Север – Юг» (1861-1865) [182].

Таким образом, в случае принятия решения о войне с Исламской республикой Иран США войдут в неё с реальной перспективой протестной волны, дестабилизирующей американский социум, с разделённой политической элитой, при возражении многих военных аналитиков, как это уже было после принятия решения о Косовской операции и на фоне решительного несогласия со стороны России, Китая (то есть без соответствующих санкций Совета безопасности ООН) и со стороны большинства в Генеральной ассамблее ООН. Случись эта война, она грозила бы практически полным уничтожением

181 Евроньюс, 14.11.2012 и 17.11.2012

182 Poe Alan Edgar – The Red Badge of Courage

Израиля (и нам, конечно, жаль наших бывших соотечественников по СССР, составляющих почти треть населения Израиля), массированными разрушениями в странах Ближнего Востока, Южного Кавказа и Южной Европы, на территориях которых размещены американские военные базы, если, конечно, эти страны не введут запрет на использование этих баз в такой войне.

Совершенно иная ситуация выявляется при беспристрастном анализе готовности Ирана к подобной вооружённой конфронтации. Начнём с того, что в мировом общественном мнении Иран предстанет в качестве жертвы агрессии, и при обсуждении ситуации на Генеральной ассамблее ООН США рискуют получить более 104 голосов в осуждение их действий, то есть больше, чем СССР получил по поводу афганской войны.

Ядерная риторика здесь не сработает сразу по двум причинам.

Во-первых, стратегический партнёр США в регионе, Израиль располагает ядерным арсеналом, превышающим необходимости национальной безопасности. Более 700 (скорее, ближе к 1000) ядерных боеголовок во всех элементах ядерной триады, включая водородные и нейтронные боеприпасы, несколько гигатонных бомб и неядерные устройства генерации мощных ЭМИ, обеспечивают Израилю, по утверждению его же руководства[183], возможность вооружённого противостояния всему миру, всему миру «параллельного человечества»[184]. Даже предположив наличие у Ирана двух-трёх десятков единиц маломощных ядерных боеприпасов, полученных из внешних источников и назначенных на сдерживание потенциального агрессора, это не идёт ни в какое сравнение со стратегическим ядерным потенциалом хоть США, хоть Израиля.

Во-вторых, мировое общественное мнение уже слышало подобные причитания в обоснование двух иракских войн, так что ни американской разведке, ни систематически «подставляемому» ею по указанию «мирового правительства», представляемого в элите США неоконсерваторами, политическому руководству США в мире нет веры. То есть политическое руководство иностранных государств твёрдо знает, что формальная администрация США чаще всего принимает важнейшие военно-политические решения под действием скрытого внешнего фактора.

Единственным важным козырем в подобной операции может стать применение оружия геоцентрического ТВД. Едва ли можно сомневаться, что США уже используют и будут в ещё большем масштабе использовать этот козырь, несмотря на явно недостаточное исследование способов и последствий его применения. Даже сама легитимность его разработки ставится под сомне-

---

183 Спектор В.Н. – Ортодоксальный иудаизм и проблемы глобальной стабильности. Труды МАН ПНБ. М., том 2, вып. 4, с. 14

184 Барац А. – «Презумпция человечности» (европейская культура в контексте иудаизма). Иерусалим, 1998

ние советником трёх президентов США Р. Кларком: «На протяжении первого десятилетия XXI века Соединенные Штаты развивают новый тип вооружения, основанного на новейших технологиях, а продуманной стратегии у нас нет. Мы создали новое командование для ведения новой высокотехнологичной войны, пренебрегая публичными дебатами, обсуждениями в СМИ, серьёзным парламентским надзором, академическим анализом или международным диалогом. Мы живём во время, в чём-то поразительно схожее с 1950-ми годами. Наверное, мы должны принять участие в просвещённой дискуссии и провести строгий анализ этого нового вида оружия, нового вида войны.

Речь идёт о киберпространстве и войне, которая ведётся в нём. 1 октября 2009 года начало работу новое подразделение Министерства обороны – Кибернетическое командование США, миссия которого заключается в использовании информационных технологий и Интернета в качестве оружия. Подобные подразделения существуют в России, Китае и ряде других стран. Эти военные и разведывательные организации готовят кибернетическое поле битвы <…>. В силу особенностей характера кибервойны у многих может возникнуть желание нанести первый удар. И в первую очередь это затронет не военных, а мирных граждан. Скорость, с которой можно поразить тысячи целей практически на всей планете, грозит стремительно развивающимися кризисами. Сила, которая предотвратила ядерную войну, – устрашение – не поможет при кибервойне. Сам феномен кибервойны покрыт такой завесой секретности, что по сравнению с ней даже холодная война кажется эпохой гласности и открытости. Но самый большой секрет кибервойны, пожалуй, заключается в том, что США, готовясь к наступательной войне, в то же самое время продолжают вести политику, при которой эффективная защита нации от кибератаки невозможна.

Страна, которая изобрела новую технологию и тактику её применения, может и не стать победителем, если её вооружённые силы зациклились на методах прошлого и слишком надеются на оружие, которое привыкли считать непревзойдённым. Создатели нового наступательного оружия могут проиграть, если не выяснят, как защищаться от оружия, которое они уже продемонстрировали всему миру».

Более того, у США уже есть опыт боевого применения такого оружия против ядерного объекта в Сирии. Это описано в работе одного из ведущих американских разработчиков современного ядерного оружия и координатора на уровне советника президентов США киберкосмического и информационного оружия, проф. Ричарда А. Кларка[185].

---

185 Кларк Ричард, Нейк Роберт – Третья мировая война: какой она будет? Высокие технологии на службе милитаризма. Изд. «Питер». 2011, 132 с. [pentagonus.ru› Книги› ... r_klark_tretja_mirovaja...

Приведём относящиеся к делу выдержки из книги Р. Кларка.

«Стояла ночь 6 сентября 2007 года, и у Евфрата вот-вот должна была произойти атака нового типа – та, что началась в киберпространстве. На восточном берегу реки, в ста двадцати километрах на юг от турецкой границы, косые тени разрезали песчаные стены высохшего русла реки. Большое строящееся здание тускло светилось. Шестью часами ранее из него вышли многочисленные рабочие из Северной Кореи, дисциплинированно выстроившись в очереди, чтобы сесть в автобусы и отправиться в общежитие. Для стройплощадки это место выглядело слишком тёмным и незащищённым, как будто подрядчик опасался привлечь внимание. Вдруг маленькие звёздочки, горевшие над стройплощадкой, вспыхнули и залили пространство бело-голубым светом, стало ярче, чем днём. Это длилось не больше минуты, хотя нескольким сирийцам и корейцам, оставшимся на стройке, показалось, что прошла вечность. Сверкнула слепящая вспышка, затем прокатилась оглушающая звуковая волна, и всё превратилось в развалины. Если бы люди <…> могли видеть сквозь пламя, уничтожавшее стройку, то заметили бы высоко в небе, над сигнальными ракетами, которые всё ещё спускались на маленьких парашютах, они заметили бы, как несколько истребителей F-15 Eagles и F-16 Falcons повернули на север и полетели по направлению к Турции. А кто-то мог бы даже разглядеть сине-белые звёзды Давида на крыльях самолетов военно-воздушных сил Израиля, полностью уничтоживших плод многолетней секретной работы. Почти столь же необычным, как и этот налёт, стало дальнейшее политическое безмолвие. <…>

Сирийские вооруженные силы ожидали сигнала тревоги. Однако ничего необычного на экранах радаров не наблюдалось. Полночь приближалась, а небо над Сирией казалось мирным и почти пустым. На самом деле со стороны Турции в сирийское воздушное пространство вторгся строй истребителей Ф-15 и Ф-16. Эти самолеты, спроектированные ещё в 1970-х, сложно не заметить. Их корпуса из стали и титана, острые рёбра и углы, бомбы и ракеты, свисающие с крыльев, должны были расцветить сирийские радары, как рождественскую ёлку на Рокфеллер-плаза в декабре. Но этого не произошло. На следующее утро сирийцы медленно, с неохотой, мучительно пришли к выводу, что накануне ночью Израиль «завладел» дорогущей сетью сирийской противовоздушной обороны. Экраны радаров показывали то, что им приказывали военно-воздушные силы Израиля, – пустоту. Картинка, которую видели сирийцы, не имела никакого отношения к действительности, а в это время израильские самолёты с востока проникли в воздушное пространство Сирии.

Сирийские ракеты противовоздушной обороны не запускались потому, что не видели целей. Сирийские истребители ПВО не могли взлететь, поскольку системы российского производства управляются с земли, а сирийские наземные управляющие устройства цели не видели.

Источник: ru.wikipedia.org

Ричард Алан Кларк

Ближе к вечеру зазвонили телефоны в российском Министерстве обороны. Почему это российская система ПВО ослепла? Сирия хотела бы знать ответ. Москва пообещала тотчас же выслать экспертов и техников. Российскому военно-промышленному комплексу не нужна такая дурная слава. Тем более, Иран уже почти купил у Москвы новую систему радаров и противовоздушных ракет. Это был шок для командиров противовоздушной обороны и в Тегеране, и в Дамаске. Кибервоины всего мира, однако, не удивились. Так в информационную эпоху и должна вестись война – кибервойна. <…>

Управление по связям с общественностью израильского правительства молчало. Что ещё более странно, Сирия, которая подверглась бомбардировке, не сделала никаких заявлений. Постепенно история начала просачиваться в американские и британские СМИ. Израиль нанёс удар по комплексу в Восточной Сирии, который строила Северная Корея. Здание было связано с производством оружия массового поражения, утверждали СМИ, ссылаясь на неназванные источники. Израильские цензоры позволили своим газетам процитировать сообщения американских средств массовой информации, но запретили писать собственные комментарии. Это, утверждали они, вопрос национальной безопасности.

Президент Джордж Буш, нехарактерно молчаливый, категорически отказался отвечать на вопрос репортёра об израильской атаке».

Ему, было, пожалуй, труднее других, так как он точно знал, что акция выполнена американскими ВВС независимо от звёзд на крыльях и был уверен, что рано или поздно, скорее рано, это станет известным фактом. Что и случилось[186] – сенсационную информацию распространила израильская газета The Jerusalem Post со ссылкой на Al-Jazeera. Оказывается недавний авианалёт на Сирию, в результате которого, как предполагается, был разрушен строящийся ядерный реактор, был осуществлён не израильскими, а американскими ВВС, то есть ВВС США применили тактическое ядерное оружие для уничтожения объекта на территории иностранного государства.

В апреле 2008 года ЦРУ предприняло необычный шаг – представило и опубликовало видеозапись того, что происходило в здании накануне бомбардировки. Фильм практически не оставлял сомнений в том, что это была северокорейская ядерная установка.

---

186 США нанесли ядерный удар по Сирии. – Newsland no-reply@newsland.ru 3 ноября 2007

Понятно, что помощник президента по кибербезопасности, самим своим присутствием на месте действия подтвердивший, что операция была американской, врал по профессиональной причине, но само его присутствие на месте действия свидетельствовало о важности для США этой операции по испытанию новой боевой технологии.

Однако эти технологии, на которые так уповают в Минобороны США для их успешного применения в стратегических целях, например, в полномасштабной войне, требуют и от операторов, и, что ещё более важно, от политического руководства принципиально новой философии ведения военных действий и принципиально нового уровня осознания динамической картины развития конфликта и времени релаксации понимания изменений этой картины на геоцентрическом театре военных действий.

Более того, хотя и недостаточным, но необходимым условием реальной победы, а не погрома является, как будет показано в последующих разделах, наличие консолидированного политического руководства, выступающего в качестве внешнего по отношению к армии оператора «заимствованной позиции», используемой для преобразования статического образа диспозиции на ТВД в динамический образ замыслов противника:

В отличие от политического руководства ИРИ политическое руководство США ни сейчас, ни в среднесрочной перспективе нельзя, во-первых, назвать консолидированным и, во-вторых, считать самостоятельным. Если же считать мировой банковский консорциум внешним по отношению к американской армии оператором «заимствованной позиции», то это изначально ставит армию в проигрышную ситуацию.

Именно это, а не соотношение вооружённых сил и вооружений, не существенно большая свобода вооружённых сил Ирана в выборе ответных действий, как бы странно это ни звучало в отношении обороняющейся стороны, предопределяет чрезвычайно высокую вероятность поражения США в случае развязывания войны с Ираном.

В отличие от прогноза проф. Р. Кларка, проявленными факторами уязвимости США могут стать высокое потери в результате действий по ситуативно детерминированной тактике поражения предварительно выбранных целей (preconcieved targets); деморализующие акты диверсий и саботажа иранскими смертниками на территории США, в том числе с применением маломощных ядерных и радиобиологических, химических и бактериологических боеприпасов и малых форм ЭМИ технологий в случае использования США ОМП против Ирана (руководство Ирана публично и открыто предупреждало о такой альтернативе); уничтожение прибрежными торпедными и ракетными комплексами, торпедными и ракетными катерами, авиацией и подводными лодками Ирана, боевых кораблей ВМФ США, в первую очередь авианосцев, в ловушке Пер-

сидского залива; частичное или полное разрушение американских военных баз в государствах Персидского залива с провоцированием методами информационной войны (призыв ко всем мусульманам, объявление джихада и т. п.) вооружённых выступлений шиитов в этих странах, а в Израиле – предваряющим массивным ракетным ударом (более 10 тысяч ракет всех типов с традиционными боеголовками) по площади для преодоления и уничтожения «Железного купола» с последующим ударом ракетами с ядерными боеголовками по выбранным целям, в первую очередь по инфраструктуре и израильским носителям ядерных вооружений. Большой помощью усилиям Ирана по нейтрализации Израиля как стратегического партнёра США могут стать действия Хэзболы, Хамаза и других освободительных движений в Палестине и Ливане, получающим в этом случае реальную возможность поквитаться за десятилетия национального унижения и готовым голыми руками завершить дело разгрома врага.

Турция и Италия, несмотря на статью 5 Устава НАТО (США выступают агрессором, а не жертвой агрессии), скорее всего, запретят использование американских военных баз на своей территории и пролёт ЛА ВВС и ВМФ США в своём воздушном пространстве в случае войны США с ИРИ, также как и некоторые исламские государства Персидского залива, что сделает ненужными удары по этим странам, и позволит Ирану сконцентрировать свои ответные действия на государствах, решивших поддержать агрессию США против Ирана.

Естественно, принятие такой гибкой стратегии противостояния потребует от Ирана принесения в жертву значительной части объектов своей ядерной инфраструктуры, которая может быть восстановлена в течение нескольких лет после окончания войны. Победа ИРИ в подобной войне при принятии такой стратегии становится уже не только высоко вероятной, но и практически неизбежной. Кроме того, высока вероятность того, что в этом случае произойдёт распад США ещё до фактического окончания войны.

Рассмотрим концептуальные основы действий на геоцентрическом ТВД, на которые так уповают Соединённые штаты в своей милитаристской и гегемонистской политике и в возможностях ведения которых США являются если не исключительным, то наиболее продвинутым игроком.

Однако, в той же работе Р. Кларк[187] посмотрел на проблемы, возникающие в случае информационной/кибернетической войны, с американской точки зрения.

Конечно, мы ещё не видели полномасштабной кибервойны, но легко можем представить себя её жертвой. Представьте день в недалеком будущем. Вы, помощник президента по вопросам национальной безопасности, собираетесь домой после рабочего дня, и вдруг вам звонят из оперативного

187 Кларк ... – Третья мировая ...

штаба Белого дома. АНБ передало сообщение CRITIC – редкий сигнал тревоги, свидетельствующий о том, что произошло нечто действительно важное. Вам сообщают: «Несколько разных вредоносных программ «нулевого дня» атакуют американский сегмент Интернета, угрожая жизнедеятельности важнейших инфраструктур». Старший дежурный офицер оперативного штаба предлагает вам спуститься к нему и помочь разобраться, что происходит.

Когда вы добираетесь до оперативного штаба, на проводе директор управления оборонной связью. Он только что совещался с министром обороны, и тот посоветовал позвонить вам. NIPRNET – несекретная сеть Министерства обороны – выходит из строя. Маршрутизаторы по всей сети непрерывно перезагружаются. Сетевой трафик, по сути, заблокирован. Пока он говорит эти слова, вы слышите, как кто-то на заднем фоне пытается привлечь его внимание. Когда генерал возвращается на линию, он спокойно произносит: «Теперь то же самое происходит в SIPRNET и JWICS». Значит, та же участь постигла секретные сети Министерства обороны.

Теперь с вами срочно хочет переговорить заместитель министра национальной безопасности, ещё не знающий, что происходит в Пентагоне. Из Федерального агентства по чрезвычайным ситуациям ему доложили, что два региональных офиса агентства, в Филадельфии и Дентоне (штат Техас), сообщают о крупных пожарах на нефтеперегонных заводах в Филадельфии и Хьюстоне, а также о выбросах смертельно опасного хлора на нескольких химических заводах в штатах Нью-Джерси и Делавэр. Он добавляет, что питсбургская компьютерная группа реагирования на чрезвычайные ситуации завалена отчётами о выходе из строя систем, но у него не было времени выяснить всё подробно.

Прежде чем вы успеваете поинтересоваться у старшего дежурного офицера, где президент, телефон начинает снова звонить. Это заместитель министра транспорта. «На нас напали?» – спрашивает она. В ответ на ваше «почему?» она выпаливает на одном дыхании, что случилось. В центре управления воздушным движением Федерального управления гражданской авиации в Херндоне (штат Вирджиния) полностью вышли из строя все системы. Альтернативный центр в Лисбурке в панике, поскольку другие региональные центры не видят, какие самолеты находятся в воздухе, и пытаются вручную установить местоположение и развести сотни самолетов. Из центра Брикьярд в Индианаполисе сообщают о столкновении двух «боингов». «Я думала, кризис затронул только авиацию, но затем начались аварии на железной дороге», – продолжает она. Федеральное управление железных дорог сообщает о крушениях товарных поездов в Лонг-Бич, Норфолке, Чикаго и Канзас-Сити.

Взглянув на информацию о местонахождении президента, вы видите «лаконичное – «в Вашингтоне». Он находится где-то за пределами Бело-

го дома. Словно читая ваши мысли, старший дежурный офицер объясняет, что президент повёл первую леди в ресторан. «Тогда соедините меня с начальником его секретной службы», – говорит кто-то. Это министр финансов прибежал из своего офиса в здании близ Белого дома. Только что звонил председатель Федерального резервного банка. Произошла крупная авария центров обработки данных, которая затронула даже резервные копии. Все данные потеряны. DTCC и SIAC тоже рушатся». Эти аббревиатуры, поясняет он, означают главные финансовые вычислительные центры Нью-Йорка. «Теперь никто не знает, кому что принадлежит. К утру вся финансовая система рухнет».

Пока он говорит, вы невольно задерживаете взгляд на экране телевизора, где сообщается о сходе с рельсов поезда метро под Потомаком. На другом канале показывают пламя, бушующее в Вирджинии, где взорвался крупный газопровод. Затем начинает мигать освещение в оперативном штабе. Лампы гаснут. Включается аварийное освещение, работающее от аккумулятора, и комнату заполняют полосы света и тени. Плоские экраны телевизоров и мониторы компьютеров ничего не показывают. Свет снова начинает мигать. Издалека доносится громкое жужжание. «Это запасной генератор, сэр», – говорит дежурный офицер. Его помощник снова вручает вам телефон и произносит слова, которые вам так не хочется слышать: «На проводе президент».

Президент на своем гигантском бронированном автомобиле, напоминающем откормленный стероидами «кадиллак», возвращается из ресторана. Секретная служба эвакуировала его, когда погас весь свет, и теперь они с трудом передвигаются по городу. На улицах Вашингтона то и дело происходят аварии, поскольку не работают светофоры. Президент хочет знать, правда ли то, что ему сообщил агент секретной службы, – все Восточное побережье осталась без электричества? «Хотя-, подождите… Что? Команда вице-президента сообщает, что в месте нахождения их шефа электричества нет. Разве он сегодня не в Сан-Франциско? Сколько там сейчас времени?»

Вы смотрите на часы. Всего 20:15. За четверть часа 157 мегаполисов остались без электричества. Облака ядовитого газа несутся на Уилмингтон и Хьюстон. Пылают нефтеперегонные заводы. Аварии в метро Нью-Йорка, Окленда, Вашингтона и Лос-Анджелеса. Товарные поезда сошли с рельсов на крупнейших железнодорожных узлах и сортировочных станциях четырёх главных железных дорог страны. Самолеты буквально падают с неба. Газопроводы взорвались, а миллионы людей замерзают. Финансовая система остановилась, потому что в центрах обработки данных уничтожены терабайты информации. Метеорологические, навигационные спутники и спутники связи покинули свои орбиты. Вооружённые силы США превратились в мно-

жество изолированных подразделений, безуспешно пытающихся связаться друг с другом. Несколько тысяч американцев уже погибли, многие ранены и пытаются добраться до больниц.

Жертв будет ещё больше, но люди, которые должны передавать вам информацию, не смогут выйти на связь. В ближайшие несколько дней города останутся без еды из-за выхода из строя системы железнодорожного сообщения, отключения программного обеспечения на оптовых базах и в транспортных компаниях.

Электричества не будет, потому что ядерные генераторы в целях безопасности заблокированы, а обычные электростанции серьёзно повреждены. Высоковольтные линии электропередач повреждены.

Некоторые жители страны, не сумев снять наличные деньги, скоро начнут грабить магазины. Полиция и экстренные службы едва ли со всем этим справятся. В ходе войн, в которых участвовала Америка, ни одна страна не наносила такой урон нашим городам.

Сейчас с помощью хорошо спланированной кибератаки это способна совершить любая страна всего лишь за пятнадцать минут и без единого террориста или солдата на нашей территории. Почему же они не сделали этого до сих пор? По тем же причинам, в силу которых девять ядерных государств не применяли ядерное оружие с 1945 года, – им нужны причины. Но в отличие от ядерного оружия, когда нападающего может сдержать ожидание ответных мер или радиоактивная «отдача» по собственной стране, запуск кибератаки сопряжён с меньшими рисками. В кибервойне мы можем никогда не узнать, кто нанёс удар. В самом деле, едва ли для дрожащих от холода американцев утешением станет мысль о том, что США отплатят вероятному противнику тем же.

«Пока вы были на линии с президентом, сэр, мне звонили из Киберкомандования. Они считают, что нас атаковала Россия, и готовы оставить без света Москву, сэр. Или это был Китай, так что они ударят по Пекину, если вы прикажете. Сэр?»

Поле битвы Киберпространство.

Можно представить, будто это ещё одно измерение, по которому скользят зеленые светящиеся столбики цифр и букв, как в «Матрице». Но на самом деле всё ещё проще. Киберпространство – это ноутбук, с которым ваш ребенок ходит в школу, ваш настольный компьютер на работе, тёмное здание без окон в деловом районе города и кабель, протянутый под дорогой. Оно везде, где есть компьютер, процессор или сеть, связывающая их. И всё это теперь – территория войны, где произойдёт множество решающих битв XXI столетия.

Чтобы понять почему, мы должны ответить на несколько важных вопросов. Что такое киберпространство? Как оно устроено? Как там будут проходить битвы? Как и почему возможна кибервойна? Киберпространство – это все компьютерные сети мира и всё, что их объединяет и контролирует.

Это не только Интернет. Давайте проясним разницу. Интернет – открытая сеть из множества сетей. Из любой части Интернета вы можете связаться с любым компьютером, связанным с Интернетом, где бы он ни находился. Киберпространство состоит из Интернета и множества других сетей компьютеров, которые не считаются доступными из Интернета. Некоторые из этих сетей похожи на Интернет, но они, по крайней мере, теоретически, не связаны с ним.

Другие части киберпространства – деловые сети, по которым передаются данные о денежных потоках, торговле на фондовых биржах и операциях по кредитным картам. Некоторые сети являются контролирующими системами, позволяющими одним устройствам общаться с другими, – в той же степени, как панели управления отдают команды насосам, лифтам и генераторам.

Но как эти сети превращаются в поле сражения? В самом широком смысле в них могут проникнуть кибервоины, чтобы взять их под контроль или уничтожить. Если кибервоины захватывают сеть, они могут выкрасть всю информацию или отдать команды, чтобы перевести деньги, разлить нефть, выпустить газ, взорвать генератор, вызвать крушение поезда, разбить самолёт, послать взвод в засаду или заставить ракету сдетонировать не там, где нужно. Если кибервоины взламывают сети, крадут данные или превращают компьютер в фильтр, дозирующий информацию, это грозит коллапсом финансовой системы, прерыванием цепочки поставок, сходом спутника с орбиты, остановке полетов.

Это вовсе не предположения. Подобное уже происходило в порядке эксперимента, по ошибке или небрежности. Как отметил адмирал Макконел, «информацию, передаваемую по компьютерным сетям, ту, что управляет нашими коммунальными услугами, транспортом, банковскими операциями и коммуникациями, могут использовать или уничтожить за несколько секунд из любой точки планеты, из-за океана. Ни одна флотилия, никакие межконтинентальные ракеты или регулярные армии не сумеют отразить такие атаки, ведь нападающий находится не просто за пределами наших границ, но и за пределами нашего физического пространства, в мире цифр».

Зачем же мы тогда используем столь сложные компьютерные сети, которые допускают несанкционированный доступ и несанкционированное управление? Разве не существует мер безопасности? Архитектура компью-

терных сетей, программное и аппаратное обеспечение дают кибервоинам тысячи возможностей обойти любую защиту.

Программы пишут люди, а людям свойственно ошибаться и отвлекаться. Сети, которые, как считается, не связанными с Интернетом, на самом деле часто оказываются связаны с ним, что остается тайной даже для их владельцев.

Давайте возьмём любое устройство, которым вы ежедневно пользуетесь, чтобы наглядно объяснить, как может случиться кибервойна. Как вы думаете, знают ли в вашем ТСЖ, что лифт, установленный в вашем доме, «звонит домой» (как в фильме «Инопланетянин»)? Ваш лифт через Интернет связывается с людьми, которые сделали его.

А знаете ли вы, что ксерокс в вашем офисе, возможно, ведёт себя так же? Героиня Джулии Робертс из фильма «Ничего личного» (Duplicity) знала, что многие копировальные аппараты имеют выход в Интернет и могут быть взломаны, но большинство об этом даже не догадывается. Ещё меньше людей в курсе последнего трюка – шредеры, машинки для уничтожения бумаг, могут делать копии документов! Прежде чем засекреченные документы отправляются под нож, они проходят перед камерой, которая их фотографирует. Вечером парень-уборщик заберёт новую коллекцию «изображений» и отправит её тому, кто его нанял.

Лифт и ксерокс «звонят домой» – это звучит правдоподобно. А что, если у вашего конкурента есть программист, которые написал несколько строк кода и внедрил его в процессор, который стоит в вашем ксероксе? Предположим, эти несколько строк программного кода заставляют его сохранять изображения всего, что он копирует и помещать в архив. Однажды ксерокс получает доступ в Интернет и – пинг! – отправляет этот файл через всю страну вашему конкуренту.

Или, ещё хуже, в день, когда ваша компания должна участвовать в конкурсе на заключение крупного контракта, – пинг! – ксерокс самовозгорается, из-за чего включается противопожарная система, весь офис залит водой, и вы не успеваете вовремя отправить заявку. Конкурент выигрывает, а вы остаетесь ни с чем. Используя подключение к Интернету, о котором вы даже не подозревали, кто-то написал программу и внедрил её в ваш ксерокс, процессор которого оказался, как ни удивительно, достаточно мощным. Затем кто-то использовал программу, чтобы заставить ксерокс сделать что-то, не свойственное его обычным функциям, например, короткое замыкание. Он знал, что в результате возникнет пожар, возможно, он экспериментировал с другими такими же копировальными аппаратами. В итоге сработала противопожарная система и залила водой ваш офис, а вы подумали, что произошел несчастный случай.

Незнакомец дотянулся до вас из киберпространства и организовал хаос в пространстве физическом, это и был хакер. Изначально хакерами называли людей, которые умели писать команды на языке компьютеров, чтобы заставить их делать что-то новое. Когда хакеры проникают в систему, доступ в которую им не разрешён, они становятся киберпреступниками, а если они работают на вооружённые силы США, их называют кибервоинами.

В данном сценарии киберпреступник использовал Интернет как средство – сначала для получения информации, затем для нанесения вреда. Его оружием стали несколько строк кода, которые он дабавил в процессор копировального аппарата. Можно рассудить иначе: с помощью программы он превратил ваш ксерокс в оружие. Ему это удалось, поскольку программу, управляющую ксероксом, можно изменить. Создатели копировального аппарата не думали, что кто-то способен превратить его в оружие, поэтому и не пытались воспрепятствовать этому на этапе написания программы.

То же самое относится к проектировщикам сети электропередачи других систем. Они не думали, что кто-то в них проникнет и превратит их в оружие. Ваш офис-менеджер не обратил внимания на слова продавца о том, что копировальный аппарат предоставляет возможность дистанционной диагностики, позволяет загружать обновления, устранять проблемы и запрашивать нужные для ремонта запчасти. А хакеры это заметили или просто исследовали соседнее киберпространство и нашли адрес «Хеопега Copier 2000, серийный номер 20-003488, Ваша Компания, Inc.».

Если вы сомневаетесь в том, что копировальные аппараты являются частью киберпространтсва, почитайте Image Source Magazine: «Раньше для дистанционной диагностики требовался модем. Методика того времени была несколько неудобной для потребителя и дорогой для поставщика, которому рядом с каждым устройством приходилось устанавливать телефонные розетки и распределительные коробки для совместимости с телефонными аппаратами клиента. Но эти барьеры исчезли с появлением Интернета и беспроводных сетей. Теперь, когда все устройства имеют адрес в сети, диагностическое сообщение об ошибке передаётся в режиме реального времени, и устройство само может связаться со специалистами ещё до того, как его владелец узнает о проблеме.

Сегодня сервисным центрам просто непростительно игнорировать экономию затрат, которую обеспечивает дистанционная диагностика. Практически каждый производитель принтеров использует либо собственные инструменты дистанционной диагностики (например, Remote от компании Ricoh, Kyocera Admin и Admin от компании Sharp, DRM от компании Xerox), либо сотрудничает с третьей стороной, такими компаниями, как Imaging Portals или Print Fleet».

Этот хоть и банальный, гипотетический сценарий полезен потому, что демонстрирует три аспекта киберпространства, которые делают кибервойну возможной:

1. дефекты в архитектуре сети Интернет;
2. дефекты программного и аппаратного обеспечения;
3. работа всё большего количества важнейших систем в режиме он-лайн.

Давайте рассмотрим каждый аспект в отдельности.

Уязвимости Интернета.

Существуют, по меньшей мере, пять основных уязвимых мест в архитектуре самого Интернета. Во-первых, это система адресации, которая всегда знает, кто и где находится в Интернете. Интернет-провайдеров иногда называют операторами, поскольку они оперируют трафиком в Интернете. Разнообразные компании производят маршрутизаторы, серверы, программное обеспечение, но именно интернет-провайдеры объединяют их.

Для удобства давайте разделим интернет-провайдеров на две категории.

Существуют национальные интернет-провайдеры, они владеют и управляют тысячами километров оптоволоконных кабелей, которые проложены по всей стране, соединяя крупные города. В США действует шесть таких крупных провайдеров (Verizon, AT&T, Qwest, Sprint, Level 3 и Global Crossing). Их называют магистральными интернет-провайдерами. Как только магистраль доходит до вашего города, она соединяется с множеством более мелких провайдеров, которые обслуживают местные предприятия и ваш дом.

Интернет-провайдерами могут быть телефонные компании или кабельное телевидение. Их кабели связывают ваш дом со всем остальным миром. Чтобы представить, как всё работает, и найти некоторые уязвимые места Интернета, посмотрим, что происходит, когда я соединяюсь с Интернетом. Я включаю ноутбук и открываю браузер. При этом я сразу выхожу в Интернет и попадаю на свою домашнюю страницу. Допустим, это будет веб-страница консалтинговой фирмы, в которой я работаю. Итак, сидя в своем домашнем офисе в округе Раппаханнок (штат Вирджиния), у подножья Аппалачей, а делаю клик мышкой, и мой браузер переносит меня на wwwjnycompany.com. Поскольку компьютер слов не понимает, адрес нужно перевести на машинный язык единиц и нулей. Для этого браузер использует систему доменных имён. Это что-то вроде телефонной справочной службы – вы называете имя человека, и вам дают его телефонный номер. Офис моей консалтинговой фирмы расположен в 120 километрах от моего дома в Вирджинии, но её веб-страница находится на удалённом сервере в Миннеаполисе и имеет адрес, например,

123.45 678.90. Столько цифр сложно запомнить. К счастью, этого и не нужно. Браузер обращается к системе доменных имён, чтобы найти адрес. Он посылает сообщение в базу данных сервера, который является составной частью сложной иерархии компьютеров, формирующих систему доменных имён.

Для кибервоинов система доменных имён – идеальная мишень. Её создавали, практически не задумываясь о безопасности, поэтому хакеры легко могут менять информацию и перенаправлять вас на фальшивые веб-страницы. Когда я открываю браузер, он посылает запрос на сервер, где расположена нужная мне веб-страница. Запрос разделяется на серию пакетов, каждый из которых передается отдельно. Давайте проследим путь одного пакета от моего компьютера до сайта. Первый «прыжок» совершается с компьютера на встроенную с него карту wi-fi, где пакеты превращаются в радиоволны и перелетают по воздуху на мой домашний wi-fi-маршрутизатор. Если этот маршрутизатор недостаточно защищён, хакеры могут проникнуть в компьютер через wi-fi соединение. Маршрутизатор ещё раз преобразовывает сигнал и отправляет его моему местному интернет-провайдеру в быстро растущий городок под названием Кэльпепер.

Это прекрасное местечко, но до центра киберпространства от него далековато. Поскольку город расположен далеко от зоны возможного ядерного взрыва, направленного на Вашингтон, именно здесь хранятся базы данных финансовых и правительственных институтов: например, узел AT&T (Американской телефонно-телеграфной компании) расположен на Аллее любовников, 13456 (вот как!). Линия моего интернет-провайдера проходит через весь город до места, где электроны моего запроса конвертируются в фотоны, чтобы попасть в оптоволоконную сеть AT&T. Затем пакет попадает в Морристаун (штат Нью-Джерси), где передается на вашингтонский маршрутизатор AT&T, затем возвращается в Нью-Джерси, на этот раз в Мидлтаун. Мидлтаунский маршрутизатор передает пакет первичному интернет-провайдеру в Level 3.

Попадая в магистраль Level 3, пакет проходит через три разных узла в Вашингтоне. К этому времени расстояние, пройденное пакетом по радиоволнам, медным проводам и высокоскоростным участкам оптокабелей, превысило 1300 километров, хотя оказался он на расстоянии всего 120 километров от места отправки. Последний маршрутизатор Level 3, находящийся в Вашингтоне, передаёт его на огромной скорости в Чикаго (наконец-то мы хоть куда-то продвинулись), где он проскакивает ещё два маршрутизатора Level 3, а затем отправляется в Миннеаполис. Вместо того чтобы сразу попасть к нашему хостинг-провайдеру, пакет проходит ещё 1120 километров до следующего маршрутизатора Level 3, находящегося в офисе компании в Колорадо, откуда пересылается обратно интернет-провайдеру нашей компании, в Миннеаполисе, и на наш веб-сервер.

Чтобы преодолеть расстояние в 1450 километров до Миннеаполиса, наш пакет прошёл около 3220 километров, но весь этот процесс длился не более нескольких секунд. Если бы кибервоинам захотелось отправить этот пакет в неправильном направлении или не дать ему попасть куда-либо, у них было бы минимум две возможности.

Во-первых, как уже говорилось, можно было атаковать «справочную службу» Интернета – систему доменных имён и отправить меня на другую страницу, возможно, поддельную и очень похожую на ту, которая мне нужна, где я мог оставить номер своего банковского счета и пароль. Помимо вмешательства в систему доменных имён с целью перехвата запроса кибервоины могут атаковать саму систему.

Так произошло в феврале 2007 года, когда шесть из тринадцати крупнейших доменных серверов высшего уровня подверглись DDoS-атаке. Как и в истории с Эстонией и Грузией, на серверы стали поступать тысячи запросов в секунду. Два атакованных сервера вышли из строя, в том числе и тот, который управляет трафиком Министерства обороны. Четыре сервера сумели справиться с атакой, перенаправив запросы на другие сервера, не тронутые хакерами. Атака продолжалась восемь часов, следы её вели в Тихоокеанский регион. Хакеры остановились, либо испугавшись, что их обнаружат, либо, что более вероятно, потому, что они только тестировали свои возможности.

В 2008 году Дэн Камински продемонстрировал, как искушённый противник может взломать систему. Он представил программу, которая открывает доступ к системе доменных имён и спокойно разрушает базу данных. После этого система начинает выдавать неверные номера. Даже неправильная адресация способна вызвать полный хаос в Интернете. Одна из компаний, занимающихся кибербезопасностью, нашла 25 разных способов взломать систему доменных имён, уничтожить или выкрасть данные.

Второе уязвимое место в Интернете – пограничный шлюзовый протокол. За несколько секунд и три тысячи километров пути моего пакета хакер имеет возможность перехватить его в момент перехода в сеть AT&T. Компания AT&T предоставляет самые безопасные и надёжные интернет-услуги в мире, но и она уязвима.

Когда пакеты попадают в магистраль, оказывается, что AT&T никак не связана с моей компанией. А кто связан? Пакеты проверяют базы данных всех крупных интернет-провайдеров. Там они находят информацию от Level 3: «Если вы хотите попасть на mycompany.com, идите сюда». Так система маршрутизации регулирует трафик в пунктах объединения интернет-провайдеров, там, где один заканчивает работу, а другой начинает, на границе. BGP – пограничный шлюзовый протокол – основная система, используемая для маршрутизации пакетов. На пакетах есть ярлыки с адресами «куда» и «откуда», а про-

токол BGP, как работник почты, решает, на какую сортировочную станцию отправить пакет. Протокол BGP, кроме того, устанавливает «равноправные» отношения между двумя разными маршрутизаторами двух разных сетей. Чтобы пакет перешел из AT&T в Level 3, нужно, чтобы маршрутизаторы этих провайдеров имели BGP-соединение. Как говорится в отчёте Internet Society, некоммерческой организации, занимающейся развитием интернет-стандартов, «в протоколах BGP нет внутренних механизмов защиты от атак, которые изменяют, удаляют или фальсифицируют данные, что может привести к нарушению всего процесса маршрутизации в сети». То есть когда Level 3 говорит: «Если вы хотите попасть на mycompany.com, идите сюда», никто не проверяет, правда ли это. BGP-система работает на доверии, а не по любимому принципу Рональда Рейгана «доверяй, но проверяй».

Если какой-нибудь злоумышленник, сотрудник крупного интернет-провайдера, пожелает воспользоваться Интернетом в своих целях, он легко сможет это сделать, взломав таблицы пограничного шлюзового протокола. Это можно сделать и снаружи – достаточно изменить команды пограничного шлюзового протокола, и интернет-трафик не достигнет своего пункта назначения.

Любой, кто занимается сетевым управлением в крупных интернет-провайдерах, знает об уязвимых местах системы доменных имён и протокола BGP. Люди, вроде Стива Кента из BBN Labs в Кембридже (штат Массачусетс), придумали несколько способов сокращения этих уязвимостей, но Федеральная комиссия по связи не требует от интернет-провайдеров применять эти разработки.

Правительственные органы США используют безопасную систему доменных имён, но в коммерческой инфраструктуре такой практики не существует. Решения по системе доменных имён принимаются в неправительственной международной организации ICANN (Ассоциация по присвоению имен и номеров (портов) Интернета), где никак не могут прийти к соглашению о системе безопасности. В результате мишенью кибервоинов может являться сам Интернет, но большинство специалистов по кибербезопасности считают, что это маловероятно, поскольку Интернет необходим для осуществления атаки.

После развала СССР Россия утратила паритет в этой области, а ФРГ по ряду причин не достигла сравнимого потенциала. Организующим и координирующим элементом действий на геоцентрическом ТВД является информационное оружие, наиболее эффективно потенциал которого реализуется киберкосмическими войсками.

Понятие о геоцентрическом ТВД является развитием идей ведущих военных теоретиков США – адмирала А. Мэхэна и особенно полковника Дж.

Бойда (OODA-Loop), много сделавшего для обеспечения военного доминирования США в современном мире.

В теоретической основе этих изысканий заложен принцип Гегеля[188], позволяющий на каждой стационарной стадии исследования объекта выделить явление и сущность, соответствующие данной стадии развития объекта.

Знание сущности является результатом теоретического моделирования. В рассматриваемой задаче – это вскрытые замыслы противника, проявляющиеся в целенаправленном изменении диспозиции, но не наблюдаемые напрямую.

В статье российского специалиста[189] и в ряде других его публикаций[190] представлен «новый класс динамических задач позиционного осознания конфликта, развивающегося во времени». А. А. Денисовым дано точное математическое определение понятия мема «как кванта бессознательной активности сознания безотносительно к его носителю» и предложено решение ключевой задачи метрологического обеспечения управления конфликтом на геоцентрическом ТВД – «генерации интерпретаций «нулевой точки», исходящей от субъекта-источника с нулевой матрицей ценности».

В работе Денисова, являющейся продолжением и развитием идей Джона Бойда, в частности отмечено, что «переход к доктрине геоцентрического ТВД порождён научно-технологической революцией в области моделирования сознания и новых технологий управления поведением. Эта революция вызвала резкий рост значимости информационных, психологических и иных небоевых операций, породив невиданный ранее тип вооружённой борьбы – конфликты на геоцентрическом ТВД». Авторы считают неуместным употребление термина «небоевые операции» по отношению к информационным, психологическим, климатическим и иным геофизическим операциям, скорее их следует именовать «нетрадиционными боевыми операциями», что логически следует из утверждения Денисова о порождении ими «невиданного ранее типа вооружённой борьбы».

Кроме того, Денисов утверждает, что для того, чтобы сформировать образ ситуации и образ действия, требуется определённое время. При этом

---

188 Материалистическая диалектика в 5 томах/Под редакцией проф. Ф. В. Константинова и В. Г. Марахова. Мысль. М., 1981-1985, том 1

189 Денисов А. А. – Основы метрологического обеспечения управления конфликтами на геоцентрическом ТВД. Информационные войны, 2011, № 3, с. с. 33-44

190 Денисов А. А. – Подавление циклов Бойда: Опыт управления военными и политическими конфликтами 1999-2009 гг. Информационные войны, 2010, № 2, с. с. 2-16; Денисов А. А. – Системы, превосходящие исследователя по совершенству. IV Международная конференция по проблемам управления. Сборник Трудов. Институт управления им. Трапезникова РАН, 2009, с. с. 1356-1363; Денисов А. А. – «Призрачные» субъекты в управлении военным и политическим конфликтом. Государственная служба, 2010, № 2 (64), с. с. 67-70; Денисов А. А., Денисова Е. В. – Подавление циклов Бойда: Новый принцип управления военными и политическими конфликтами. Информационные войны, 2010, № 3, с. с. 2-17; Денисов А. А., Денисова Е. В. – Подавление циклов Бойда: Полная схема управления военным и политическим конфликтом. Информационные войны, 2010, № 4, с. с. 26-37

Источник: ru.wikipedia.org

Альфред Мэхэн

Источник: vk.com

Джон Бойд

неважно, идёт ли речь о коллективном сознании армии или об индивидуальном сознании человека. Характеристическое время релаксации сознания τ – всегда есть время формирования субъективного образа.

Во второй половине 90-х годов XX века независимое тестирование показало, что при создании одинаковых условий осознания сложной нестандартной ситуации $\tau_{\text{Пентагона}}$ оказалось на 29% меньше, чем $\tau_{\text{РА}}$ – Российской армии: $\tau_{\text{Пентагона}} = (1–0{,}29)\ \tau_{\text{РА}}$.

Измерения характеристических времён релаксации коллективного сознания армий противника – важнейшая задача разведки в условиях конфликта на геоцентрическом ТВД и для обеспечения готовности к нему.

Чем быстрее и чем по большему числу нестандартных ситуаций армия может адекватно реагировать, тем выше её боеспособность. Это утверждение справедливо, естественно, только для случая боеготовности всей армии.

Важным следствием философского обоснования метрологических изысканий Денисова явилась сформулированная им концепция необходимости формирования любой страной, стремящейся сохранить свой суверенитет, собственной системы метрологического обеспечения за счёт генерации собственного «нуля» отсчёта. Собственное метрологическое обеспечение рассматривается им как панацея, позволяющая осуществлять подавление и преодоление циклов Бойда.

Каждая страна нуждается в собственном механизме генерации «нуля» времени, что обусловлено не только отличием географического положения, но и проблемой обеспечения независимости и самостоятельности в проведении военной, научно-технической и производственной политики.

Появление Доктрины геоцентрического ТВД ничего в этом не меняет. Любая страна или сетевая надгосударственная система влияния, претендующая на равноправное отношение со стороны других действующих сил (акторов) мировой политики, должна создать собственную генерацию «нуля»[191].

---

191 netocracy. us›Articles/2011_10_19.pdf

Всякая страна или система, которая начинает пользоваться уже созданной генерацией «нуля», автоматически и на самом глубоком уровне подпадает сначала под влияние, а затем и под контроль той системы, чьей генерацией она пользуется.

Это обеспечивает всё возрастающую зависимость в принятии собственных военных, экономических и политических решений, но одновременно ведёт к непрерывному повышению ценности таких решений. Возникает петля положительной обратной связи, из которой невозможно выбраться, так как «отключение» от чужой генерации «нуля» вызывает катастрофический провал эффективности и результативности собственного управления и, как следствие, гибель в конфликтах с естественными противниками.

Ещё один важный вывод из работ Денисова состоит в том, что конфликты на геоцентрическом ТВД являются динамическими, и успех в информационном и, как следствие, в любом ином противоборстве, может быть обеспечен учётом временного (темпорального) фактора.

Динамическая модель принятия решений в бинарном конфликте оставляет неразрешённым один важный момент: что такое «заимствованная позиция» $^{\wedge}|\Sigma\tau_n$? На определённых этапах она используется для преобразования статического образа диспозиции на ТВД в динамический образ замыслов противника:

$$T_y|\tau_1 \text{ Å } \Lambda|\tau_1 \rightarrow w(\tau_1);$$
$$T_y|(\tau_1 + \tau_2) \otimes \ ^{\wedge}|\Sigma(\tau_1 + \tau_2) \rightarrow w(\tau_1 + \tau_2).$$

Речь идёт о важнейшей по отношению к участникам конфликта позиции, представляющей собой субъективный образ реальности, используемый в качестве «политического руководства», которое позволяет по-новому осознать ситуацию на ТВД и возможные, точнее – вероятные, действия противника.

Поток $^{\wedge}|\Sigma\tau_n$ представляет собой динамический образ, разъясняющий «политический момент».

Практика общественной жизни однозначно свидетельствует, что войны начинают политики[192]. Однако авторы хотели бы добавить к этому тезису, что согласно историческому опыту ответственность за поражение несут военные, а все тяготы поражения ложатся на плечи народа проигравшей страны. Слава богу, в новой истории есть пример, когда нацистских политиков настигла заслуженная кара народов в результате катастрофического для немецкого народа поражения в войне, начатой этими политиками для захвата мирового господства и установления «нового порядка» во всём мире. Этот прецедент позволяет надеяться, что такая

---

192 А. А. Денисов

Источник: www.milresource.ru

Алексей Алексеевич Ивлев

Источник: www.reflexion.ru

Владимир Александрович Лефевр

судьба ждёт и других политических преступных авантюристов, затевающих войны с целью достижения мирового господства.

Поток $^{\wedge}|\Sigma\tau_{n}$ есть генерация интерпретаций «нулевой точки».

В форме потока $^{\wedge}|\Sigma\tau_{n}$ «политики» осуществляют вмешательство и общее управление войной. С позиции динамической модели принятия решений вмешательство «политиков» жизненно необходимо военным.

Именно механизм осознания конфликта, развивающегося во времени, требует создания единого источника потока $^{\wedge}|\Sigma\tau_{n}$, внешнего относительно к армии.

Переход к Доктрине геоцентрического ТВД порождён совершенно новой технологической реальностью, требующей перехода к новому способу генерации потока интерпретаций «нулевой точки».

Такой тип конфликта становится слишком сложным и быстро меняющимся. Использование прежних технологий генерации $^{\wedge}|\Sigma\tau_{n}$ перестаёт удовлетворять задачам практического управления. Они несли (в случае НСДАП и т. п.) и несут в настоящее время (в случае неоконсерваторов с их идеологией «исторической миссии»[193], или в случае единороссов с единственной идеологией неограниченного личного обогащения[194] слишком значительный отпечаток групповых интересов правящей организации (партии, ложи и т. п.). Требуется радикальное повышение объективности и незаинтересованности источника потока.

Из этого следует, что необходимо создать генерацию потока интерпретаций «нулевой точки» от субъекта-источника с нулевой матрицей ценности, то есть от источника-субъекта, не имеющего никаких интересов в конфликте и абсолютно объективного. Уточним – никаких интересов в конфликте, кроме достижения победы. И ещё раз уточним, что действительной причиной начала и ведения войны является её цель, а победа – лишь декларацией достижения цели. К сожалению, ни в работах американских теоретиков,

193 В. Спектор – О нарушениях норм международного права и общечеловеческой морали в современной внешней политике США. Труды МАН ПНБ. М., том 2, вып. 5, с. 3

194 В. Спектор – Меморандум об очередном витке предкризисной стагнации российской государственности, его исторических корнях и возможных управляющих мерах по обеспечению позитивной эволюции. Труды МАН ПНБ. М., том 2, вып. 1, с. 4

ни в публикациях А. А. Денисова не уделяется должного внимания оценке роли цели войны. Однако именно цель войны является определяющим, изначальным элементом всех последующих изысканий и выводов. Цель войны всегда должна быть рациональной, то есть не выводить решение дальнейших задач управления войной ни на нуль (поражение), ни на бесконечность – случай формулирования цели как достижения мирового господства.

В работе Лефевра[195] были опубликованы элементы модели так называемого «призрачного субъекта» и приведены результаты экспериментального подтверждения. «Призрачный субъект» рассматривался Лефевром как скрытый субъект стратегического управления с бесконечным циклом Бойда [196]или как система, превосходящая исследователя по совершенству[197]. Это означает, что его («призрачный субъект») нельзя победить с точки зрения современной военной науки.

Выстраивание взаимодействия с «призрачным субъектом» при весьма узких граничных условиях позволяет создать технологию генерации интерпретаций «нулевой точки», удовлетворяющую требованиям управления конфликтом на геоцентрическом ТВД.

А. А. Денисов полагает, что предложенная в его работах математическая модель осознания конфликта, развивающегося во времени, представляет собой основу теоретической меметики, системы технологий конструирования сознаний с новыми свойствами (психоинжиниринга) и основу метрологического обеспечения управления конфликтом на геоцентрическом ТВД.

Работы Дж. Бойда, В. Лефевра, А. Денисова и А. Ивлева, безусловно, являются необходимыми источниками при анализе и планировании мероприятий по созданию теории и перспективных средств, обеспечивающих, как минимум, паритет в разворачивающихся информационных войнах на многомерном геоцентрическом театре военных действий.

Формирования ВС США, назначенные на ведение информационной войны.

Приведём лишь несколько примеров конкретных военно-организационных мероприятий по модернизации современных структур вооружённых сил США и по их адаптации к проведению политики агрессивного информационного противоборства.

---

195 Лефевр В. – Психографика. Знаки страстей в математических структурах. В кн.: Лефевр В. – Рефлексия. «Когито-центр». М., 2003, с. с. 311-371

196 Ивлев А. А. – Основы теории Бойда. Направления развития, применения и реализации. М., 2008

197 Денисов А.; Лефевр В. –Системы, сравнимые с исследователем по совершенству. В кн.: Лефевр В. – Рефлексия. «Когито-центр». М., 2003, с. с. 408-414

С точки зрения военно-политического руководства США обеспечение национальной безопасности государства становится всё более сложным и комплексным мероприятием. В эпоху XXI века на первое место выходят новые информационные технологии, производящие «революцию» в военном деле. Их внедрение направлено на повышение боевых возможностей формирований за счёт обеспечения всех участников боевых действий своевременными и точными данными для осведомленности об обстановке на поле ведения боевых действий, а также сокращения времени на принятие решений.

Применение информационных технологий в рамках боевых систем будущего, предусматривает в первую очередь возможность боевых формирований получать доступ к инфраструктуре информационных баз МО: базам разведывательной информации, аналитическим центрам, находясь в любой точке земного шара и в любое время. Активное внедрение современных информационных технологий в ВС США требует уделять особое внимание безопасности военных информационных систем. Так же большую роль приобретают операции по нарушению аналогичных систем противника, проведение кибер-атак на серверы противника.

Глобальная информационная сеть Министерства обороны США включает около 7 миллионов компьютеров и более 15 тысяч различных компьютерных сетей. Часть из них содержит совершенно секретную информацию.

В конце 2006 года, министр ВВС Майкл Уинн объявил о создании Киберкомандования ВВС США (AFCYBER), формирование которого было назначено на лето 2007 года, а окончательное введение в боевой состав на 1 октября 2008 года. Командующим был назначен генерал-лейтенант Роберт Элдер, мл. (Robert Elder Jr). Однако, летом 2008 года эти планы были отложены из-за смены высшего руководства ВВС США, в частности были назначены новый министр ВВС Майкл Донли и начальник штаба Нортон Шварц. Создание Кибер-командования было отложено до тех пор, пока новое руководство ВВС не вникнет в особенности проекта чтобы принять окончательное решение относительно сферы охвата и миссии командования.

Создание 24 Воздушной армии Космического командования ВВС США представляет собой качественный скачок в информационной защите, а так же создание наступательного потенциала для проведения организованной масштабной информационной войны и усиление глобальной разведывательной деятельности США в информационных сетях.

ГЛАВА 3
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ИЕРАРХИИ СИСТЕМ УПРАВЛЕНИЯ – НЕОБХОДИМОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ЕЁ ПРОХОЖДЕНИИ ПО ИЕРАРХИЧЕСКИМ СТРУКТУРАМ.

Суть системы мероприятий по определению облика и формированию «вертикали власти», осуществлённых в Российской Федерации в последнее десятилетие, состоит в осознании повышенной уязвимости всей системы управления страны в условиях информационного противоборства и, тем более, при проецировании существовавшей до начала 2000 годов расхлябанной, децентрализованной системы на вероятную ситуацию информационной войны.

Эта система представляла собой причудливое чередование локальных кластеров федерализма (в первую очередь регионы так называемого «красного пояса»), конфедеративных отношений федерального центра с регионами Поволжья, более или менее выраженного сепаратизма: от абстрактного «областничества» в Сибири и дальневосточных регионах до вооружённого противостояния с центром на Северном Кавказе. Кроме того, существовали территориальные кластеры, чаще всего контролировавшиеся местной организованной преступностью, не отличавшиеся склонностью к сепаратизму, но в которой и местные, и федеральные органы власти, не вовлечённые в организованную преступность, не оказывали практически никакого управляющего влияния, а закон подменялся «понятиями» (Сочи, станица Кущёвская, как пример ситуации на большей части Краснодарского края, Гусь Хрустальный и многие другие).

Такая ситуация не могла не привести к состоянию повышенной тотальной уязвимости большинства подсистем структуры управления – в первую очередь, органов юстиции и правоохранительных, включая природоохранные, органов; налогового администрирования; финансового оборота и банковского контроля; антимонопольного контроля и контроля взаимоотношений хозяйствующих субъектов. Однако и не только их, структурная анархия охватила все уровни управления во всех сферах жизни российского общества, оставляя граждан страны практически беззащитными перед лицом системного произвола.

Именно в такой ситуации укрепились позиции организованной преступности с развитой системой связей со структурами международной организованной преступности, за витриной приватизации (народом переименованной в «прихватизацию») произошла системная экспроприация общенародной собственности, приведшая к формированию олигархической формы управления экономикой страны и к перерождению всей системы государственной службы от службы гражданскому обществу (civil service) к системе обслуживания и защиты интересов олигархического капитала. Возникшие «ножницы» в доходах и социальном статусе, вызвав перманентную социальную напряжённость, стали дополнительным фактором уязвимости государства и общества в ситуации нарастающего информационного противоборства на грани, а иногда и за ней, информационной войны[198].

Свой вклад в развитие деструктивных процессов внесла и добровольно «подведомственная» олигархам «свободная» и свободно коммерционализировавшаяся российская пресса, легко подменившая понятие «свободы слова» на целую серию понятий по «понятиям» – слив информации, диффамация и свобода вторжения в частную жизнь граждан, свобода доступа к запрещённой и /или общественной информации, заданность, продажность и свобода от ответственности за намеренную или случайную дезинформацию/заведомо ложную информацию. Дело в том, что свобода слова в хрестоматийном смысле неразрывно связана с ответственностью за публично распространяемое слово, но именно это и вызывает наиболее бурные и гневные протесты российской «свободной» журналистики[199] и всей разнородной и разношёрстной демократической (часто именуемой «дерьмократической») оппозиции.

---

198 Спектор В.Н. – Международная обстановка, внутренняя политика России и национальная безопасность (Редакционная преамбула). Труды МАН ПНБ. М., том 2, вып. 1, с. 3

199 Спектор В.Н. – Свобода слова и ответственность журналистов. Труды МАН ПНБ. Территория надежды. М., том 1, 1997

ГЛАВА 4

ИНФОРМАЦИОННАЯ БОРЬБА И ЕЁ МЕСТО В ДИНАМИКЕ УСТАНОВЛЕНИЯ ГЕОПОЛИТИЧЕСКОГО РАВНОВЕСИЯ.

Современная политика Российской Федерации, в том числе, военная, формируется в сложных условиях геополитической конкуренции и информационного противоборства[200]. Это, в первую очередь, связано со стремлением к неограниченному доминированию со стороны США[201], создающему идеологические и консциентальные угрозы выживанию Человечества, поддерживаемому военно-политическим блоком НАТО и осложнённому проявлениями международного терроризма и организованной преступности[202]. Кумулятивно эти факторы действуют в направлении ослабления позиций России в политической, экономической, военной и других областях. Подтверждением этому являются непрекращающиеся попытки отдельных государств сформировать негативный образ России в широких кругах мировой общественности.

На основе антироссийских настроений прилагаются усилия по изменению расстановки сил в наиболее важных регионах мира. Периодически реанимируется информационная поддержка подрывных действий сил сепаратизма на Северном Кавказе под предлогом борьбы за соблюдение прав человека и систематически ведётся информационная война, направленная против интересов России в Закавказье[203].

Большой бедой обернулась дезориентированность российских средств массовой информации, в первую очередь телевидения, большинство каналов вещания которого контролировалось олигархическими группами (Гусинский, Березовский и другие) во время кавказских войн. Кроме того,

200 Щекотихин В. М.; Королёв А. В.; Королёва В. В., Крикунов А. В., Сёмкин С. Н. – Основы противодействия информационной войне. Академия ФСО России. Орёл, 2009, 305 с.

201 В. Н. Спектор – Формирование нового мирового устройства. Прогнозируемая роль отдельных государств и цивилизационных сообществ. Труды МАН ПНБ. М., 1999, том. 2, вып. 4

202 Спектор В. Н. – Политический, религиозный и этнический экстремизм, организованная преступность и терроризм как элементы единой системы дестабилизации планетарного социума (Триединство планетарного зла). Труды МАН ПНБ. М., 2010, том 3, вып. 3, с. 3

203 Спектор В. Н. – Силовая продажа демократии по-американски и ситуация в Закавказье. Труды МАН ПНБ. М., том 2, вып. 5, с. 14; Захаров В. А – Политика НАТО в государствах Закавказья и проблемы безопасности России. Там же, с. с. 29-68; Захаров В. А. – Оценка влияния активности НАТО в Армении и геополитические последствия для России (доклад и дискуссия на заседании Круглого стола «Расширение НАТО в государствах Закавказья и ситуация в Армении» Общественной Академия наук, культуры, образования и бизнеса Кавказа и Московского общества дружбы с Арменией). Там же, с. с. 69-111

Источник: ru.wikipedia.org

Татьяна Миткова

руководство российского телевидения находилось под постоянным моральным и финансовым давлением деморосов, проводивших если не полностью антироссийскую, то абсолютно антирусскую политику, так как они планировали включение России в полуколониальный ареал Запада, предпочтительно без русских.

Сложилась абсурдная ситуация использования национальных СМИ, с одной стороны, в «грязных» политических технологиях, в дискредитации национальных силовых структур, в первую очередь армии, государственных институтов, политических и государственных деятелей и в проведении антигосударственной и антирусской пропаганды. В СМИ возникла ситуации сумасшедшего дома – свободы без ответственности. С другой стороны, практиковалось использование Минпечати РФ и силовых структур в публично и юридически необоснованных акциях против СМИ. Это нашло отражение в довольно тенденциозной статье Булата Касмантиева «К вопросу об особенностях современной российской прессы», опубликованной в теоретическом журнале «Кредо/Credo New» (1997).

Иностранными спецслужбами оказывается комплексное воздействие на систему государственного и военного управления страной, её политическое и военное руководство[204]. Расширяется антиправительственная и антигосударственная деятельность ряда неправительственных организаций, активно поддерживаемых из-за рубежа[205].

Западные СМИ, поддерживавшие дестабилизирующую деятельность западных, в первую очередь американских фондов и международных сетевых структур, пестрели провокационными заголовками типа «Назначение кремлёвского идеолога в состав российско-американской комиссии вызвало возмущение» (Франс-Пресс), «Перед Обамой российские оппозиционеры обличали цензуру» (Ле Фигаро, Франция). «Быть журналистом в России смерти подобно» (Гардиан, Великобритания) и не менее провокационными рекомендациями: «По горькой иронии судьбы, российские журналисты сегодня менее свободны, чем в те времена … Если г-н Медведев хочет, что-

204 Спектор В. Н., Ильин И. А. – Макроисторический пасьянс интересов: Что было? Что будет? Чем сердце успокоится? Труды МАН ПНБ. М., 1999, том 1, вып. 3, с. 16

205 Манчич В. – Письмо Председателю Совета Федерации Федерального Собрания России С. М. Миронову «Об отношении России к ситуации на Балканах и в Центральной Европе». Труды МАН ПНБ. М., том 2, вып. 5, с. 316; Комментарий официального представителя МИД России о прекращении деятельности в Российской Федерации Агентства США по международному развитию (USAID). МИД РФ. Официальный сайт. 19.09.12; Нарочницкая Н. А. – Американские «аналитические институты» – глаза, уши и совесть Америки. В кн.: Оранжевые сети: от Белграда до Бишкека/Под ред. д. и. н. Н. А. Нарочницкой. Алетейя. Санкт-Петербург, 2008

бы его принимали всерьёз, он должен сломать спираль страха, в которой зажаты российские журналисты с момента прихода к власти г-на Путина … И он должен не только защищать нынешних Хлебниковых (Форбс) и Политковских, но и поощрять их работу» (редакционная статья в Ле Монд, Франция, 13.07.09). А г-н Медведев очень хочет, чтобы его воспринимали серьёзно.


Источник: ru.wikipedia.org

Анн-Мари Слотер

Сегодня информация стала стратегическим ресурсом, который в значительной мере определяет и оказывает влияние на состояние политической, военной, экономической, социальной и других составляющих безопасности современного общества в суверенном государстве. Активизируется негативное воздействие информационного пространства и коммуникационных технологий на политическую, военную, экономическую компоненты безопасности общества и государства.

Примером попыток воздействия на политику Российского государства являются перманентные нападки на обеспечение сохранности ядерных технологий в свете Договора о нераспространении ядерных вооружений, где на самом деле стратегические нарушения были связаны с США и Великобританией (Израиль-ЮАР, Пакистан, в меньшей мере Индия и другие). Тем не менее, западная пресса организует информационные атаки, основанные на дезинформации, ложной информации и подходах двойных стандартов. Примером такой атаки служит, например, статья в респектабельной газете «Вашингтон пост».

Статья Анн-Мари Слотер, декана Школы общественных и международных отношений Вудро Вильсона в Принстонском университете и содиректора Принстонского проекта по национальной безопасности и Томаса Райта, старшего научного сотрудника этого же проекта «Наказание, соответствующее ядерному преступлению», подготовленная к опубликованию в The Washington Post/«Вашингтон пост» журналисткой Синтией Зайсс[206], в качестве запева содержит ложную информацию о перехваченной ЦРУ и грузинскими «официальными лицами» попытке якобы русского продать на чёрном рынке уран оружейного качества. Далее они утверждают, что этот инцидент, информация о котором появилась почти через полгода после задержания в Грузии гражданина Грузии из Южной Осетии, явился последним в череде вызывающих беспокойство инцидентов (без указания каких именно), напоминающих о чрезвычайности угрозы, связанной с ядерным терроризмом.

206 Slaughter Anne-Marie, Wright Thomas – Punishment to Fit the Nuclear Crime. Presented by Cynthia Zeiss. The Washington Post. 2007

В своей статье эти «остепенённые» провокаторы ставят на одну доску «утечки» ядерных технологий из группы пакистанского «отца ядерной бомбы», проф. А.К. Хана, которого пакистанские власти хотя и содержат «под домашним арестом», но категорически отказываются выдать американцам, и ядерные программы СССР. При этом они утверждают, что из Союза не было утечек ядерных технологий и материалов из-за страха перед возмездием со стороны США. По-видимому, это очень молодые политологи – их не учили, что от страха не российский, а американский министр обороны выбросился из окна с криком «Русские идут».

В конечном итоге вся статья посвящена тому, что международное право должно служить интересам национальной безопасности США, которые своими действиями разрушают важнейшие механизмы международного права. Безусловный интерес представляет дословное цитирование отдельных пассажей этой статьи из арсенала информационной войны, приводимых ниже:

«...making nuclear transfer a crime against humanity would greatly expand opportunities for prosecution, denying national governments the ability to shelter these criminals./...признание передачи ядерных технологий (материалов) преступлением против человечества неимоверно расширит возможности преследования, лишая национальные правительства (в явном виде, как обычно, отсутствует указание на релевантность этого предложения для внутреннего законодательства США) возможности предоставления убежища этим преступникам.

The International Criminal Court has jurisdiction over crimes against humanity. The inclusion of nuclear transfer as such a crime could be confirmed at the next review conference, in 2009./Международный уголовный суд имеет юрисдикцию в отношении преступлений против человечества. Включение передачи ядерных технологий (материалов) в число таких преступлений может быть подтверждено (такое предложение ещё даже не рассматривалось в установленном порядке) на следующей обзорной конференции в 2009 году <..> The ICC could then indict and prosecute those suspected of such acts. Even if the United States cannot bring itself to join the ICC, it could work with allies to empower the ICC to act.../МУС тогда сможет предъявлять обвинения и выносить приговор лицам, подозреваемым в совершении таких действий. Даже если Соединённые Штаты не смогут убедить себя к присоединению к МУС, они смогут действовать через союзников для того, чтобы МУС имел возможность действовать ...

That means that any nation, including the United States, could prosecute nuclear traders anywhere in the world./Это значит, что любое государство, включая Соединённые Штаты, сможет осуждать ядерных торговцев где угодно во всём мире (из этого, правда, не следует, что это «где угодно» включает Соединённые Штаты.

Finally, the U.N. Security Council could pass a Chapter VII resolution urging a prosecutor to investigate these cases or even establish a special tribunal to prosecute those suspected of nuclear transfer./Наконец, Совет Безопасности ООН в рамках Главы VII может принять резолюцию, призывающую обвинителя расследовать эти дела, или даже создать специальный трибунал для осуждения лиц, подозреваемых в передаче дерных технологий (материалов).

This initiative would make international law work as a tool of American national security strategy rather than as a constraint on it. Failing states would no longer provide safe haven for rogue individuals. <..> It would be multilateralism and international law at its best: hard-edged tools to further American and global interests».//Эта инициатива вынудит международное право работать как инструмент стратегии американской национальной безопасности, скорее чем её ограничение. Государства-нарушители не смогут более предоставлять убежище злодеям. <..> Это будет лучшим примером многостороннего и международного права: острым инструментом продвижения американских и глобальных интересов (точнее было бы сказать: продвижения американских глобальных интересов).

Не желая оставлять безответной эту лживую и двуличную информационную атаку, соавтор настоящей работы направил в газету (ВП) свои комментарии, отредактированные до избыточной политкорректности американскими коллегами по Академии (МАН ПНБ) д-ром Гленом Швайцером (ННФ и НАН США) и д-ром Ренсом Ли (Исследовательский институт иностранной политики). В этом комментарии[207] содержится указание на ложную исходную информацию и на императив равных возможностей и равной ответственности США перед международным правом. В связи с его краткостью и самоочевидностью это комментарий приводится полностью на языке оригинала.

To: *Mrs. Cynthya Zeiss of Washington Post* letters@washpost.com

Re: *remarks to the article «Punishment to Fit the Nuclear Crime» by Drs. Slaughter and Wright*

Dealing with Nuclear Crimes.

The timely proposal of Drs. Slaughter and Wright to make an illegal transfer of weapon-usable nuclear material or related technology a crime against humanity is a much needed pro-active measure to counter proliferation of weapons of mass destruction. Certainly, the Russian Federation would be among the first countries to support such an initiative that should be enshrined in international law.

At the same time, I do not believe that sting operations to capture an Ossetian or other traffickers, useful as they may be, would be a serious effort to address

---

207 Spector V.N. – Dealing with Nuclear Crimes. letters@washpost.com

nuclear smuggling. The problem is simply too widespread to be solved through such limited actions. Second, criticisms of the Russian Federation, which should be a key partner in this effort, do not help but rather complicate the problem. Finally, the proposed International Tribunal for Nuclear Crimes will be successful only if it is universally accepted by all countries, including the United States.

Valery Spector, President International Academy of Sciences on Problems of National Security. Moscow.

Бурное развитие научно-технического прогресса, обеспечившее стремительное и масштабное внедрение современных инфокоммуникационных технологий во все сферы деятельности общества[208], наряду с очевидными преимуществами неизбежно создает благоприятную среду для формирования новых вызовов и угроз в современном мире[209].

В условиях перехода от советского деформированного постиндустриального к дезориентированному и криминализованному информационному обществу в Российской Федерации в целях снижения уровня коррумпированности и под предлогом повышения эффективности функционирования госаппарата разворачивается процесс широкомасштабного перехода от бумажных к электронным технологиям поддержки государственного управления всех ветвей и уровней власти, то есть к электронному правительству. Без выполнения системы мероприятий по обеспечению контроля санкционированного доступа, без создания процедуры проверяемой регистрации граждан и организаций в создаваемых информационных сетях и без внедрения комплексных процедур поддержания безопасности в результате такого перехода может резко возрасти уязвимость всей инфраструктуры электронного правительства.

В связи с этим особую остроту в процессе деятельности органов государственной власти и управления, их взаимодействия с подведомственными им учреждениями, организациями и предприятиями, а также непосредственно с гражданами с применением современных средств информатизации и связи приобретают вопросы обеспечения информационной безопасности[210].

В России крайне низкая квалификация управленцев (на самом деле в большинстве своём являющихся не управленцами, а бюрократами – bureau – место сидения, в настоящее время – место кормления (сажают их уже потом,

---

208 Nesterikhin Yu. E. – Plenary Report on DUT Interacademy (RF-US) Meeting. M., 1992

209 Инновационные решения для безопасности России. – Доклад первого заместителя начальника Генерального штаба ВС РФ генерал-лейтенанта А. Бурутина. Десятый Национальный форум информационной безопасности. («ИНФОРУМ – 10»). Москва, 31 января – 1 февраля 2008 г.; Батранков Д. В. – Новые угрозы безопасности. Материалы Десятого Национального форума информационной безопасности. «Инновационные решения для безопасности России» («ИНФОРУМ – 10»), Москва, 31 января – 1 февраля 2008 г.

210 Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 9 сентября 2000 г., № 1895-р.

когда они пережрут), cratos – власть)) всех уровней в области информационных технологий. Это приводит к неоправданно высокому уровню уязвимости всей системы управления – от муниципального до федерального уровня[211].


Источник: www.tdisie.isc.ru

Юрий Ефремович Нестерихин

В стране, безусловно, предпринимаются, как правило, бесплодные попытки совершенствования системы управления с целью снижения её уязвимости в условиях информационного противоборства, тем более в условиях информационной войны[212]. К сожалению, эти попытки идут по одному из двух порочных сценариев – перемешивание колоды или перенесение порток с одного гвоздка на другой гвоздок – и ведут лишь к увеличению численности некомпетентных алчных бездельников и бездельниц и к расширению ареала коррупции.

Важным событием последнего времени явилось формирование организационной структуры государственной системы обеспечения информационной безопасности. Она включает главу государства и возглавляемый им Совет Безопасности Российской Федерации, межведомственную комиссию Совета Безопасности по информационной безопасности, являющуюся его рабочим органом, а также органы законодательной, исполнительной и судебной властей[213].

Заметным, хотя и не всегда бесспорным, вкладом в понимание традиционного современного информационного противоборства, включая традиционные элементы информационной войны, стали работы продвинутого специалиста в этих вопросах С. Н. Гриняева, с отличием окончившего Военную инженерно-космическую краснознаменную академию им. А. Ф. Можайского в г. Санкт-Петербург,. в 1997 году успешно окончившего адъюнктуру при этой Академии, защитившего диссертацию на соискание учёной степени кандидата технических наук и поработавшего по специальности в должностях научного сотрудника и старшего научного сотрудника в НИИ Мино-

---

211 Рыжков В. И. – Информационные технологии в государственном и муниципальном управлении. Учебное пособие. Хабаровск: Дальневосточная академия государственной службы, 2004, включая оборону и правоохранительную систему [Военные известия//PC WEEK/RE, № 36, 30.09-6.10.2008; Новиков А. А., Устинов Г. Н. – Уязвимость и информационная безопасность телекоммуникационных технологий. Учебное пособие для вузов. Радио и связь. М., 2003, 294 с.

212 Онорский Б. – Информационная война – основная форма борьбы ближайшего будущего? Обозреватель/Observer, 1998, № 5

213 Черешкин Д. С., Смолян Г. Л. – Нелегкая судьба российской информатизации. Информационное общество, 2008, вып. 1-2, с. 47-71

Источник: www.custodiexpert.ru

Сергей Николаевич Гриняев

бороны. В 1999 году С. Н. Гриняев был утверждён в научном звании старшего научного сотрудника, уволился из армии и продолжил научную деятельность в качестве независимого эксперта.

Наиболее заметны и наименее противоречивы следующие работы этого автора, имеющего более 70 научных публикаций[214]. Эти работы и некоторые его статьи в сборнике «Актуальные проблемы информационного противоборства» (МАКБП. М., 2000, 334 с.), безусловно, могут быть рекомендованы для прочтения как сохранившие элементы актуальности. В тоже время такая его работа как «Информационное превосходство вместо «ядерной дубинки»» журнале «Армейский сборник, №5, 2002», памятуя выражение генерала армии, проф. М. А. Гареева «Не торопитесь выносить ядерное оружие за скобки – оно ещё кого угодно за скобки вынесет» и учитывая тот факт, что ядерное оружие является одним из энергетических элементов перспективного оружия геоцентрического ТВД, включая информационное, может ввести читателя в заблуждение, а ряд других работ этого автора уводят и специалистов, и политиков от понимания технических аспектов информационной войны будущего. Это особо относится к представлению «о войне в четвёртой сфере».

В тоже время, две более поздних публикации С. Н. Гриняева в Интернете, в рамках традиционного и современного информационно противостояния, представляют несомненный интерес.

4.1. В СОЦИАЛЬНО-ПОЛИТИЧЕСКОЙ СФЕРЕ – СЕТЕВЫЕ ТЕХНОЛОГИИ.

По мнению российских военных экспертов, специальные службы США и их союзников, назовём их Западом, в настоящее время в рамках традиционных технологий информационной борьбы заметно активизировали применение так называемых методов «сетевого противоборства». Увеличилось число информационно-психологических и иных мероприятий с использованием «сетевых структур». Основной целью данных мероприятий является оказание влияния на формирование политических, экономических и идеологических взглядов различных слоев населения в выгодном Западу направле-

214 Гриняев С., Кудрявцев В., Родионов Б. – Информационная безопасность избирательных кампаний. МАКБП. М., 1999, 104 с.; Гриняев С. Н. – США развертывают систему информационной безопасности. Независимое военное обозрение; Война в четвертой сфере. Независимое военное обозрение; Системы обнаружения вторжений на основе мобильных программ-агентов [Connect! Мир связи, № 7, 2001

нии, а также на поведение отдельных социальных групп в создаваемых этими службами кризисных ситуациях[215].

Источник: petit-objet-a.livejournal.com

Жиль Делез

Дэвид Бетц, преподаватель кафедры военных исследований в Кингс Колледже (Лондон) пишет[216]: «Запад для остального мира практически недосягаем. Только Запад располагает высокотехнологичными стратегиями, при которых быстрота маневра становится важнее численного перевеса, разведывательные сенсорные приборы способны своевременно и безошибочно обнаруживать ключевые объекты в лагере противника, а оружие обладает достаточно высокой точностью, чтобы атаковать эти объекты с дальнего расстояния».

Источник: uzrf.ru

Феликс Гваттари

Концепция «сети» как парадигмы социальной организации в условиях информационного общества начала разрабатываться гораздо раньше теории «сетевых войн» в таких направлениях западной философской мысли, как постструктурализм, синергетика, теория нелинейных динамик и других. Метафоры «корня» (линейный принцип) и «клубня» (нелинейный принцип) были введены в оборот в работе известных французских мыслителей – философа Жиля Делеза и психиатра Феликса Гваттари «Капитализм и шизофрения» в 1980 году[217].

Для провоцирования антиправительственных акций, массовых выступлений и демонстраций иностранные спецслужбы формируют сетевые структуры на базе правозащитных движений, партий либерально-демократической направленности, профсоюзных и экологических объединений, независимых средств массовой информации, религиозных, этнических и сепаратистских группировок. Для их негласного финансирования часто привлекаются зарубежные фонды и легально действующие в стране неправительственные организации.

Создатели сетевых структур тщательно скрывают наличие единого управляющего центра, представляя происходящие события как стихийные

---

215 Официальный сайт директора Национальной разведки США, http://www.dni.gov

216 Бетц Дэвид Дж. -. Революция в военном деле и «армейские операции вне условий войны»: Обоюдоострое оружие [http://www.strana-oz.ru/? numid=26&article=1133

217 Deleuze Gilles et Guattari Felix – Rhizome Capitalisme et schizophrénie. Mille plateaux. Les Editions de Minuit. Paris, 1980

действия местных граждан (Киргизия), как стремление реализовать прогрессивные идеи (Грузия), восстановить социальную справедливость (Тунис и Ливия) или защитить свои права (Египет, Сирия). В связи с этим инициируемые из-за рубежа акции сетевых структур, в том числе информационные кампании, демонстрации, митинги, пикеты, выглядят как спонтанные проявления политической и иной активности населения.

Одной из основных целей сетевых структур является изменение политического баланса в странах-мишенях в ходе «бархатных» революций, осуществляемых под лозунгом «демократизации». Это достигается, прежде всего, посредством проведения многочисленных ненасильственных акций, которые парализуют деятельность основных государственных механизмов, включая работу спецслужб и других силовых структур.

Указанные мероприятия могут проходить на фоне реально существующих экономических и социальных проблем (Молдавия, Украина), так и в условиях искусственно вызываемого роста недовольства населения постепенным систематическим информационно-психологическим воздействием на отдельных лиц и массовое сознание граждан. Для этого могут использоваться формальные предлоги, среди которых наиболее распространенными являются нарушение прав человека и иных демократических норм, а также ограничение свободы слова.

В монографии[218] проведен анализ информационных операций и сетецентрических действий зарубежных неправительственных организаций при проведении «цветных» революций, действий специальных структур Министерства обороны США, а также стран блока НАТО по использованию глобальной сети Интернет для манипулирования общественным сознанием в ходе локальных конфликтов.

4.2 СОЦИАЛЬНЫЕ СЕТИ – ИСТОЧНИК ИНФОРМАЦИИ И ИНСТРУМЕНТ ПОЛИТИЧЕСКОГО ВЛИЯНИЯ

Нельзя отрицать, что использование социальных сетей в открытой политической борьбе стало отличительной чертой волнений в Иране, Тунисе и Египте. В данном случае мы имеем дело с революционным расширением функций присущего социальным медиа феномена, ставшего в последние десять лет известным как «пользовательское наполнение» (от англ. UGC – user-generated content). Такое наполнение, как правило, производится непрофессионалами и включает в себя блоги, видеоклипы, подкасты, комментарии

218 Беликова Ю. В., Крикунов А. В., Королёв А. В. – Сетевые технологии в информационных операциях НАТО и зарубежных неправительственных организаций в ходе цветных революций и военных конфликтов. ЦАТУ. М., Академия ФСО России, 2012, 89 с.

на Интернет-форумах или статусы в социальных сетях, таких как Facebook или Twitter. Порталы, основанные на принципах пользовательского наполнения, принято называть «новыми медиа», «социальными медиа» и т. д.

Единственное необходимое уточнение касается внутренней классификации социальных сервисов и ее оснований. Принято выделять две категории таких сервисов:

а) собственно социальные сети – как универсальные, так и специализированные, профессиональные (Facebook, Одноклассники, Вконтакте, LinkedIn, MySpace, Friendster, Google+);

б) квазисоциальные сообщества (блоговые сообщества, микроблоговые сервисы (Twitter), сообщества на интерактивных платформах типа Ushahidi и т. д. – данный перечень является открытым)[219].

Провести четкое разграничение между обозначенными категориями достаточно сложно. Те же блоги могут быть лишь отдельным сервисом в рамках социальных комьюнити, обычные сайты могут иметь развитые социальные закладки, геосоциальные сети могут работать просто как сервис определения местонахождения, а могут приобретать полноценные социальные функции[220]. Для удобства все эти виды Интернет-сервисов, основанных на пользовательском наполнении, в данной работе будут объединены понятиями «социальные медиа», «новые медиа», «социальные сети» и т. д.

Медиа-площадки стали фактически единственным источником информации об этих событиях как для наблюдателей со всего мира, так и для находившихся в этих странах людей. Кроме того, они выступили инструментом организации для повстанцев, будучи для них зачастую единственным средством быстрой коллективной связи. Как мы увидим далее, этим пути их использования не ограничиваются.

При более детальном рассмотрении выбранной нами темы мы пришли к выводу, что для должного ее понимания и раскрытия необходимо ответить на следующие вопросы: Вследствие каких причин социальные сети стали инструментом политического влияния именно в указанных трех странах, и почему другие государства, вовлеченные в волнения Арабской весны, не стали частью дискурса «Твиттер-революций»? Насколько широким было использование социальных медиа повстанцами и является ли в связи с этим правомерным использование терминов «Твиттер-революция» и «Фейсбук-революция»?

Хотя целью данного исследования не является выяснить, имели ли произошедшие в этих странах беспорядки политический или общественный харак-

---

219 Олег Демидов. Социальные сетевые сервисы в контексте международной и национальной безопасности [Электронный ресурс] // ПИР-Центр. – 2011. – Режим доступа: http://www.pircenter.org/kosdata/page_doc/p2714_1.pdf

220 Олег Демидов. Социальные сетевые сервисы в контексте международной и национальной безопасности [Электронный ресурс] // ПИР-Центр. – 2011. – Режим доступа: http://www.pircenter.org/kosdata/page_doc/p2714_1.pdf

тер, были ли они поддержаны силами из военного руководства или другими политическими образованиями, для наиболее полного и всестороннего рассмотрения избранного вопроса необходимо определить причины и предпосылки произошедших в Иране, Тунисе и Египте событий, повлиявшие на характер беспорядков и сделавших возможным возникновения феномена «Твиттер-революций» в регионе. Само слово «революция» в данном сочетании скорее для удобства из-за его широкого использования в популярной прессе и литературе, в том числе и по отношению к акциям протеста в Иране в 2009 г.

Надо также отметить, что события Арабской весны в Египте и Тунисе, а также акции протеста в Иране не стали первым случаем подобного сетевого взаимодействия. Твиттер широко использовался во время волнений в Молдавии в 2009 г., и тогда наблюдатели также использовали термин «Твиттер-революция»[221]. Известный случай свержения президента Филиппин Джозефа Эстрады, вошедший в истории как «СМС-революция», характеризовался широким использованием обмена текстовыми сообщениями для сбора и организации протестующих. Тогда представитель университета ООН описал это как «возможно, первую электронную революцию – смену режима, проведенную с новыми формами информационных и коммуникационных технологий»[222].

Достоверно известно, что в средства новых медиа использовались не только в Иране, Тунисе и Египте, но также в Ливии и Сирии[223], однако в этих двух странах демонстрации быстро переросли в полномасштабные гражданские войны, и использование социальных сетей происходило лишь на втором плане борьбы. Таким образом, лишь в трех странах объем созданной и распространенной прямо на месте событий информации и масштаб последствий, позволяют назвать произошедшее беспрецедентным. Новые информационные и коммуникационные технологии, такие как мобильные телефоны с камерой и подключением к Интернету, могли сыграть важную роль для развития протестного и освободительного движения в Иране, Тунисе и Египте.

Нельзя забывать, что распространение термина «Твиттер революция» частично связано с тем, что мы имеем возможность видеть события лишь глазами образованных городских жителей, активно пользующихся социаль-

---

221 Термин был впервые применен Евгением Морозовым по отношению к протестам в Молдавии (см. Евгений Морозов: «Moldova's Twitter Revolution» (Net Effect, 7 апреля 2009) neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution). С тех пор Морозов не раз критиковал западные СМИ за преждевременность использования термина по отношению к событиям в Иране и на Ближнем Востоке и признал, что поторопился охарактеризовать так события в Молдавии. Он пишет об этом в своей книге, The Net Delusion: The Dark Side of Internet Freedom (New York: Public Affairs, 2011).

222 Julius Court. People Power II in the Philippines: The First E-Revolution? [Electronic resource]/Background Paper. – Overseas Development Institute, January 2001. – Mode of access: www.odi.org.uk/resources/details.asp?id=3147&title=people-power-iiphilippines-first-e-revolution.

223 Пользователи Facebook готовят новую революцию – в Сирии [Электронный ресурс] // БалтИнфо, 27 февраля 2011. – Режим доступа: http://www.baltinfo.ru/2011/02/27/Polzovateli-Facebook-gotovyat-novuyu-revolyutciyu-190430

ными сетями и выкладывающими информацию в Интернет. В действительности использование терминов «Твиттер-революция» и «Фейсбук-революция» скрыто заключает в себе момент переоценки распространенности этих сервисов. В 2009 г. в Тунисе, Египте и Иране лишь 34,1%, 24,3% и 11% населения соответственно имели доступ к Интернету[224], и только 16% и 7% населения в Тунисе и Египте были зарегистрированы в сети Facebook. В регионе самую большую популярность Facebook имеет в ОАЭ (36%), Бахрейне (29%), Катаре (24%) и Ливии (23%)[225], однако во время «Арабской весны» не обнаружилось прямой корреляции между этими цифрами и уровнем волнений: из перечисленных стран только в Бахрейне происходили протестные митинги. За пределами столиц и крупнейших городов рассматриваемых нами стран координационными центрами протестующих становились уже не группы в социальных сетях, а рынки и мечети. Впрочем, эти факты нисколько не умаляет роли новых медиа на начальном этапе: без их широкого использования население крупных городов вряд ли смогло бы поднять «протестную волну» в своих странах.

Безусловно, Интернет-технологии сами по себе не могли послужить причиной протестов и беспорядков ни в одной стране, и в Тунисе, Египте и Иране скорее сказался целый комплекс различных факторов, таких как годы подавления гражданских свобод, политическое и экономическое отчуждение, разложение социальных институтов, рост цен на еду и т. д. Нельзя недооценивать и зарубежное вмешательство во внутренние дела этих государств. Все это, подкрепленное желанием народных масс заявить о своих правах и добиться достойного представительства в органах власти, и вылилось в уличные протесты. Так или иначе, но мы все же выделяем события в Иране, Тунисе и Египте в отдельную категорию «твиттер-революций», которая привлекла внимание мировой общественности уникальной ролью использованных оппозицией Интернет-сервисов. Взаимосвязь всех факторов, обусловивших возникновение подобного феномена, будет более подробно рассмотрена во второй главе данной работе.

Как бы там ни было, многие авторы размещаемого контента действительно позволяли нам узнать о требованиях протестующих масс и, по всей видимости, нельзя отрицать связи между призывами к демонстрантам в социальных медиа и их действиями на улицах. Социальные медиа дали толчок протестам: люди, узнавали о ходе событий из социальных сетей и блогов и выходили на улицу, чтобы присоединяться к акциям митингующих, и, даже если сами по себе термины «Твиттер-революция» или «Фейсбук-рево-

---

224 Freedom on the Net 2011 [Electronic resource]/Freedom House, 2011. – Mode of access: http://www.freedomhouse.org/report/freedom-net/freedom-net-2011

225 Источники: International Telecommunication Union 2009 (http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx) и Social Map (http://geographics.cz/socialMap/)

люция» нельзя считать вполне точными, заявления о том, что «революция будет в твиттере»[226] (а также в блогах и видео-трансляциях) далеко небезосновательны. В Египте, Тунисе и Иране массы людей выходили протестовать на улицы, держа в руках не бутылки с зажигательной смесью или куски арматуры, а сотовые телефоны, с помощью которых они призывали еще больше людей и распространяли сводки с мест происшествий. Пользовательское наполнение, создаваемое и распространяемое прямо во время волнений, сыграло важную, но необязательно решающую роль в событиях «Арабской весны». Таким образом, возникает вопрос: «Стало ли широкое использование социальных медиа одной из причин, повлекших смену политических режимов? Для ответа на него необходимо определить причины, предопределившие пути использования социальных медиа оппозиционерами

4.2.1. Интернет-технологии в событиях в Тунисе, Египте и Иране

Почти все исследователи сходятся во мнении, что социальные медиа стали новым оружием в арсенале оппозиционных активистов. Впрочем, Малькольм Глэдвелл в своей статье «Революция не будет в твиттере»[227] подчеркивает, что развитие социального активизма значительно опередило появление социальных медиа. В своем интервью с Фаридом Закарией для CNN он ставит под сомнение важность новых медиа в революционном движении и утверждает, что оппозиционеры могли организовать свою деятельность и другими путями, приводя в пример ГДР, где правительство было свергнуто в то время как только 13% населения имело стационарные телефоны[228]. Кроме того, он напоминает, что Арабская весна затронула и такие страны, как Йемен, где Интернет-покрытие достаточно невелико.

Профессор Нью-йоркского университета Клэй Ширки, вступил с Глэдвеллом в полемику, приведенную в издании Foreign Affairs[229] под заголовком «От инновации к революции», где утверждает, что развитие таких инструментов как социальные сети изменило динамику общественного развития и не могло не сказаться на гражданской активности». В заочный спор с Глэдвеллом вступила также Зейнеп Туфеки со статьей «Почему методы органи-

---

226 Andrew Sullivan. The Revolution Will Be Twittered [Electronic resource]/The Atlantic, The Daily Dish, 13 June 2009. – Mode of access: http://andrewsullivan.theatlantic.com/the_daily_dish/2009/06/the-revolution-will-be-twittered-1.html

227 Thomas Sander. Why the revolution won't be tweeted [Electronic resource]/Social Capital Blog, September 29, 2010. – Mode of access: http://socialcapital.wordpress.com/2010/09/29/why-the-revolution-wont-be-tweeted/

228 Malcolm Gladwell. Social media platforms and revolutions [Electronic video resource]/CNN, March 27, 2011. – Mode of access: http://vijana.fm/2011/04/04/social-media-and-revolutions/

229 Malcolm Gladwell, Clay Shirky. From Innovation to Revolution [Electronic resource]/Foreign Affairs. – Council on Foreign Relations, March/April 2011. – Mode of access: http://www.foreignaffairs.com/articles/67325/malcolm-gladwell-and-clay-shirky/from-innovation-to-revolution

зации социальной активности имеют значение, а послание Глэдвелла уходит мимо цели» и Дэвид Вайнберг с записью в личном блоге[230], озаглавленной «Глэдвелл доказывает слишком многое».

Журналист Энтони Шадид пишет в своем твиттере[231] о Сирии: «Это не революция твиттера или фейсбука. Революция делается на улицах, и она пахнет кровью». Ему вторит и Джулиан Йорк: «Не будьте техно-утопистами. Твиттер хорош для распространения новостей, но революция была совершена не в сети»[232].

В ответ на это очень важную мысль высказала[233] Зейнеп Туфеки: «Я не понимаю дихотомии «В сети или не в сети». Интернет является частью реального мира и играет свою роль». Она также добавляет[234], что попытки ответить на вопрос, была ли Твиттер-революция – это то же самое, что «спросить, была ли Французская революция революцией печатного станка?»

К критикам теории «твиттер-революций» относится также обозреватель Евгений Морозов, автор статей «Почему Интернет подводит иранскую оппозицию»[235], «Как диктаторы наблюдают за нами в сети»[236] и многих других, где он приводит примеры того, как социальные медиа становятся палкой о двух концах, когда их берет на вооружение правительство, и как они становятся бесполезными, когда власти блокируют доступ к мировой Сети. Эти статьи стали частью его обширной полемики с Клэем Ширки, ставшей знаковой для развития дискурса. Аргументы обоих исследователей подробно разобраны в статье Филиппа Майера «С чем я не соглашусь в споре «Морозов против Ширки» о социальном активизме в Интернете»[237].

Поборники новых технологий указывают на то, что отсутствие телефона или Интернета во времена первых революций не означает, что их появление никак не увеличило возможности для уличных протестов и не позволило им становиться более эффективными там, где раньше они были невозможны.

Адъюнкт-профессор Вашингтонского университета Филипп Говард с командой исследователей проанализировали миллионы твитов, видеоро-

---

230 David Weinberger. Gladwell proves too much [Electronic resource]/Joho the Blog, February 4, 2011. Mode of access: http://www.hyperorg.com/blogger/2011/02/04/gladwell-proves-too-much/

231 http://twitter.com/anthonyshadid

232 http://twitter.com/#!/jilliancyork/status/25972726774636544

233 http://twitter.com/#!/techsoc/status/25973597747023872

234 http://twitter.com/#!/techsoc/status/25984459006279680

235 Evgeny Morozov. Why the internet is failing Iran's activists [Electronic resource]/Prospect Magazine, January 5, 2010. – Mode of access: http://www.prospectmagazine.co.uk/2010/01/why-the-internet-is-failing-irans-activists/

236 Evgeny Morozov. How dictators watch us on the web [Electronic resource]/Prospect Magazine, November 18, 2009. – Mode of access: http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/

237 Patrick Philippe Meier. Where I Disagree with Morozov vs Shirky on Digital Activism [Electronic resource]/iRevolution. From innovation to revolution, January 7, 2010. – Mode of access: http://irevolution.net/2010/01/07/morozov-vs-shirky/

ликов и записей в блогах и заключили[238], что «социальные медиа сыграли центральную роль в формировании политического плюрализма перед Арабской весной. Результаты показали, что поток сообщений о свободе и демократии в социальных медиа привел людей на Ближнем Востоке и в Северной Африке к мысли об успехе политических демонстраций. Люди, разделявшие стремление к демократии выстроили устойчивые социальные сети и организовали политическую активность. Социальные медиа стали важнейшим инструментом в арсенале демократического движения».

Подводя итог этому обзору основных точек зрения на вопрос о том, могли ли состояться массовые волнения в Иране и революции в Тунисе и Египте без использования новых медиа, приведем цитату из статьи Клэя Ширки «Политическая сила социальных медиа»[239]:

«Гораздо более обещающей видится роль социальных медиа как долгосрочных условий для укрепления гражданского общества и общественной среды. В противовес «инструментальному» подходу к рассмотрению сети Интернет, этот можно назвать «атмосферным» [environmental – так в тексте]. Согласно этой концепции, положительные изменения в жизни той или иной страны, включая смену режима на более демократический, скорее следуют, а не предшествуют, развитию сильной общественной среды».

К этой точке зрения склоняется и доклад «The Contribution of Facebook to the 2011 Tunisian Revolution: A Cybepsychological Insight», опубликованный в научном журнале Cyberpsychology, Behavior, and Social Networking, который приводит следующую точку зрения: «Протесты в современных странах вызваны не только экономической нуждой, но и в большей степени стремлением к таким человеческим ценностями как свобода и достоинство, с учетом культурных особенностей и общей гражданским сознанием. В условиях арабского мира такое стремление было усилено сетью Интернет как площадкой для спонтанного гражданского коллективного взаимодействия, в котором приняли участие представители разных общественных классов»[240].

Таким образом, мы видим, что в рассмотрении проблематики «Твиттер-революций» исследователи расходятся касательно роли интернет-техноло-

---

238 Catherine O'Donnell. New study quantifies use of social media in Arab Spring [Electronic resource]/University of Washington, September 12, 2011. – Mode of access: http://www.washington.edu/news/articles/new-study-quantifies-use-of-social-media-in-arab-spring

239 Clay Shirky. The Political Power of Social Media [Electronic resource]/Foreign Affairs. – Council on Foreign Relations, January/February 2011. – Mode of access: http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media

240 Yousri Marzouki, Inès Skandrani-Marzouki, Moez Béjaoui, Haythem Hammoudi, and Tarek Bellaj. The Contribution of Facebook to the 2011 Tunisian Revolution: A Cyberpsychological Insight [Electronic resource]/Cyberpsychology, Behavior, and Social Networking, May 2012, 15 (5). – p. 237-244. – Mode of access: http://online.liebertpub.com/doi/abs/10.1089/cyber.2011.0177.

гий, однако зачастую поднимаемые ими вопросы носят скорее философский характер: Какое место имеют социальные медиа в современном обществе? Являются ли они одним из условий демократизации современного общества? Было ли развитие интернет-технологий обязательным условием для революций в Египте и Тунисе? В попытках ответить на эти и другие связанные с ними вопросы исследователи приходят к разным выводам, многие из которых выглядят сейчас вполне жизнеспособными. В общем и целом появляющиеся концепции можно разделить на «техноскептические» и «техноутопические», однако и это тоже является большим упрощением.

Все эти вопросы еще долго будут интересовать ученых, однако одно мы можем с полной уверенностью констатировать уже сейчас: тема использования социальных медиа как политического инструмента прочно заняла свое место в научном дискурсе и открывает большие перспективы для дальнейшего исследования.

4.2.2. Социальные и технологические предпосылки использования новых медиа для организации гражданских беспорядков

Как уже отмечалось, социально-политические беспорядки затронули не только Иран, Египет и Тунис, однако формулу «твиттер-революция» принято использовать только по отношению к этим трем странам. В чем же заключаются в данном случае причины социально-деструктивной роли сетевых технологий, радикально повлиявших на развитие гражданских волнений в этих странах? Что принципиально отличает развитие ситуации в них от параллельных политических потрясений в Сирии, Ливии, Йемене? Ответы на эти вопросы не могут носить простого и однозначного характера, так как мы имеем дело здесь с комплексом гетерогенных факторов.

Прежде всего, следует указать, что истоки волнений в этих трех странах далеко не сводятся к макроэкономическим причинам, как это было зачастую характерно для арабских революций прошлого. Экономика Египта за тридцать лет правления Хосни Мубарака выросла в 4,5 раза[241]. В Тунисе при президенте Бен Али темпы роста экономики не опускались ниже 5% в год[242] (для сравнения: рост экономики США в 2010 году составил 3,0%[243]). Экономика Ирана на 2010 год была 18-ой в мире по объёму национального производства (по данным ЦРУ, 2010) и крупнейшая среди государств Западной

---

241 Андрей Коротаев, Леонид Исаев. Революция бугров и разломов [Электронный ресурс] // Эксперт, 2012, №30-31 (813), стр.7. – Режим доступа: http://expert.ru/download/1/magazine/381960/

242 Сергей Долмов. Вирус в колыбели [Электронный ресурс] // Эксперт, 2012, №30-31 (813), стр.18. – Режим доступа: http://expert.ru/download/1/magazine/381960/

243 http://ru.wikipedia.org

Азии, Ближнего Востока и ОПЕК. Иран по объёму ВВП является крупнейшей экономикой в исламском мире после Турции.

Нельзя считать основной причиной социального взрыва и фактор бедности. Доля населения, живущего менее чем за $2 в день в Иране в 2008 году составляла всего 7% (для сравнения: в России – 12%)[244]. В Египте и Тунисе доля населения, живущего в крайней бедности (менее чем на 1,25 доллара на человека в день) была чрезвычайно мала и вполне сопоставима с соответствующей долей в таких откровенно благополучных странах, как Эстония или Словения.

Главный редактор журнала India Today Муджибур Акбар считает, что «демонстрации в Индии являются частью международного движения против коррупции, которое охватило многие страны мира, в том числе Тунис и Египет»[245]. Впрочем, по данным Transparency International уровень коррупции в Тунисе и Египте был далеко не самым высоким, а в Тунисе накануне революции был даже несколько ниже, чем в Италии[246].

Относительно высокий уровень жизни сделал возможным широкое распространение доступа к Сети, а также приобретение значительными слоями населения мобильных телефонов с доступом к Сети, однако и это не может дать нам ключ к пониманию причин «твиттер-революций». Очевидно, что сам по себе фактор развития и широкого распространения интернет-технологий не может стать решающей предпосылкой для начала волнений.

В качестве фактора, косвенно связанного с экономическим ростом, и ставшего «катализатором» волнений в Тунисе, Египте и Иране, принято рассматривать омоложение населения в этих странах. Стремительное снижение смертности, в том числе младенческой (например, в Египте с 1970-го по 1990-е годы общая смертность упала в два раза, младенческая – в три, а детская – в четыре раза), вкупе с запоздалым снижением рождаемости привело к резкому росту доли молодежи в общей численности населения, в том числе взрослого, то есть к так называемым «молодежным буграм» (необычно высокой доле молодежи в общем взрослом населении), что потенциально заключает в себе угрозу дестабилизации политических систем[247]. На начало рассматриваемых событий в Тунисе средний возраст жителей составлял 30 лет, в Египте – 24[248], а в Ира-

---

244 Бедность в мире [Электронный ресурс] // RATE1, 11 сентября 2009. – Режим доступа: http://www.rate1.com.ua/issledovanija-rate1/1290/

245 Сергей Филатов. Ближний Восток: «Идеальный шторм» [Электронный ресурс] // Международная жизнь, 28 февраля 2011. – Режим доступа: http://interaffairs.ru/read.php?item=664

246 Андрей Коротаев, Леонид Исаев. Революция бугров и разломов [Электронный ресурс] // Эксперт, 2012, № 30-31 (813), стр.8. – Режим доступа: http://expert.ru/download/1/magazine/381960/

247 Андрей Коротаев, Леонид Исаев. Революция бугров и разломов [Электронный ресурс] // Эксперт, 2012, № 30-31 (813), стр.8. – Режим доступа:://expert.ru/download/1/magazine/381960/

248 Philip N. Howard. Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring? [Electronic resource]/Project on Information Technology and Political Islam, September 11, 2011. – Mode of access: http://pitpi.org/?p=1051

не более 70% населения родилось после 1979 года[249]. Вкупе с повсеместным распространением высшего образования и высоким уровнем безработицы среди молодежи в возрасте 18-29 лет (по данным местной прессы, в Тунисе в 2009 году этот показатель составлял 49%[250]) это создавало идеальные условия для социального взрыва в среде молодежи – категории населения, наиболее активно пользующейся социальными сетями.

Впрочем, одного только фактора социальной напряженности для серьезного политического потрясения, каким стали перевороты в Египте и Тунисе и которым грозили обернуться протестные акции в Иране, было бы недостаточно. Среди других возможных причин эксперты называют конфликты в среде правящих элит: в случае Туниса говорят о противостоянии армии и спецслужб, на которые опирался президент Бен Али, а в случае Египта – между армейской верхушкой и группировкой сына президента Гамаля Мубарака[251]. В Иране же, где попытка переворота провалилась, элиты объединяет общее понимание необходимости исламской власти в стране, которую сейчас возглавляет шиит Ахмадинежад, ведущий свой род от пророка Мухаммеда.

Существует и другое видение ситуации. События в Тунисе, Египте и Иране вписываются не только в концепцию «твиттер-революций», но и в более общую – «цветных революций». Эта точка зрения проистекает из того обстоятельства, что произошедшие там потрясения не имели в своей основе свойственных классическим революциям рубежа XIX-XX веков причин и прежде всего – то, что они произошли в отсутствие революционной ситуации, три главных признака которой указывал в своей работе «Крах II Интернационала» В. И. Ленин[252].

По одному из определений, «цветная революция» – это «государственный переворот, осуществленный с преимущественным использованием методов ненасильственной борьбы, силами «цветного» движения», как правило «в интересах и при непосредственном участии в планировании, организации и финансировании со стороны иностранного государства, группы иностранных государств, общественных или коммерческих организаций»[253]. Казалось бы, в этом определении ничто не говорит нам об использовании новых медиа, однако директор Института политических исследований С. А. Марков

---

249 Freedom on the Net 2011 – Iran [Electronic resource]/Freedom House, 2011. – Mode of access: http://www.unhcr.org/refworld/pdfid/4dad51b6d.pdf

250 Сергей Филатов. Ближний Восток: «Идеальный шторм» [Электронный ресурс] // Международная жизнь, 28 февраля 2011. – Режим доступа: http://interaffairs.ru/read.php?item=664

251 Андрей Коротаев, Леонид Исаев. Революция бугров и разломов [Электронный ресурс] // Эксперт, 2012, № 30-31 (813), стр.9. – Режим доступа: http://expert.ru/download/1/magazine/381960/

252 Подробнее в статье «Секреты «Цветных революций», Елена Пономарева, журнал «Свободная мысль», 2012, № 1/2 (1631)

253 Михаил Остроменский. Основы противодействия гражданского общества «цветным» революциям [Электронный ресурс] // Война и мир, 23 октября 201. – Режим доступа: www.warandpeace.ru/ru/exclusive/view/62983/

акцентирует внимание на технологической природе «цветных революций», понимая под ними «новый тип политических технологий по смене политической власти»[254]. В этой работе мы не будем вдаваться в анализ геополитических аспектов, лежащих в основе событий в Тунисе, Египте и Иране, а остановимся на сути и технологиях цветных революций как особого феномена, неразрывно связанного с использованием социальных медиа.

Как следует из определения «цветной революция», такая форма политического переворота требует как одно из обязательных условий внешнее ненасильственное вмешательство. Косвенным доказательством такого вмешательства во время событий на Ближнем Востоке может служить, например, размещение на страницах израильской газеты «Маарив» подробной инструкции египетских революционеров. В ней, в частности, на литературном арабском языке была предложена тактика действий оппозиционеров в период восстаний. Эта простая с виду инструкция давала революционерам чёткий план действий с описанием первоочередных для штурма объектов, учила, как правильно выбрать экипировку, противостоять полиции и останавливать машины спецслужб, описывала примерное содержание плакатов и лозунгов. Распространять документ рекомендовалось через e-mail или в печатном виде. Авторы документа также намеревались провести серьёзную агитацию в египетской армии и привлечь военных на свою сторону. Они уверяли демонстрантов, что если на улицы выйдут десятки тысяч людей, полиция с такой массой справиться не сможет. На картах, прилагающихся к документу, указан план по захвату кварталов вокруг резиденции Мубарака, нейтрализации полицейских участков и дорог[255].

Другим примером деструктивного вмешательства в медийное поле Египта может послужить деятельность египетского активиста Ваэля Гонима, с января 2010 года работавшим директором по маркетингу Google на Ближнем Востоке и в Северной Африке. Так, перед началом активной фазы выступлений в Египте, Гоним создал в Facebook страницу We are all Khaled Said, где призывал сограждан выходить на улицы и противостоять правительственным силам[256]. Ваэль был арестован полицией во время беспорядков и отпущен лишь по требованию организации Amnesty International через 11 дней. Освободившись из-под стражи, Гоним немедленно дал пространное, эмоциональное и при-

---

254 С. Марков. Цветная революция – это новый тип политических технологий по смене политической власти [Электронный ресурс] // km.ru, 15 ноября 2005. – Режим доступа: www.km.ru/glavnoe/2005/11/15/arkhiv/

255 Сергей Грачев. Информационные технологии в египетских событиях 2011 года. [Электронный ресурс] // Вестник Института стратегических исследований ПГЛУ, 2012, №3. – Режим доступа: http://www.pglu.ru/science/researches/nii-panin/vestnik/v3/Grachev_Sheshneva_Zavjalov.pdf

256 Jon Swaine. Egypt crisis: the young revolutionaries who sparked the protests [Electronic resource]/The Telegraph, February 11, 2009. – Mode of access: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8317055/Egypt-crisis-the-young-revolutionaries-who-sparked-the-protests.html

зывное телеинтервью, которой послужило значительным импульсом к новым массовым выступлениям. Газета The Times по этому поводу отметила, что «… специалист по компьютерам Ваэль Гоним стал лицом народных волнений в Египте, первым из новой породы молодых революционных лидеров, превративших мышку и клавиатуру в оружие, способное свергнуть диктатуру»[257].

На первый взгляд может показаться, что Ваиль Гоним, действовал сугубо как частное лицо, с 2010 г. развивая деятельность протестного сообщества на платформе главного конкурента своего работодателя – Facebook. При этом, как утверждается, Гоним не обсуждал и не координировал свою деятельность с представителями Facebook, хотя и выражал в интервью надежду встретиться с Марком Цукербергом, чтобы поблагодарить его за возможности, которые Facebook предоставила египтянам. Более того, свою деятельность в качестве интернет-активиста топ-менеджер Google на Ближнем Востоке поначалу осуществлял параллельно с исполнением своих обычных рабочих обязанностей в Google, ведя, по его собственному признанию, двойную жизнь.

Сложно поверить, что высокопоставленный сотрудник международной корпорации мог вести обширную общественную деятельность без ведома работодателя и не в ущерб исполнению своих непосредственных обязанностей. Особенно сомнительным это кажется на фоне все учащающегося вмешательства в международные дела компании Google, которая, по выражению основателя сайта Wikileaks Джулиана Ассанжа, сейчас «претендует едва ли не на место идеолога американской империи»[258]. Характерным случаем подобного вмешательства стало, например, выступление главного юриста компании Дэйвида Драммонда в январе 2010 г., в котором он выступил с резкими заявлениями в адрес властей КНР. Google не только обозначил Пекин как главного подозреваемого в серии «весьма продвинутых хакерских атак» на почтовые ящики китайских правозащитников в декабре 2009 г., но и пошел еще дальше, увязав этот эпизод со своим решением об отказе цензурирования поисковых запросов в китайском сегменте интернета и возможном уходе с китайского поискового рынка[259].

Еще одним примером организации оппозиционной молодежи с помощью социальных медиа в Египте является деятельность «Движения 6 апреля». Участники движения использовали Facebook, Twitter, блоги для привлечения внимания общественности к своим действиям, информирования

---

257 Мартин Флетчер. Толпы приветствуют мечтателя из Facebook, вдохновившего нацию [Электронный ресурс] // Инопресса, 9 февраля 2011. – Режим доступа: http://www.inopressa.ru/article/09Feb2011/times/facebook.html

258 Julian Assange. The Banality of 'Don't Be Evil'. [Electronic resource]/The New York Times, June 1, 2013. – Mode of access: http://www.nytimes.com/2013/06/02/opinion/sunday/the-banality-of-googles-dont-be-evil.html?smid=tw-share&_r=3&

259 Олег Демидов. Социальные сетевые сервисы в контексте международной и национальной безопасности [Электронный ресурс]/Индекс Безопасности, №4 (99), Том 17, стр. 63. – Режим доступа: http://www.pircenter.org/kosdata/page_doc/p2714_1.pdf

СМИ, предупреждения о действиях полиции и организации правовой защиты оппозиционеров[260]. Характерно, что в марте 2010 года некоторые из лидеров движения были приняты американской стороной[261] и прошли обучение в области технологий общественной мобилизации, стратегического планирования и использования новых средств коммуникации. Кроме того, они учились тому, как «сделать гражданское общество компетентным в вопросах информации» и «способствовать тому, чтобы политики и общественность делились в Интернете информацией об истинном положении демократических свобод в Египте»[262].

29 января 2011 года WikiLeaks распространило материалы, которые аргументировано продемонстрировали, что США предпринимали усилия для смены режима в Египте, используя для этого, в частности, «Движение 6 апреля»[263]. В документах упоминается, что ряд блоггеров приняли участие в одной из обучающих программ, организованных в Вашингтоне НПО Freedom House под называлась «New Generation» (Новое поколение). Она была профинансирована госдепартаментом США и Агентством США по Международному Развитию и была направлена на обучение так называемых «политических и социальных реформаторов»[264]. В январе 2010 года данная поддержка была оказана американскими дипломатами тогда еще формирующейся египетской оппозиции с целью организовывать «демократический» государственный переворот. Она была публично озвучена в программе под названием «Проект за демократию на Ближнем Востоке» (Pomed – Project on Democracy on the Middle East)[265]. Характерно, что программа не ограничивалась только территорией Египта, но и касалась всего Ближнего Востока.

Из материалов газеты «The Guardian», следует, что в США в настоящее время реализуется программа информационного воздействия с использованием социальных сетей Twitter и Facebook. В центре управления программой на базе ВВС США «Макдилл» в штате Флорида работают 50 операторов, каждый из которых курирует до 10 «агентов влияния», находящихся в раз-

---

260 Courtney Radsh. Core to Commonplace: The evolution of Egypt's blogosphere [Electronic resource]/ Arab media society, Issue 6, Fall 2008. – Mode of access: http://www.arabmediasociety.com/?article=692

261 Bloggers Learn New Media Tools [Electronic resource]/Freedom house, – Mode of access: http://www.freedomhouse.org/template.cfm?page=115&program=84&item=87

262 БИТВА ЗА ВОСТОК. ЧАСТЬ II. Египетское «Движение 6 апреля» – арабский «Отпор»? [Электронный ресурс] // WORLD INVESTIGATION NET. – Режим доступа: http://old.win.ru/win/8045.phtml

263 За революцией в Египте стоит Вашингтон [Электронный ресурс] // LR News, 31 января 2011. – Режим доступа: http://lrnews.ru/news/full/25311/

264 Secretary Rice Meets with 'New Generation' of Egyptian Reformers [Electronic resource]/Freedom house, December 2007. – Mode of access: http://www.freedomhouse.org/article/secretary-rice-meets-new-generation-egyptian-reformers

265 БИТВА ЗА ВОСТОК. ЧАСТЬ II. Египетское «Движение 6 апреля» – арабский «Отпор»? [Электронный ресурс] // WORLD INVESTIGATION NET. – Режим доступа: http://old.win.ru/win/8045.phtml

личных странах мира[266]. В свете этой информации не стоит удивляться тому, что, по данным спецслужб, в ходе двух североафриканских бунтов во франкоязычном Тунисе и в арабском Египте до четверти сетевых публикаций (где собираться, что при себе иметь и т. д.) были англоязычными[267].

В своей статье «Секреты «цветных революций»[268] профессор МГИМО (У) МИД России, Елена Пономарева пишет о том, что организация смарт-толпы[269] осуществляемая посредством социальных сетей и интернет-ресурсов, стала важнейшим фактором организации беспорядков на Ближнем Востоке. Так, везде, где происходили события «арабской весны», для привлечения союзников протестующие использовали новые интернет-приложения и мобильные телефоны, перебрасывая ресурсы из киберпро-странства в городское пространство и обратно. Для посетителей социальных сетей создавалось впечатление, что в протестные действия включились миллионы людей. Однако в действительности число реально протестующих и протестующих в сети различается многократно. Достигается это с помощью специальных программ. Одна из этих программ, созданная компанией HBGary Federal для правительства США, может создавать многочисленные фиктивные аккаунты в соцсетях для манипулирования и влияния на общественное мнение по спорным вопросам, продвигая пропаганду[270]. ВВС США также заказала разработку Persona Management Software, которую можно использовать для создания и управления фиктивными аккаунтами на сайтах социальных сетей, чтобы искажать правду и создавать впечатление, будто существует общепринятое мнение по спор-ным вопросам. «Персонажи» соцсетей должны производить впечатление, что они происходят почти из любого места в мире и могут взаимодействовать посредством обычных онлайн-сервисов и сетевых платформ. В июне 2010 года эта программа была запущена[271].

---

266 Карякин В.В. Наступила эпоха следующего поколения войн – информационно-сетевых. Каков будет наш ответ на этот вызов? [Электронный ресурс] // Зарубежное военное обозрение, 22 апреля 2011. – Режим доступа: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html

267 Сергей Филатов. Ближний Восток: «Идеальный шторм» [Электронный ресурс] // Международная жизнь, 28 февраля 2011. – Режим доступа: http://interaffairs.ru/read.php?item=664

268 Елена Пономарева, «Секреты «Цветных революций» (продолжение) [Электронный ресурс] // Свободная мысль, 2012, №3/4 (1632), стр. 43. – Режим доступа: http://svom.info/media/files/2012/07/04/Svobodnaya_misl_3.pdf

269 «Смартмо́б (англ. smart mob – умная толпа) – форма самоструктурирующейся социальной организации посредством эффективного использования высоких технологий. Смартмобы организуются посредством сети Интернет и беспроводных устройств – мобильных телефонов и PDA.» – http://ru.wikipedia.org

270 Darlene Storm. Army of Fake Social Media Friends to Promote Propaganda [Electronic resource]/PCWorld, February 23, 2011. – Mode of access: http://www.pcworld.com/article/220495/army_of_fake_social_media_friends_to_promote_propaganda.html

271 George Monbiot. The need to protect the internet from 'astroturfing' grows ever more urgent [Electronic resource]/The Guardian, February 23 2011. – Mode of access: http://www.guardian.co.uk/environment/georgemonbiot/2011/feb/23/need-to-protect-internet-from-astroturfing

Пономарева пишет также о том, что социальные медиа стали важным средством подготовки и осуществления «цветных революций» прежде всего в силу того, что «позволили активизировать зрелищную сигнальную семантику», позволяющую создать коллективное чувство – синтонию, формирующую новое качество отношений между объектами воздействия, то есть зрителями, а кроме того создающую эффект самоидентификации с героями сюжетов[272]. Значительную роль на этом направлении сыграл видео-сервис YouTube, позволяющий мгновенно распространять по мобильной связи как подлинные, так и ретушированные или просто сфальсифицированные видеосюжеты, возбуждающие в сенсибилизированном обществе генерализованные реакции ужаса, переходящего в яростное неприятие заведомо указанного виновника. В роли последнего, как правило, выступают политический лидер или члены правящей партии[273].

Итак, мы видим, что широкое использование социальных медиа в протестном движении в Иране, Тунисе и Египте во многом было обусловлено высокой долей образованной, но нетрудоустроенной молодежи в населении этих стран, получившей благодаря относительно высокому уровню жизни возможность доступа к сети Интернет. Значительную роль в поддержке этого движения оказали силы из-за рубежа, прежде всего США, воспитывавшие гражданских активистов и обучавшие их пользоваться средствами новых медиа, а также осуществлявшие серьезную координационную и моральную поддержку оппозиции при помощи различных манипулятивных технологий, усиливавших эффект от действий активистов в сети Интернет.

4.2.3. Деструктивно социально-сетевые технологии

Все ведущие мировые Интернет-сервисы, – Facebook, YouTube, Twitter и др. – были созданы в США. Там они достигли пика своего развития, там же были впервые разработаны и применены наиболее эффективные модели взаимодействия с помощью этих сервисов, новых медиа. В США же были разработаны и наиболее продвинутые технологии по смене политических режимов. Теоретическую основу для этих исследований заложил американский общественный деятель Джин Шарп. В 1983 он основал институт Альберта Эйнштейна, специализирующийся на методах ненасильственной борьбы против недемократических режимов. Одним из основных спонсоров этого образования является Национальный фонд демократии, где 6 ноября 2003 года президентом Дж. Бушем был впервые сформулирован план «реконструкции» Ближнего Востока. Впрочем, главной заслу-

272 Елена Пономарева. Секреты «Цветных революций» [Электронный ресурс] // Свободная мысль, 2012, № 1/2 (1632), стр. 93. – Режим доступа: http://svom.info/media/files/2012/07/04/Svobodnaya_misl_1.pdf

273 Там же

гой Джина Шарпа, которого журналисты New York Times назвали идейным отцом Арабской весны[274], являются его труды «От диктатуры к демократии» («From Dictatorship to Democracy») и «198 методов ненасильственных действий» («198 Methods of Nonviolent Action»). Книги Шарпа переведены на десятки языков (в 2012 сообщалось о 44 переводах) и используются, как практические пособия борцами против государственной власти во всем мире. Существует и арабский перевод[275]. Эти работы, в частности, использовались на тренингах в Каире Международным центром ненасильственных конфликтов. Там с идеями американского учёного познакомились тунисские оппозиционеры. «Братья-мусульмане», которые выложили брошюру Шарпа «От диктатуры к демократии» на своём сайте, чтобы с ней мог ознакомиться любой желающий[276]. Эти труды Шарпа предлагают способы ненасильственного сопротивления политическим режимам с целью смены власти. Вместо насилия такая борьба использует психологическое, социальное, экономическое и политическое оружие, применяемое населением и общественными институтами[277]. Именно такой сценарий удалось претворить в жизнь оппозиционерам в Египте и Тунисе, где правительство было свергнуто без открытого военного противостояния.

Будучи написанными и впервые изданными в первой половине девяностых, эти работы не могли содержать никаких сведений об использовании социальных медиа, однако содержащиеся в них практические советы по противодействию правительству нашли в открытых форматом Web 2.0 возможностях благодатную почву для развития.

Одним из примеров использования техник Джина Шарпа в тесной связке с возможностями новых медиа может послужить «эпидемия» самосожжений с немедленной героизацией жертв в сетевых медиа, сыгравшая роль «запала» «арабской весны» в Тунисе и Египте. Надо отметить, кстати, что созданию «кумиров» предшествовала длительная подготовка исламского общества к восприятию самоуничтожения как подвига, что явно противоречит канонам ислама[278]. Методологически побуждение к самоуничтожению числилось в рецептуре перехода «от диктатуры к демократии» Дж. Шарпа под пунктом 158 – «Самоотдача во власть стихии (самосожжение, утопление и т. п.)»[279]. О роли самосожжений и их отображении в социальных медиа

---

274 http://www.nytimes.com/2011/02/17/world/middleeast/17sharp.html?pagewanted=all&_r=1&

275 http://www.bbc.co.uk/russian/international/2012/02/120217_gene_sharp_revolutions_interview.shtml

276 http://www.ng.ru/world/2011-02-18/1_revolutions.html

277 Джин Шарп. От диктатуры к демократии. Режим доступа: http://www.aeinstein.org/organizations/org/FDTD_Russian.pdf

278 Елена Пономарева, «Секреты «Цветных революций», журнал «Свободная мысль», 2012, №1/2 (1632), стр. 95

279 См. G. Sharp. The Methods of Non-violent Action. Boston, 1973.

писала М. Джойс, издатель сайта «Meta-Activism». Акты самосожжения – это «наглядно и это шокирует… Что сделало истории Буазизи, Саида и аль-Хатиба резонансными? Их необыкновенная брутальность, причем брутальность, видимая на фото- и видеоснимках сразу после происшедшего. Увидеть эти картинки – куда более чувствительно, чем о них услышать, и уже испытываемый гнев против режима достигает лихорадочной амплитуды»[280].

Хорошо растиражированные в социальных сетях трагические истории Халида Саида, Мохаммеда Буазизи и Неды Солтани[281] вполне вписываются и в то, что Джин Шарп пишет о механизме «перемены убеждений», применяемом в ходе ненасильственной борьбы: «Если члены группы противника эмоционально тронуты страданиями от репрессий против мужественных участников ненасильственного сопротивления или рационально убеждаются в справедливости дела движения сопротивления, они могут принять цели участников сопротивления»[282].

А вот, что Шарп пишет по поводу методов информационной подготовки восстания: «Общие руководства по сопротивлению могут быть подготовлены и распространены с помощью заблаговременного стратегического планирования. В них могут быть описаны случаи и обстоятельства, при которых население будет протестовать и ограничивать сотрудничество, а также возможные способы проведения данных действий. Теперь, даже при отсутствии связи с демократическими лидерами и невозможности выпуска или получения конкретных инструкций, население будет знать, как действовать в некоторых важных случаях»[283]. Возможности сети Интернет значительно упрощают эту задачу лидеров сопротивления.

Меры ненасильственной борьбы перечислены в работе Джина Шарпа «198 методов ненасильственных действий». Вот лишь некоторые из них:

1. Публичные выступления
2. Письма протеста или поддержки.
3. Декларации организаций и учреждений
4. Публичные заявления, подписанные известными людьми
5. Декларации обвинения и намерений
6. Групповые или массовые петиции
7. Лозунги, карикатуры и символы
9. Листовки, памфлеты и книги
10. Газеты и журналы

---

280 M. C. Joyce. Stories of Mobilization. – www.metaactivism.org/2011/06

281 См. Глава 3. Особенности использования социальных медиа в революционных процессах на ближнем востоке

282 Джин Шарп. От диктатуры к демократии. [Электронный ресурс] Режим доступа: http://www.aeinstein.org/organizations/org/FDTD_Russian.pdf

283 Джин Шарп. От диктатуры к демократии. [Электронный ресурс] Режим доступа: http://www.aeinstein.org/organizations/org/FDTD_Russian.pdf

11. Магнитофонные записи, пластинки, радио, ТВ
47. Собрание протеста или поддержки
48. Митинги протеста
49. Тайные митинги протеста
50. Семинары[284]

Социальные медиа позволяют напрямую реализовывать многие из описанных Джином Шарпом мер или способствуют реализации других, предоставляя координационные и информационные возможности для их проведения.

4.2.4. Использование социальных медиа в революционных процессах на Ближнем Востоке

В опубликованном в ноябре 2005 г. организацией Reporters Without Borders отчете Иран и Тунис значились среди 15 «врагов интернета», а Египет вошел в число десяти государств «под наблюдением[285]. В отчете утверждается, что в Иране и Тунисе действует жесткая цензура в отношении интернет-содержимого, включающая блокировку большого количества веб-сайтов, в первую очередь связанных с оппозиционерами и правозащитниками. Во всех трех странах были отмечены случаи арестов людей за содержимое их блогов. Как бы там ни было, стремительное распространение сети Интернет в регионе во второй половине 2000-х позволило социальным медиа стать относительно свободной площадкой для выражения общественного мнения по сравнению с традиционно контролируемыми и подавляемыми печатными СМИ, телевидением и радио.

В Египте

К 2011 году Египет остается относительно свободной для прессы страной с пометкой «Частично свободен» в отчете Freedom House. Как бы там ни было, распространение ложных сведений, критика президента или очернение частных лиц остаются уголовно наказуемыми деяниями[286].

В 2009 году было продлено действие закона о чрезвычайном положении, введенного еще в 1981 году после убийства президента Анвара ас-Садаты и позволяющего, в числе прочего, закрывать и цензурировать газеты «в целях национальной безопасности». Несмотря на сравнитель-

284 Джин Шарп. 198 методов ненасильственных действий. [Электронный ресурс] // Режим доступа: http://www.aeinstein.org/organizations/org/FDTD_Russian.pdf

285 Enemies of the Internet [Electronic resource]/Reporters Without Borders, 2011. – Mode of access: march12. rsf.org/i/Internet_Enemies.pdf

286 Freedom of the Press 2009 – Egypt [Electronic resource]/Freedom House, 2009. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2009/egypt

ное разнообразие печатных изданий в Египте, большая их часть и прежде всего крупнейшие принадлежат государству, а журналисты нередко становятся объектами судебного преследования и физического насилия. 57 журналистов из 13 изданий проходили по 28 делам лишь в первой четверти 2009 года[287].

Не лучше в Египте обстояли дела и с телевидением. Показателен случай, когда полиция вторглась в офис Каирской новостной компании и конфисковала часть оборудования после показа репортажа Аль-Джазиры о беспорядках в египетском городе Махала эль-Кобра[288], где также были арестованы два репортера телеканала[289].

Разительный контраст составляет с традиционными СМИ египетская блогосфера, которая в докладе Freedom House за 2010 год характеризуется как «чрезвычайно оживленная»[290]. Как следует из доклада организации Human Rights Watch за 2005 год[291], Египет уже к этому году добился положительных результатов в развитии сети Интернет. Отчет цитирует речь президента Мубарака, произнесенную на Всемирном саммите по информационному обществу в 2003 г., в которой он называет интернет инструментом для «поддержки стремления народа к большей свободе, демократии и правам человека». Исследование утверждает, к 2005 году сеть Интернет значительно распространила и усилила движение за права человека в Египте, и приводит слова правозащитника Гамаля Эида о том, что правозащитные организации в Египте могут «запускать онлайн-кампании, направленные на обычных граждан, чиновников и министров, рассылая по электронной почте письма за подписями активистов». В то же время, отмечается, что в Египте заблокированы сайты основного оппозиционного движения – «Братья мусульмане». В общем и целом, ситуация со свободой интернета в Египте являлась образцовой для региона, интернет-содержимое практически не цензурировалось, аресты блоггеров были крайне редким явлением, правозащитные организации имели возможность работать с гражданами через интернет, распространение интернет-покрытия шло при поддержке правительства с высокими темпами, интернет предоставляется неподконтрольными правительству частными компаниями-провайдерами. Значительные меры по контролю

287 Freedom of the Press 2010 – Egypt [Electronic resource]/Freedom House, 2010. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2010/egypt

288 Freedom of the Press 2010 – Egypt [Electronic resource]/Freedom House, 2009. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2009/egypt

289 В Египте арестованы два журналиста «Аль-Джазиры» [Электронный ресурс] // rin.ru, 8 апреля 2010. – Режим доступа: http://news.rin.ru/news_text/160058/

290 Freedom of the Press 2010 – Egypt [Electronic resource]/Freedom House, 2010. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2010/egypt

291 Online Censorship in the Middle East and North Africa [Electronic resource]/Human Rights Watch, November 2005 Volume 17, No. 10 (E). – Mode of access: http://www.hrw.org/sites/default/files/reports/mena1105webwcover.pdf

над Интернетом в Египте проявились лишь в 2010 году в связи с парламентскими выборами, когда многие оппозиционные блоги были заблокированы, а их авторы оказались за решеткой. Именно в этом предшествовавшем революции году статус свободы Интернета в Египте по версии организации Freedom House изменился с «частично свободен» на «не свободен»[292] (после революционных событиях Египет снова вернул себе статус «частично свободен»[293]), а организация Reporters Without Borders поместила страну в список «Врагов Интернета»[294].

Иранские медиа

В посвященных свободе прессы докладах Reporters Without Borders за 2009 и 2010 гг. Иран стабильно занимает 4 с конца место – по соседству с Туркменистаном, КНДР и Эритреей[295]. Несмотря на то, что конституция Ирана (так же, как и Египта, и Туниса) гарантирует свободу мнения и прессы, многочисленные законы все же ограничивают свободу слова. Например, статья 500 уголовного кодекса предусматривает тюремное заключение от трех месяцев до года каждому, кто будет распространять пропаганду против государства, при чем сам термин «пропаганда» остается в законодательстве не определенным. Среди прочего подразумеваются наказания и за публикацию идей, противоречащих принципам ислама и общественным порядкам Ирана.[296]

Всем этим власти Ирана охотно пользуются, что вылилось в многочисленные аресты журналистов. Согласно данным Reporters Without Borders, в 2007 году преследованию подверглись более 50 журналистов.[297] С 2000-го по 2008-й год Министерством культуры и исламского просвещения в стране было закрыто более 150 изданий.[298] Поводом для закрытия того или иного издания могло стать как публикации о жизни преуспевающих западных кинозвезд, так и освещение беспорядков внутри страны, что стало поводом

---

292 Rafael Lorente. Freedom House: Press freedom dropped to lowest point in a decade in 2010 [Electronic resource]/February 2, 2011. – Mode of access: http://ijnet.org/stories/freedom-house-press-freedom-dropped-lowest-point-decade-2010

293 Freedom on the Net 2011- Egypt [Electronic resource] Freedom House, 2011. – Mode of access: http://www.freedomhouse.org/sites/default/files/inline_images/Egypt_FOTN2011.pdf

294 Enemies of the Internet – Countries under surveillance [Electronic resource]/Reporters Without Borders, 2010. – Mode of access: http://en.rsf.org/IMG/pdf/Internet_enemies.pdf

295 Press Freedom Index 2009 [Electronic resource]/Reporters Without Borders, 2009. – Mode of access: http://en.rsf.org/press-freedom-index-2009,1001.html

296 Freedom of the Press 2008 – Iran [Electronic resource]/Freedom House, 2008. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2008/iran

297 Freedom of the Press 2008 – Iran [Electronic resource]/Freedom House, 2008. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2008/iran

298 Freedom of the Press 2009 – Iran [Electronic resource]/Freedom House, 2009. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2009/iran

для смертной казни журналистов курдского происхождения Абдолвахеда Бутимара и Аднана Хасанпура[299].

Доклад ассоциации иранских журналистов в 2007 году отмечал падение качества и финансовой независимости в журналистской среде, последовавшие за гонениями на независимую прессу со стороны пришедшего к власти консервативного правительства.[300] Реакция была незамедлительной: в июне 2008-го года Министерство труда и социальных вопросов Ирана пригрозило распустить ассоциацию.[301]

Несмотря на непрекращающиеся попытки иранских властей все медиа под свой контроль, проникновение сети Интернет увеличивается в стране с каждым годом: в первые семь лет тысячелетия количество пользователей увеличилось на 7,1% (что стало самым стремительным ростом в регионе)[302] и в 2008 году достигло 35% населения, в связи с чем правительство даже попыталось провести закон о смертной казни для блоггеров, пропагандирующих «коррупцию, проституцию или отступничество от веры»[303].

В отчете Human Rights Watch за 2005 год говорится и о стремительном развитии блогов в Иране, где они стали важным средством получения и распространения информации в условиях ожесточенной цензуры над традиционными СМИ. Президентство Мохаммада Хатами (1997-2005) было благоприятно для развития интернета. Этот иранский лидер проводил политику сближения с Западом, и при нем интернет-покрытие стремительно расширялось, количество пользователей увеличилось с 250000 в 2001 г. до 6,3 млн. в 2005, а к 2009 году планировалось достигнуть отметки в 25 млн. пользователей. Впрочем, этим планам не суждено было сбыться[304]. Стремительное развитие продолжалось вплоть до 2004 года, когда в преддверии очередных выборов, участвовать в которых Хатами уже не мог, силовики начали кампанию по свертыванию интернет-свобод: в стране был заблокирован доступ ко многим интернет-ресурсам, многие блогеры были арестованы. Иранское законодательство подразумевает наказания по таким недостаточно точно определен-

---

299 FIDH and LDDHI condemn the death sentence for Kurdish journalists in Iran [Electronic resource]/kurd.net, July 26, 2007. – Mode of access: http://www.ekurd.net/mismas/articles/misc2007/7/irankurdistan274.htm

300 Freedom of the Press 2008 – Iran [Electronic resource]/Freedom House, 2008. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2008/iran

301 Freedom of the Press 2009 – Iran [Electronic resource]/Freedom House, 2009. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2009/iran

302 Freedom of the Press 2008 – Iran [Electronic resource]/Freedom House, 2008. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2008/iran

303 Freedom of the Press 2009 – Iran [Electronic resource]/Freedom House, 2009. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2009/iran

304 Вопреки официальной статистике, исследование организации Freedom House за 2011 г. насчитывало немногим более 8 млн. пользователей в Иране в 2009 г. – http://expression.freedomhouse.org/reports/freedom_of_the_press/2009/iran

ным статьям как оскорбление правительственных лиц, оскорбление религии, подстрекательство, цитирование антиисламской прессы, и эти статьи были широко использованы в гонениях на блогеров. В Иране на 2005 год существовало большое количество интернет-провайдеров, однако все они были подконтрольны Иранской компании по телекоммуникациям (Data Communications Company of Iran). Таким образом, несмотря на бум в развитии сети Интернет в Иране первых 2001-2005 гг., к концу этого срока в стране сложилась одна из самых сильных систем контроля за интернетом в мире. Тенденция «закручивания гаек» углубилась в президентство Ахмадинежада: в докладе Freedom House сообщается, в частности, о введении в 2006 г. ограничения на скорость соединения к Интернету. В 2008 г. Парламент Ирана провел Закон о компьютерных преступлениях, устанавливающий наказания за шпионство, хакерство, пиратство, клевету и распространение аморальных материалов в Интернете.

СМИ в Тунисе

Несмотря на то, что президент Туниса Бен Али подписал в 2006 году указ, отменяющий предварительную цензуру для печатных изданий, согласно отчетам организации Freedom House ситуация со свободой прессы последовательно ухудшалась все предшествовавшие революции годы. Иностранная печать продолжала подвергаться премодерации, которая из прерогативы Министерства юстиции перешла в ведение Министерства внутренних дел. Согласно Закону о прессе оскорбление президента в печати каралось вплоть до пяти лет лишения свободы, а оппозиционные журналисты зачастую подвергались избиениям и преследованиям. После того, как в 2008 году Национальный синдикат тунисских журналистов объявил, что не поддержит кандидатуру Бен Али на предстоявших выборах, а годом позже осудил состояние свободы прессы в стране, проправительственные журналисты начали кампанию против оппозиционеров в совете организации. Это привело к отставке его нескольких значимых членов и проведению новых выборов руководства организации, а президент синдиката был избит полицейскими в штатском. В то же время иностранным журналистам, замеченным в критическом освещении событий в стране, власти отказывали во въезде или продлении визы.[305]

Из восьми крупных ежедневных газет, издававшихся в стране, две принадлежали правительству, а еще две – правящей партии. Частные ежедневники также находились в ведении собственников, близких к властям. Несмотря на существование семи изданий, относившихся к оппозиционным партиям и пользовавшихся относительной свободой для крити-

305 Freedom of the Press 2010 – Tunisia [Electronic resource]/Freedom House, 2010. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2010/tunisia

ки правительства, их усилия во многом сводились на нет финансовыми ограничениями и боязнью рекламодателей сотрудничать с «нежелательной прессой». Власти Туниса использовали и другие методы притеснения оппозиционных СМИ. Например, в марте 2007 года они скупили все копии оппозиционного еженедельника Эль-Мокиф с материалом о совместном участии тунисских и израильских политиков в межпарламентском совете стран Средиземноморья.[306]

В 2005 г. в Тунисе из 10102000 человек к интернету было подключено 788,415[307]. По данным Freedom House в 2007 году это количество составило 16% населения[308], в 2008 – порядка 29%[309] и в 2009-34%[310].Государство ставило себе цель обеспечить доступ к сети как можно большему числу граждан. Интернет проводился в образовательные и культурные центры, открывалось множество интернет-кафе, граждане получали в банках кредиты на льготных условиях на покупку компьютеров.

В то же время необходимо отметить, что содержимое сети подвергалось в Тунисе цензуре фактически с момента появления доступа к интернету в стране. Уже в 2000 г. у тунисцев не было доступа ко многим интернет-ресурсам, прежде всего связанных с правозащитными организациями. Кроме того, все работавшие в стране провайдеры были обязаны передавать всю доступную им информацию Тунисскому агентству по интернету и были ответственны за всю хранящуюся на их серверах информацию. Из-за этого пользователи не раз сталкивались с проблемой взлома их почтовых ящиков и аккаунтов в социальных сетях. В стране нередки случаи задержания гражданских активистов и блогеров, связанные с их онлайн-активностью. 18 августа 2008 г. правительство Туниса сделало попытку заблокировать в стране доступ к социальной сети Facebook, однако волна возмущения, прокатившаяся по стране, заставила власти отменить запрет уже менее чем через две недели[311]. Тем не менее, репрессии не прекратились и к 2009-2010 гг. достигли невиданного размаха. Цензуре начали подвергаться даже ресурсы без политического или порнографического содержания. Блоги и страницы в социальных сетях часто подвергались взлому и цензуре.

---

306 Freedom of the Press 2008 – Tunisia [Electronic resource]/Freedom House, 2008. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2008/tunisia

307 Данные в отчете приведены по статистике Тунисского агентства по интернету, размещенной по ныне недоступному адресу http://www.ati.tn/stats/

308 Freedom of the Press 2008 – Tunisia [Electronic resource]/Freedom House, 2008. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2008/tunisia

309 Freedom of the Press 2009 – Tunisia [Electronic resource]/Freedom House, 2009. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2009/tunisia

310 Freedom of the Press 2010 – Tunisia [Electronic resource]/Freedom House, 2010. – Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2010/tunisia

311 Internet Filtering in Tunisia [Electronic resource]/Open Net Initiative, 2009. – Mode of access: http://opennet.net/sites/opennet.net/files/ONI_Tunisia_2009.pdf

Слежение за Интернетом – достаточно обыденное явление для ближневосточного региона, и для фильтрации Интернет-ресурсов даже используются разработанные на Западе программы. Проект The Open Net Initiative, следящий за свободой Интернета в мире, докладывает, что в Бахрейне, ОАЭ, Катаре, Омане, Саудовской Аравии, Кувейте, Йемене, Судане и Тунисе используются западные технологии блокировки сайтов, содержащих скептические взгляды на ислам, светский или атеистический дискурс, а также сервисов знакомств и инструментов анонимизации в сети[312]. Ограничения свободы интернета также затронули интернет-кафе, которые обязали следить за тем, какие сайты просматривают их посетители и узнавать личные данные посетителей.

Таким образом, есть все основания утверждать, что несмотря на жесткий контроль со стороны властей Туниса, Египта и Ирана за содержанием и наполнением СМИ, им удавалось лишь частично контролировать медийное поле в своих странах. Вопреки отлаженному механизму регулирования традиционных СМИ и прежде всего печатных, стремительное развитие сети Интернет позволяло гражданским активистам и оппозиционерам открывать все новые и новые площадки для выражения своего мнения и организации акций. Глобальный характер Сети не позволял властям эффективно и своевременно реагировать на возникающие угрозы, что и обусловило популярность и социальных медиа в протестной среде. Развитие оппозиционных медиа в Интернете позволило возмущениям в Тунисе, Египте и Иране стать возможными и дало повстанцам возможность эффективно координироваться и обмениваться информацией в обход традиционных каналов СМИ.

4.2.5. Социально-деструктивная роль новых медиа во время событий в Тунисе, Египте и Иране

Необходимо указать, что, хотя события в Иране, последовавшие за президентскими выборами 2009 г. и не повлекли смену режима и даже не послужили причиной ослабления цензурного гнета, эти волнения стали беспрецедентными в новейшей истории страны и региона в целом. Они послужили примером использования социальных медиа оппозиционным движением в цензурных условиях, характерных для стран Ближнего Востока и Северной Африки и потому стали одной из важных предпосылок для дальнейшего развития событий на Ближнем Востоке.

---

312 Helmi Noman, Jillian C. York. West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011 [Electronic resource]/OpenNet Initative, March 2011. – Mode of access: opennet.net/west-censoring-east-the-use-westerntechnologies – middle-east-censors-2010-2011

Акции протеста в Иране в 2009 году начались после официального объявления ЦИК победы Ахмадинежада с массовых выступлений сторонников Мир-Хосейна Мусави, оппозиционного кандидата. В Тегеране несколько тысяч человек вышли на демонстрации под лозунгами «Долой диктатора!» и «Смерть диктатору!»[313]. Эти лозунги были активно поддержаны и в социальных медиа, в связи с чем 13 июня 2009 года в стране был закрыт доступ к сайтам YouTube и Facebook[314].

Подобно тому, как позднее убитый полицейскими блоггер Халид Саид стал символом революции в Египте, а совершивший самосожжение Мохаммед Буазизи – в Тунисе, «звездой» протестных выступлений после выборов в Иране стала Неда Солтани, убитая неизвестным снайпером во время беспорядков. Смерть девушки, чье имя переводится как «голос» или «призыв», была запечатлена на видео тремя свидетелями. Эти видеозаписи, широко использовавшиеся затем оппозиционерами, приобрели огромную известность по всему миру[315], а журнал Time, включивший событие в десять наиболее значимых в 2009 году, назвал это «возможно, самой широко освещенной смертью в истории»[316]. Сообщения о ее смерти, размещаемые под хэштегом[317] #neda стали «трендовой темой» сайта Twitter уже к концу дня 20 июня[318]. Позднее одному из видео присудили премию Джорджа Полка, как лучшему видеосюжету 2009[319].

Кибер-борьба в Иране началась сразу после оглашения результатов выборов, выявившего очевидные подтасовки в пользу действующего президента Ахмадинежада. Сторонники выступавшего за реформы кандидата Хусеина Музави вышли на улицы с протестом, начав параллельно DDoS атаку[320] на сайты иранского правительства и президента. Инструкции и программ-

---

313 В Иране начались демонстрации протеста против переизбрания Ахмадинеджада [Электронный ресурс] // lenta.ru, 13 июня 2009. – Режим доступа: http://lenta.ru/news/2009/06/13/iran/

314 Мобильная связь и веб-сайты отключены в Тегеране на фоне протестов [Электронный ресурс] // РИА Новости, 14 июня 2009. – Режим доступа: http://ria.ru/world/20090614/174300365.html

315 'Neda' becomes rallying cry for Iranian protests [Electronic resource]/CNN, June 22, 2009. – Mode of access: http://edition.cnn.com/2009/WORLD/meast/06/21/iran.woman.twitter/

316 The Top 10 Everything of 2009 [Electronic resource]/Time, December 08, 2009. – Mode of access: *http://www.time.com/time/specials/packages/article/0,28804,1945379_1944701_1944705,00.html*

317 Хэштег – специальная метка для сообщений в Твиттере, позволяющая объединить разнообразные сообщения от разных авторов в единое смысловое целое. (http://tyomma.ru/passport/hashtag/)

318 'Neda' becomes rallying cry for Iranian protests [Electronic resource]/CNN, June 22, 2009. – Mode of access: http://edition.cnn.com/2009/WORLD/meast/06/21/iran.woman.twitter/

319 Anonymous video of Neda Aghan-Soltan's death wins Polk award [Electronic resource]/The Guardian, February 16, 2010. – Mode of access: http://www.guardian.co.uk/media/pda/2010/feb/16/george-polk-awards

320 DoS-атака (атака типа «отказ в обслуживании», от англ. Denial of Service) – атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднён. Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). – hhttp://ru.wikipedia.org

ное обеспечение, необходимые для осуществления атаки, а также призывы присоединиться к борьбе распространялись между пользователями в сетях Facebook и Twitter[321]. В ответ правительство отключило в стране доступ к Интернету на 20 часов, а затем заблокировало доступ к Facebook.com, наложило новые фильтры и снизило скорость соединения. Тем не менее, недовольные продолжили атаки на правительственные сайты, во многом благодаря помощи со стороны общественности всего мира, привлеченной кампанией оппозиционеров в сети Твиттер. Ввиду того, что Твиттер может использоваться не только через веб-интерфейс, но и через многие сторонние сервисы и клиенты, полное перекрытие доступа к нему было невозможно[322]. Сеть стала важным инструментом для обмена информацией и организации митингов. Люди рассказывали друг другу о том, как обходить наложенные властями Интернет-фильтры и блоки, в том числе и для доступа к социальной сети Facebook и видео-сервису YouTube.

Революция в Тунисе (2010-2011)

В декабре 2010 г. в небольшом тунисском городе Сиди Бузид Мохаммед Буазизи, бедный торговец овощами, совершил самосожжение неподалеку от офиса местной администрации в знак протеста против произвола со стороны местной полиции, вымогавшей из него взятки и отнимавшей его продукты.

Распространявшиеся через социальные сети новости о его самосожжении сразу спровоцировали протесты в Сиди Бузиде и других тунисских городах. Тем не менее, телевидение и печатная пресса избегали сообщений об этих манифестациях. Значительная часть выкладываемой в интернет информации, такой как видео на YouTube, была блокирована тунисским интернет-фильтром. Фейсбук, который тогда не подвергался ограничениям, стал главным источником информации о Буазизи и волнениям в Сиди Бузиде. Твиттер, хотя и не слишком тогда еще популярный в Тунисе, также стал инструментом информирования о протестах. Люди по всему миру узнавали о происходящем в стране из этих источников. Новости, появляющиеся в твиттере, воодушевляли людей, живущих в этом регионе, таких как египетский активист Гиги Ибрагим, который после свержения президента Туниса Зайна аль-Абидина написал в свой твиттер: «The Tunisian revolution is being twitterised…history is being written by the people

321 Angela Moscaritolo. Iran election protesters use Twitter to recruit hackers [Electronic resource]/SC Magazine, June 15, 2009. – Mode of access: http://www.scmagazine.com/iran-election-protesters-use-twitter-to-recruit-hackers/article/138545/

322 Katie Combs. Iran's «Twitter Revolution» – myth or reality? [Electronic resource]/World Focus, June 19, 2009. – Mode of access: http://worldfocus.org/blog/2009/06/18/irans-twitter-revolution-myth-or-reality/5869/

#sidibouzid #Tunisia.»[323] – «Тунисская революция пишется в твиттере… историю пишет народ».

Важной вехой стала также публикация сайтом WikiLeaks доклада американского посла в Тунисе Роберта Годека[324]. Он рассказывает о частном ужине с зятем президента Мохаммадом Эль-Матери. В то время как значительная часть населения жила в условиях бедности и коррупции, в описании обеда упоминались такие детали как панорамный бассейн, римские колонны, фонтан, вытекающий из львиной головы и многие другие предметы роскоши. Доклад вызвал волну возмущения в прогрессивной части тунисского общества, и вскоре доступ к сайту Wikileaks в Тунисе был закрыт.

Меры, направленные против Wikileaks привлекли к ситуации в стране внимание международной хакерской группы Anonimous[325], инициировавшей «Операцию Тунис», результатом которой стали кибер-атаки, выведшие из строя, по меньшей мере, восемь правительственных сайтов, включая сайты президента, премьера и ключевых министров. Акция хакеров включала в себя координацию и набор волонтеров через группу в сети Фейсбук и в твиттере при помощи хэштега #optunisia.

Революция в Египте (2011)

Воодушевленные свержением президента Туниса Бен Али, египетские оппозиционеры призвали народ выйти на улицы в «День гнева» – 25 января 2011 г., чтобы выступить против 30-летнего правления президента Хосни Мубарака. Сделано это было через популярные группы в сети Фейсбук – «We are all Khaled Said»[326] – страницы в память об убитом полицейскими блоггере с несколькими сотнями тысяч египетских подписчиков и группу «Движения 6 апреля»[327]. Планы и требования протестующих распространялись как традиционно (с помощью «сарафанного радио» и распечатанных листовок), так и по электронной рассылке.

То, насколько широко были использованы социальные сети во время египетских событий, хорошо проиллюстрировало появление книги «Твиты

---

323 Alex Comninos. 2011 – Internet rights and democratization [Electronic resource]/Global Information Society Watch, 2011. – Mode of access: http://www.giswatch.org/ca/node/511

324 US embassy cables: The 'OTT' lifestyle of Tunisian president's son-in-law, including pet tiger [Electronic resource]/The Guardian, 7 December 2010. – Mode of access: http://www.guardian.co.uk/world/us-embassy-cables-documents/218324

325 Yasmine Ryan. Tunisia's bitter cyberwar [Electronic resource]/Al Jazeera, 06 January, 2011. – Mode of access: http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html

326 В фейсбуке было открыто множество страниц в память о Халиде Саиде, забитом полицией прямо возле интернет-кафе, где он пытался выложить фотографию, на которой было видно, как полицейские продают наркотики. Одна из самых популярных страниц – www.facebook.com/ElShaheeed

327 См. «6th of April Youth Movement – حركة شباب 6 ابريل», www.facebook.com/shabab6april

Тахрира», собравшей в себе записи, которые в реальном времени публиковались оппозиционерами на площади Тахрир – месте, ставшем судьбоносным для египетской революции. Важность этих сообщений нельзя переоценить, учитывая, что правительство Египта, одной из наиболее либеральных стран региона, даже распорядилось отключить Интернет и мобильную связь во многих регионах страны, включая Каир[328]. После того, как начались столкновения, значимым инструментом в руках оппозиционеров стали видеокамеры мобильных телефонов: снятые во время столкновений видеозаписи, были просмотрены сотни тысяч раз. Ролики, снятые очевидцами происшествий, появлялись на каналах крупных СМИ в Youtube, и так становились популярными. Из 20 наиболее известных видео, пять появились на канале RussiaToday[329]. Для египтян они стали важным сплачивающим фактором, поднимавшим на борьбу с властями, в то время как во всем мире эти видео вызвали волну акций в поддержку восставших. Президент Египта подал в отставку через две недели после начала волнений.

Итак, социальные сети выполняли следующие функции в протестном движении в Иране, Тунисе и Египте:

Создание оппозиционных настроений в обществе

Координирование действий оппозиции

Получение повстанцами информационной поддержки из внешнего мира

Привлечение внимания к проблеме со стороны международного сообщества

Передача информации о происходящем в условиях, когда традиционные СМИ оказываются бессильны

Обмен опытом между оппозиционерами из разных стран

Социальные медиа сыграли значительную роль в подготовке и запуске протестных событий в Тунисе, Иране и Египте, даже не смотря на то, что их проникновение в этих странах далеко отставало от показателей развитых западных государств. Во многом, их значимость для протестного движения была обусловлена цензурным бременем, лежавшим на традиционных СМИ и не позволявшем использовать их для распространения оппозиционных идей и координации действий манифестантов. Впрочем, этот фактор стал далеко не решающим. Важной особенностью новых медиа, сослужившей большую услугу участникам волнений, стала возможность быстро создавать и распространять мультимедийный контент без необходимости в сложных технических устройствах – митингующие могли делать это с помощью мобильных телефонов прямо с места событий.

---

328 David D. Kirkpatrick. Mubarak Orders Crackdown, With Revolt Sweeping Egypt [Electronic resource]/The New York Times, January 28, 2011. – Mode of access: http://www.nytimes.com/2011/01/29/world/middleeast/29unrest.html?_r=1&hp

329 Philip N. Howard. Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring? [Electronic resource]/Project on Information Technology and Political Islam, September 11, 2011. – Mode of access: http://pitpi.org/?p=1051

Особый характер событий в Тунисе, Египте и Иране обусловили и социально-демографические, а также политические причины волнений. Значительную часть недовольных, положивших начало волнениям составляла образованная, но нетрудоустроенная молодежь из крупных городов. Эти люди обладали знаниями и навыками работы в сети Интернет и потому активно использовали ее средства в своих целях. Поддержку им оказывали силы из-за рубежа, обучавшие оппозиционеров, а зачастую и непосредственно принимавшие участие в информационной борьбе на стороне оппозиции этих стран при помощи специальных приемов и технологий, позволяющих влиять на общественное мнение в социальных сетях.

Оппозиционеры использовали имевшиеся у них средства для решения самых разнообразных задач. Для распространения кратких сообщений о происходящем и привлечения международного внимания к своей борьбе они использовали сервис микроблогов Twitter, для координации протестных акций, распространения идей и специальной литературы использовалась социальная сеть Facebook, а для более красочного освещения происходящих событий в условиях информационной блокады со стороны властей использовался видео-сервис YouTube. Особая эффективность достигалась при комплексном использовании всех этих ресурсов. Нужно также отметить, что достоверность контента, размещаемого на этих интернет-сайтах, зачастую невозможно было проверить, чем могли пользоваться в своих целях как силы властей, так и зарубежные государства, стремившиеся воспользоваться протестным движением для своей выгоды.

В общем и целом, мы можем говорить, что пути использования социальных медиа в значительной степени укладывались в описанные Джином Шарпом меры по ненасильственной смене власти, которые обрели в возможностях новых Интернет-сервисов идеальную опору. Впрочем, некоторые исследователи идут дальше и утверждают, что социальные медиа были не только инструментом в руках оппозиционеров, но и сами по себе оказали влияние на развитие общественного движения за счет демократических принципов пользовательского наполнения, превративших рядовых граждан из наблюдателей в творцов окружающего их информационного поля и, соответственно, реальности.

Сейчас уже можно со всей уверенностью сказать, что социальные сети все прочнее занимают свое место среди инструментов политического влияния. Они подняли на новый уровень уже известные ранее технологии политического маркетинга и добавили новые эффективные приемы в этот арсенал. Новые медиа используются при проведении выборов и для подготовки населения к тем или иным социальным преобразованиям, однако наибольшей разрушительной силы их использование достигает в условиях открытого противостояния между властью и оппозицией в условиях политического кризиса.

Тщательное изучение опыта Ирана, Туниса и Египта должно позволить властям других государств избегнуть подобного развития событий. Главный урок заключается в необходимости тщательно анализировать информацию, размещаемую в новых медиа, чтобы быть в курсе назревших в обществе проблем и требований недовольных, а также участвовать в формировании содержимого этих сетей, чтобы не терять контроля над настроениями в обществе.

4.3. НЕПРАВИТЕЛЬСТВЕННЫЕ ОРГАНИЗАЦИИ В СИСТЕМЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА.

Зарубежные неправительственные организации как механизм влияния на внутреннюю политику России и стран СНГ.

В разведсообществе США существуют специальные межведомственные группы, занимающиеся координацией деятельности самых различных неправительственных структур, в частности, на российском направлении. Так, в Национальном совете по разведке (National Intelligence Council – NIC/Национальный совет по разведке – НСР) существует Секция российских и евразийских исследований/National Intelligence for Russia and Eurasia[330]. Это подразделение непосредственно подчинено Директору национальной разведки и отвечает за подготовку Национальной разведывательной сводки (National Intelligence Estimate), которая готовится на основе открытой информации и регулярно докладывается президенту США. Во взаимодействии с оперативными подразделениями американских спецслужб российская секция НСР участвует в координации финансирования и методического обеспечения западных и прозападных НПО в странах Восточной Европы и бывшего СССР, создавая эшелонированную сеть влияния.

Именно этим занимаются такие НПО как Национальный демократический институт, Международный республиканский институт, Международный фонд электоральных систем, фонд Джорджа Сороса – Институт «Открытого общества», «Freedom House», а также сотни других подобных организаций.

Указанные структуры аккумулировали огромные средства, санкционированные Конгрессом и Госдепартаментом США, для создания форпостов американского влияния в иностранных государствах под благовидными предлогами, чаще всего под видом помощи для построения «гражданского общества», защиты прав человека, оказания содействия в проведении «демократических» выборов и создании «альтернативной прессы».

Как подчеркивалось в исследовании Американского института предпринимательства, Национальный демократический фонд и его семейство

330 Официальный сайт директора Национальной разведки США, http://www.dni.gov

как раз и занимались изменением политического баланса в государстве-мишени под предлогом помощи «гражданскому обществу». У «семейства» были многочисленные успехи на этом поприще – удачные вмешательства для обеспечения должного результата на выборах на Филиппинах, в Пакистане, на Тайване, в Чили, Никарагуа, Восточной Европе и по всему свету»[331].

Интересные данные, вскрывающие, в том числе, роль неоконсерваторов в организации и финансировании информационных провокаций кибердиссидентами, приводятся в статье Л. Савина. Сложно сказать, где впервые появился этот новый тип борцов с правительствами, правда, не со всеми. Известно только, что к становлению сообщества кибердиссидентов приложили усилия «Репортеры без границ»[332]. Важным событием в становлении этой организации было учреждение в 2008 г. Всемирного дня борьбы против киберцензуры, который отмечается 12 марта. В том же году представители организации пытались сорвать церемонию зажжения олимпийского огня Игр-2008 в Пекине[333].

Агентура «Репортёров без границ» (РБГ) собирает информацию на местах и отправляет их тем, кто сопоставляют и анализируют факты, полученные из различных источников, после чего делается перевод материала на английский язык и обработанная информация распространяется в Интернете. Видео и фото вбрасываются на Facebook и фотоблоги[334].

Подобно «Фридом Хаус» и другим борцам за «демократию», РБГ также имеют свой индекс свобод. В отчёте, который прозвали «списком врагов Интернета», за прошедший год в разряд таких стран попали Бахрейн, Беларусь, Бирма, Китай, Куба, Иран, Северная Корея, Саудовская Аравия, Сирия, Туркменистан, Узбекистан и Вьетнам. Интересно, что обычные журналисты в версии РБГ отделены от блогеров, что свидетельствует об особом статусе и роли сетевых активистов.

Для поощрения своих информаторов «Репортёры без границ» учредили «приз обитателя Сети» в сумме 2500 евро. Его получают обычно граждане тех стран, где предпринимаются попытки демонтажа существующего режима. Так, в 2010 году премию получил информатор из Ирана, в 2011-м – из Туниса, а в 2012-м – из Сирии. Спонсором этой акции является Google, представители которого присутствуют на церемонии вручения наград. Интересы этой компании в поддержке кибердиссидентов напрямую связаны с коммерческой прибылью: продукция Google, как указывают РБГ, блокируется в 25 из 125 стран, где работает компания. Следовательно, нужно оказать давление

---

331 Чолиа С. – Демократизация, НПО и «цветные революции»

332 Савин Леонид – Кибердиссиденты. Интернет. «Фонд стратегической культуры». 02.04.2012

333 Интернет. 24.03.2008 http://www.eer.ru/archive/10481.html

334 Савин – Кибердиссиденты

на правительства этих стран изнутри, поддерживая оппозицию под предлогом защиты свободы слова в виртуальном пространстве.

Альянс Google и правительства США сложился давно[335]. Как в других крупных компаниях США, руководство которых приходит из госдепа и Пентагона, здесь тоже работают кадровые карусели. Например, в марте нынешнего года стало известно, что директор перспективного оборонного агентства DARPA Регина Дункан переходит в Google[336].

Кстати, в том же 2008 г., когда РГБ придумали день борьбы с киберцензурой, в США была создана и международная организация кибердиссидентов CyberDissidents.org[337]. Кибердиссиденты приглашают всех желающих присоединиться к их работе. Причастность США к данному проекту очевидна. Предполагают, что Вашингтон решил взять в свои руки глобальное управление протестами. Сервер, на котором размещен сайт кибердиссидентов, находится в Аризоне, США. Независимый ресурс SourceWatch указывает, что эта организация является неоконсервативной[338].

Это подтверждается и сведениями о лидерах организации. Директор и соучредитель CyberDissidents.org Давид Кейс служил координатором программ в Институте стратегических исследований Адельсона и работал помощником посла в ООН. Связь с неоконсерваторами проявляется и в том, что Кейс публикуется в их изданиях – The Wall Street Journal, The New Republic, National Review, Commentary, Daily Beast, The Jerusalem Post. Следует также отметить, что Давид Кейс имеет диплом специалиста по дипломатии Тель-Авивского университета и является основателем движения Students Against Dictators.

А Нир Бомбс, являющийся вторым лицом в организации, служил в посольстве Израиля в США и занимал пост вице-президента и директора программ Фонда защиты демократий, неоконсервативного мозгового центра в Вашингтона, где он до сих пор числится исследователем[339].

На сайте CyberDissidents.org не указаны источники финансирования организации, но есть данные, что Давид Кейс связан с Phillips Foundation[340] – ещё одной неправительственной структурой в Вашингтоне (в её Совете числится вице-президент Heritage Foundation Бэки Нортон Данлоп), поддерживающей онлайн-журнализм, американскую культуру, свободное общество и свободные рынки.

---

335 Савин – Кибердиссиденты

336 Noah Shachtman. Exclusive: Darpa Director Bolts Pentagon for Google. March 12, 2012. http://www.wired.com/dangerroom/2012/03/dugan-darpa-google/

337 http://www.cyberdissidents.org/

338 http://www.sourcewatch.org/index. php? title=Cyber_Dissidents

339 Савин – Кибердиссиденты

340 http://www.thephillipsfoundation.org

CyberDissidents.org также занимается мобилизацией американских студентов и привлекает их в качестве кибер пропагандистов и, возможно, хакеров. Последний призыв к американскому студенчеству направлен на поддержку свободы на Ближнем Востоке[341] и раскручивание арабских и иранских блогеров.

Явная причастность руководства CyberDissidents.org к политике Израиля и движению Students Against Dictators, пристальный интерес к Ближнему Востоку и к протестам молодежи Туниса, Египта, Ливии говорят сами за себя.

Деятельность кибердиссидентов связана также с распространением дезинформации о правительствах тех государств, гражданами которых они являются. Например, в Венесуэле оппозиционные интернетчики целенаправленно раскручивали мифы об антисемитизме Уго Чавеса, о государственной поддержке таких организаций, как ХАМАС и «Хизбалла», об их присутствии в Венесуэле (в анонимных публикациях они названы террористическими)[342].

Хотя США ратуют за чёткие правила в киберпространстве, контролируют Интернет и столбят за собой всяческие права[343], [344], аналогичные действия других государств трактуются Вашингтоном как ущемление прав и свобод.

В намеренно провокационной статье Стивена Кауфмана, размещенной на сайте правительства США на семи языках, говорится о том, как нужно уклоняться от цензуры в Интернете, какие существуют веб-сайты, видеоролики в сети YouTube, руководства и другие материалы, предлагающие советы, передовой опыт и инструкции по использованию анонимайзеров, прокси-серверов, средств обхода барьеров и других инструментов, затрудняющих отслеживание властями деятельности пользователя в Интернете. В статье прямо указано, что «Государственный департамент предоставляет финансирование НПО для проведения учебных программ внутри страны или для разработки новых инструментов».

Текущие программы в области гражданского общества и государственного управления, такие как курсы журналистики, получают новые дополнения к учебным программам. Начинающие журналисты и активисты не только учатся тому, как использовать Интернет более эффективно, но они также учатся делать это более безопасно»[345]. Там же приведены ссылки на пособие «Как обойти цензуру в Интернете»[346], существующее на девяти языках, в том

---

341 http://www.cyberdissidents.org/ourstudentmovement. html

342 Venezuela, el centro de operaciones de Hezbollah mas grande del continente americano. 10 julio, 2011. http://www.minutodigital.com/2011/07/10/venezuela-el-centro-de-operaciones-de-hezbollah-mas-grande-del-hemisferio/

343 Савин – Кибердиссиденты

344 http://www. fondsk.ru/news/2011/05/18/terra-americana-v-kiberprostranstve. html

345 Кауфман Стивен – Как обеспечить собственную безопасность и свободу, пользуясь средствами связи. 10 ноября 2011 года. http://iipdigital.usembassy.gov/st/russian/article/2011/11/20111110101925x0.1477254.html#axzz1pTJKi0to

346 http://www. howtobypassinternetcensorship. org/ru. html

числе на русском, и на международную организацию «Коллектив тактической технологии»[347].

Эта организация, созданная в 2003 г., учит тому, как использовать современные технологии для распространения информации, установления связи и политической пропаганды. Коллектив имеет филиалы во многих странах, а проводимые им семинары ориентированы на различные темы, например, как активизировать новую сеть активистов или применять мобильные гаджеты в уличных революциях. Как и следовало ожидать, среди доноров этой организации значатся Фонд Форда, Институт Открытого общества Сороса и ряд других с пропиской в США.

Один из современных идеологов киберлиберализма Милтон Мюллер считает, что «денационализированный либерализм выступает за всеобщее право на получение и распространение информации независимо от государственных границ и рассматривает свободу общения и обмена информацией как первичный элемент человеческого выбора, а также общественно-политической активности» <…>. денационализированный либерализм стремится превратить интернет-пользователей в автономную глобальную политическую систему.

Мюллер предлагает политизировать виртуальное пространство в чисто западном либеральном ключе. В своей книге, посвящённой государствам, управлению и сетям, он пишет: «Мы должны найти способы перевода классических либеральных прав и свобод в структуру управления, подходящего для глобальной сети Интернет. Там не может быть киберсвободы без политического движения, направленного на определение, защиту и институционализацию права и свободы личности на транснациональном масштабе»[348]. Фактически мы имеем здесь дело с идеологией упразднения государства и введения «глобального управления»[349].

В разных странах с кибердиссидентами борются по-разному. В Китае, например, существует закон, по которому их отправляют в тюрьмы. В настоящее время, по данным РБГ, в Китае в заключении находилось 68 блогеров и 30 журналистов. Россия, кстати, в этой статистике не фигурирует.

Что касается Китая и его охранительных практик, то там, как считают западные эксперты, уже давно установлен Великий Китайский Брандмауэр, который фильтрует входящую и исходящую информацию. На международном законодательном уровне Китай вместе с Россией выступают за создание чётких правил действий в киберпространстве, но их предложения игнорируются. КНР без оглядки на Запад в марте 2012 г. ввел обязательную регистрацию всех блогеров, официально запретив анонимность в Интернете.

---

347 http://www. howtobypassinternetcensorship.org/ru. html

348 Muller Milton L. – Networks and States: The Global Politics of Internet Governance. MIT Press, 2010

349 Савин – Кибердиссиденты

Для контроля ситуации в случае бунта есть два решения – отключить каналы связи, как было в Ливии, либо фильтровать и отлавливать провокаторов, как поступала полиция Нью-Йорка и Лондона во время беспорядков на улицах этих городов.

Самым оптимальным решением по отношению к антигосударственному интернационалу, действующему в виртуальном пространстве, было бы создание альтернативного кибрпространства с соответствующими правилами игры[350].

«Цветные революции» на постсоветском пространстве проводились по отработанным ещё в период холодной войны сценариям. Под псевдогуманитарными предлогами с участием НПО, щедро профинансированных правительствами и разведками (спецслужбами), осуществлялась задача по манипулированию итогами местных выборов, водворению марионеточного прозападного и, прежде всего, антироссийского правительства[351].

Существует много неполитических НПО, и некоторые из них действительно являются институтами гражданского общества, структурами самоорганизации граждан в разных сферах жизни и деятельности. Вместе с тем, особая категория НПО претендует на роль судей в вопросах мировоззрения всего общества и государственной политики.

В 60-х – 70-х годах XX века деятельность по созданию ячеек политических партий и организаций в различных странах тайно осуществляло ЦРУ. Затем было решено, что такая деятельность США будет прозрачной и публичной. Косвенным подтверждением тому являются слова первого президента Национального демократического фонда А. Вайнштейна в отношении тактики проникновения НАТО в зоны евроатлантического интереса: «Многое из того, что мы открыто делаем сейчас, 25 лет назад скрытно делало ЦРУ». На официальном уровне Вашингтон всегда открещивается от деятельности НПО за рубежом.

Описывая историю путча 2004 года в Украине, американский исследователь С. Чолиа отмечает: «Никакие из описанных махинаций не имели бы значения без оспоренного результата выборов, без собрания людей на улицах и инжиниринга демократии через гражданское неповиновение. Вот здесь-то Национальный демократический фонд и семейство международных неправительственных организаций оказались более всего нужны»[352].

В качестве примера успешной деятельности сетевой структуры можно привести работу НПО «Freedom House» (FH) по организации «цветной революции» в Украине в 2004 году.

---

350 Савин – Кибердиссиденты

351 Беликова ... – Сетевые ...

352 Чолиа С. – Добрые советы от «Freedom House». НПО как инструмент «цветных революций» на постсоветском пространстве. [http://scienceport.ru/content/dobrye-sovety-freedom-house-nepravitelstvennye-organizatsii-kak-instrument-tsvetnykh-evolyu

С ноября 2003 года FH финансировал поездку лидеров сербского движения «Отпор» по Украине. Они посетили с лекциями, посвящёнными проблеме ненасильственного сопротивления, пять крупнейших украинских городов, включая Донецк и Одессу. FH подготовил более 1000 инструкторов по выборам, которые контролировали избирательный процесс на Украине. Сотрудник FH А. Каратницкий участвовал в организации лагерей для украинских активистов, где сербы из организации «Отпор» обучали украинскую молодёжь ненасильственным (и не только) методам сопротивления власти. Так, 1 августа 2004 года в летнем кемпинге Евпатории был организован недельный слёт 320 молодых украинцев[353].

Примерная схема работы НПО такова: на начальном этапе в стране, где предполагается смена власти, под благовидным предлогом (например, «демократизация» общества) разворачивается деятельность ряда координирующих неправительственных (сетевых) структур, каждая из которых действует строго в своем секторе. С научной точки зрения социальное управление – это направленная координация и организация объекта управления – человеческих ресурсов.

Можно выделить несколько направлений работы НПО:

Первое направление – работа с оппозиционными партиями, блоками и их молодёжными структурами. Из неформальных лидеров формируются пирамиды сетевого маркетинга. Студент-лидер, создавший свою группу в количестве десяти человек и возглавивший её, получает вознаграждение. Высший доход получает тот, кто становится во главе тысячи человек.

Второе направление – работа с представителями органов местного самоуправления, направленная якобы на развитие самостоятельности областей, а на практике – на ослабление их управляемости из центра (в качестве примера можно привести движение «областничества» в Сибири и на Дальнем Востоке РФ и временное принятие Конституции Татарстана).

Третье направление – развитие подконтрольных НПО, «альтернативных» государственным СМИ.

Четвёртое направление – создание новых и укрепление уже существующих общественных организаций, а также реализация через них методов ненасильственной борьбы.

В результате деятельности международных НПО создаётся целая система приёмов и технологий, направленных на оказание выгодного влияния на внутриполитическую ситуацию в стране и обеспечение смены режима:

---

353 Революция. com или США – завоевание Востока [rutube.ru/tracks/646352.html

1. Информационная обработка общественного мнения, создание негативного образа высшего руководства страны и позитивного образа оппозиции.
2. Усиление правозащитной риторики со стороны местных и западных правозащитников, создание условий прессинга властей, при которых на уровне общественного сознания трудно уловить грань между правозащитной и провокационной деятельностью.
3. Налаживание механизма давления «международной общественности» с помощью «демократической фразеологии» с целью обеспечения «честных выборов» и «развития демократии».

Навязывание института международных наблюдателей для контроля фактически за любой проблемой. Создание таких условий, при которых международные наблюдатели становятся действенным инструментом поддержки оппозиции.

Непосредственно в ходе выборов схема, применяемая НПО, проста, однообразна, но эффективна – экзит-полы и международные рейтинговые агентства заранее сообщают о победе прозападного кандидата, официальные результаты выборов опротестовываются западными «независимыми» наблюдателями, поднимается шум в местной прессе с широким освещением на Западе, вывод людей на улицы и организация акций гражданского неповиновения.

В этой схеме «цветных революций» важнейшую роль играет сам факт международного финансирования таких переворотов, создающего разветвлённую коррупционную сеть, включающую в свою орбиту как бизнесменов, заинтересованных лиц из западных диаспор, правительственных чиновников и силовиков, так и щедро проспонсированный «альтернативный» журналистский корпус и молодёжь.

Основная форма поддержания контактов – Интернет и проведение регулярных выездных семинаров, на которые приглашаются «активисты» из России и стран СНГ. Используются также выезды зарубежных наблюдателей на выборы и референдумы в странах постсоветского пространства, в особенности в наиболее зависимые от международного общественного мнения «непризнанные» государства. Так, во время конституционного референдума в Арцахе (Нагорно-Карабахской республике) седовласый профессор из американской делегации вместе с британской аспиранткой собрали вокруг себя местную молодёжь из худо-бедно англоговорящей элиты и начали проповедовать прелести американской демократии, призывать их голосовать против Конституции и приглашали их на учёбу в США или в Британию. Услышав замечание представителей делегации МАН ПНБ о незаконности такой деятельности международных наблюдателей, они резко засмущались и собрали свои манатки[354].

354 Спектор В.Н. – Отчёт на Президиуме Академии об участии Делегации Академии в работе международных наблюдателей за проведением Референдума по Конституции Республики Арцах (Нагорно-Карабахской республики

Кроме того, региональные центры под покровительством западных спецслужб работают над созданием сетей влияния в Беларуси, Украине, Казахстане, Узбекистане, Таджикистане, Киргизии, Армении. Иногда в качестве сетей – инструментов влияния – выступают уже существующие диаспоры, землячества, религиозные секты, молодёжные объединения[355].

Особое место в продвижении «демократии» посредством «цветных революций» занимает формально независимое правительственное Агентство международного развития США/Agency for International Development – USAID (в настоящее время запрещено в России), деятельность которого ориентирована на распространение демократии по-американски и на консолидацию проамериканских режимов в мире (решение проблем, связанных с «нарушением прав человека», проведением «демократических» выборов, развитием рыночной экономики, оказанием содействия в создании «демократических» институтов).

США потратили на проведение двух «цветных» революций в Украине и в Киргизии более 110 миллионов долларов. По данным авторов документальной ленты, первоначально метод подобного переворота был опробован на Сербии. Именно там впервые нашли применение тезисы книги американца Дж. Шарпа «От диктатуры к демократии» – своеобразного руководства по применению «мирной революции» с простыми рецептами. Дж. Шарп (Gene Sharp) является научным руководителем Института Альберта Эйнштейна/Albert Einstein Institution, возглавляемого бывшим сотрудником Разведывательного управления Министерства обороны США (РУМО), полковником в отставке Р. Хэлви (Robert Helvey).

Свержение режима Милошевича, смещение в ноябре 2003 года Э. Шеварнадзе в ходе «революции роз», приход к власти на Украине в результате «оранжевой» революции в декабре 2004 года В. Ющенко и торжество киргизской «тюльпановой» революции в марте 2005 года – звенья одной цепи. «Четыре ненасильственные революции, четыре тоталитарных режима – следы былого советского могущества канули в лету за несколько недель, и каждый раз использовался один и тот же сценарий – фальсифицированные выборы, судорожно сопротивляющаяся власть, которая, в конце концов, уступает протестующим», – отмечают авторы документального фильма «Революция. com. или США: Завоевание Востока».

На постсоветском пространстве почти везде существуют разного рода представительства и офисы так называемого Международного республиканского института (МРИ) США. Чем занимаются члены этого института, стало ясно 19 мая 2005 года, когда президент США Дж. Буш поблагодарил своих сограж-

355 Макеев М. – Механизмы влияния США на Россию и СНГ

дан за огромный вклад в продвижении свободы в зарубежных странах, заявив: «Свобода демонстрирует беспрецедентный прогресс по всему земному шару, мы стали свидетелями революций «роз», «оранжевой», «пурпура», «тюльпана» и «кедра» и это только начало. По всему Кавказу и Средней Азии растут ожидания в связи с перспективами перемен, и эти перемены наступят»[356].

В целом, анализируя деятельность международных правительственных и неправительственных организаций в странах СНГ в связи с подготовкой и проведением президентских и парламентских выборов, приходится признать следующее:

1. Создан относительно эффективный, адаптированный к условиям новых независимых государств механизм изменения политического курса путём государственных переворотов с помощью избирательных кампаний.
2. Смена неугодных режимов осуществляется во взаимодействии различных заинтересованных структур, организаций и политических институтов. Главным субъектом, осуществляющим данный политический курс, являются США, которые используют в своих целях европейские организации и мировые институты (ООН, ОБСЕ, ЕС, НАТО). Авторы «Национальной военной стратегии» особо подчеркивают, что превосходство должно достигаться за счёт создания необходимых условий, а не за счёт подавляющего перевеса в численности сил и средств. В связи с этим признано необходимым преобразовать ВС США в единые сетецентричные, распределённые силы, прежде всего для совершенствования системы сбора, обработки и распределения информации. Пентагон уже приступил к развертыванию глобальной информационной сети – ГИС.

3. Основным инструментом проникновения в соответствующие страны являются многочисленные НПО и фонды. С их помощью осуществляется создание национальных оппозиционных политических сетей, которые впоследствии и составляют основную организационную и движущую силу местных революций.

Созданный механизм оказания влияния на внутриполитическую ситуацию в стране вплоть до свержения правительств в результате «цветных революций», осуществляемых в ходе выборов, представляет собой угрозу для любого режима, даже того, который был установлен в результате этих революций. Продолжающаяся деятельность НПО, наличие разветвлённых политических сетей, поддерживаемых в «рабочем состоянии», дальнейшее корректируемое из соображений целесообразности финансирование различных проектов, программ и кампа-

356 Буш: демократические революции придут на Кавказ и в Среднюю Азию», [www.rian.ru/politics/20050519/40378390.html

ний делают фактически любое правительство заложником внешнего фактора. Как только оно перестает отвечать интересам мировой закулисы, велика вероятность того, что те же самые способы, с помощью которых новое руководство, в конце концов, пришло к власти, могут быть использованы и для его свержения.

4.3.1. Неправительственные организации в системе информационно-управленческого превосходства и современных манипулятивных технологий США

Одним из самых эффективных методов, успешно практикуемых США со второй половины XX века, является осуществление мер по завоеванию сознания опорных социальных групп, а не только территории государства – объекта управляемого воздействия.

Парадигма «сетецентричной войны» состоит в следующем. Вместо нескольких «птиц» или «акул» (в зависимости от среды боевых действий) со «сверх дальнозоркими» органами чувств, развитым интеллектом и большой физической силой, целесообразно иметь «рой насекомых» или «стаю пираний». Каждое из этих «насекомых» существенно уступает «птице» по любому из сенсорных и силовых параметров и в прямом сопоставлении ей безнадежно проигрывает. Однако противостоять хорошо организованному «рою» неизмеримо сложнее, чем «птице», хотя бы потому, что обнаружить отдельное «насекомое», а значит, и уничтожить его, гораздо труднее[357], [358].

По мнению военных экспертов, данный подход уже активно применялся американским банковским консорциумом[359] с использованием Генштаба Кайзеровской Германии против России при подготовке революции в 1917 году и Великобританией в ходе работы с басмачеством в Средней Азии. Такой же подход использовался СССР в деятельности Коминтерна, а затем в поддержке национально-освободительных движений Африки и Ближнего Востока.

В начале 90-х годов XX века Госдепартамент США, оценив итоги эффективно проведенных под эгидой Фонда «Наследие» долгосрочных программ, направленных против СССР и стран Организации Варшавского Договора (ОВД) в рамках доктрины «Освобождение» («Цели США в отношении России» – директива СНБ США №20/1, «Задачи США в отношении Восточной Европы» – директива СНБ США №58), разработал концепцию воздействия на неправительственные центры[360].

---

357 Ильин В. М. (профессор, действительный член Международной Академии «Информация, связь, управление в технике, природе, обществе») – Новейшие технологии XXI века в борьбе за души людей

358 Дугин А. – Сетецентричные войны. 08.02.2006 [http://wwwevrazia.org/modules. php? name=News &file=article&sid=2893

359 Курепина ... – Факторы ...

360 Димлевич Н. – Информационное противоборство в современном мире. Инфофорум, №45, ноябрь 2009, с. с. 49-51

В 1998 году в Объединенной доктрине информационных операций американскими экспертами было дано определение информационной войне как комплексному воздействию на систему государственного и военного управления противостоящей стороны. По их мнению, такое целенаправленное влияние на военно-политическое руководство противника в мирное время способно привести к принятию государственных решений, благоприятных для страны-инициатора, а в ходе военного конфликта полностью парализовать функционирование инфраструктуры управления противника.

В настоящее время заместитель госсекретаря и глава Координационного комитета стратегических коммуникаций и общественной дипломатии К. Хьюз предложила развернуть эффективную работу с так называемыми «группами влияния» и «уязвимыми группами населения». Госпожа Хьюз при этом скромно упустила работу по созданию и взаимодействию с «пятой колонной» как с частью «групп влияния», а именно она, а не «информационные мероприятия» способна парализовать и банковскую структуру и «функционирование инфраструктуры управления противника».

Согласно концепции Карен Хьюз, в «группы влияния» включены политики, общественные деятели, религиозные лидеры, крупные предприниматели, ведущие журналисты. К «уязвимым группам населения» отнесена молодёжь, женщины, национальные, религиозные и иные меньшинства. Инструментами в организации информационно-управленческого превосходства призваны стать сетевые структуры.

Концепция «сетецентричной (сетецентрической) войны» (далее СЦВ, в англоязычных источниках – Network Centric Warfare, NCW) изложена Игорем Анатольевичем Шереметом – начальником Информационно-аналитического управления Федеральной службы по оборонному заказу, доктором технических наук, профессором в «Независимом военном обозрении»[361] от 11.11.2005:

«Концепция «сетецентричной войны» представляет собой сложившуюся в последние 5-7 лет в США систему взглядов на военно-техническое обеспечение и ведение боевых действий в условиях тотальной компьютеризации сил и средств вооруженной борьбы.

4.4. ЭВЕРСИОННЫЕ МОББЕРНЫЕ ТЕХНОЛОГИИ

Флэш-моб как способ привлечь внимание окружающих, стал использоваться недавно, однако сразу же приобрел огромное количество сторонников и популяризаторов в самых разных уголках мира. Сейчас трудно найти такие сферы жизнедеятельности человека, где бы не применяли новейшие технологии умной

361 Опубликовано в Независимом военном обозрении от 11.11.2005. Оригинал: http://nvo.ng.ru/concepts/2005-11-11/4_computers. html

толпы, (технологии мгновенной толпы или толпы – вспышки). Спектр использования флэш-моба необычайно широк и разнообразен: от призыва к решению экологических проблем, акций политического протеста до привлечения покупателей в новый супермаркет. Во многих российских центрах флэш – моб из увлекательного направления молодежного времяпрепровождения стал основой субкультуры и превратился в серьезную социальную технологию.

В нашу задачу не входит выявление тенденций, присущих флэш-мобу в целом или описанию его классического применения, поэтому мы остановимся лишь на тех его проявлениях, которые используют технологи «цветных революций» для противостояния и свержения неугодного режима.

Сейчас в Мировой паутине не трудно обнаружить десятки и сотни фото, видео отчетов о флэш-мобах, которые изобилуют комментариями очевидцев или самих участников действа. Есть специализированные сайты, которые не просто описывают флэш-мобы, но и публикуют подробный инструктаж для новичков, желающих организовать «мгновенную акцию». В блогосфере и форумах последователей новых социальных технологий даже вывешиваются списки планируемых флэш-мобов и рекомендации для их потенциальных участников.

Специалисты и ученые передовых научных учреждений мира всерьез заняты изучением причинно – следственных связей и последствиями использования «толпы – вспышки». Технология «умной толпы» не могла не заинтересовать и военных, в частности, американских, которые разрабатывают способы и методы применения флэш-мобов в региональных вооруженных конфликтов. Для управления «мгновенной толпой» технологическими и IT – компаниями Запада и особенно Японии разрабатываются карманные микро устройства, работающие длительное время автономно. Высокую эффективность технологии «толпы – вспышки» в условиях растущего количества «цветных революций» подтверждает и число публикаций в средствах массовой информации и ссылки на материалы в Интернете.

Принято считать, что первый флэш-моб в своем классическом проявлении был проведен в 2003 г. в Нью-Йорке. В этом же году первая акция мобберов была осуществлена и в России. Изначально акции мобберов задумывались как неполитические, не рекламные, не преследующие какой-либо коммерческой выгоды. «Правильные мобберы» никогда не оповещают о своих акциях средства массовой информации, не создают неудобств людям, находящимся в непосредственной близости от проводимых акций, не нарушают привычный ритм городской жизни.

Идея технологии «умной толпы» заключается в использовании, якобы неорганизованной, массы людей, выполняющих заранее оговоренные и согласованные действия. Выглядит это так. Участники акции, незнакомы друг с другом лично, неожиданно собираются в общественном месте, выполняют

определенные действия и также неожиданно расходятся восвояси. Поскольку местом проведения флэш-мобов являются места большого скопления людей, то именно на ничего не ведающих сограждан, одновременные и нередко нелогичные, но выстраивающиеся в одну общую картину действия должны, по замыслу организаторов акции, оказать большое психологическое воздействие. Примеров тому множество. Группа людей в одинаковых одеждах, пришедших в одно время к назначенному месту, могут неожиданно, без обращений друг к другу и разговоров, устроить большую танцплощадку, исполняя им одним известный танец, а спустя несколько минут, также без слов, раствориться в толпе людей. Участники флэш – моба могут обратить на себя внимание окружающих, организовав очередь в торговом центре и с невозмутимым видом просить у продавца показать несуществующий или экзотический товар.

Популярность «умных толп» возрастает и будет возрастать с развитием цифровых технологий и беспроводных источников доступа в онлайн-сети. Все возрастающее распространение миникомпьютеров, нательных цифровых устройств, коммуникаторов только усиливает возможности для организации «умных толп». Доступ все более широких групп населения к технологиям, которые ранее имели возможность осваивать лишь специальные государственные службы и организации (таких, например, как технологии шифрования сигналов, криптографических устройств и технологий), может в дальнейшем привести к расширению возможностей и функций мобберных технологий, применение которых представляет значительную потенциальную опасность для правящих режимов. Следует предположить, что в скором времени появятся карманные устройства, которые сами будут координировать действия участников массовых акций и подсказывать конкретные действия. Подробнее об этом речь пойдет немного позже.

Современная массовая культура с ее карнавальным поверхностным характером сама по себе детерминирует появление новых форм манифестации и презентации. Сетевой характер современного общества также поощряет создание временных массовых скоплений людей. По словам американского социолога Говарда Рейнгольда, «умные толпы» помогают людям отстаивать свои позиции и не несут за собой никакой потенциальной опасности. Более того, мы полагаем, что флэш-моб, появившийся как исключительно молодежное увлечение, имеет множество положительных следствий. Так, например, он мог бы стать действенным средством пропаганды здорового образа жизни, социальной активности, привлечения внимания общества к актуальным социальным проблемам.

Но популярная социальная технология не могла остаться без использования в криминальных кругах. Многие флэш – мобы экстремистско настроенных лиц управляются посредством Всемирной паутины. Раскрытие таких пре-

ступлений очень сильно затруднено. Ведь нередко электронная почта и форумы участников регистрируются за пределами страны, а они сами зачастую не знают друг друга. Маркетологи для увеличения объемов торговли с помощью технологий «умной толпы» раскручивают продажи самой разнообразной продукции, включая продукты питания или оказание сервисных услуг. Технологии «толпы- вспышки» зачастую используются в протестных акциях, которые проводят антиглобалисты. Но более всего флэш-мобы используют как эффективное визуальное средство для решения политических задач, таких как очернение политических противников, дискредитация оппонентов, вплоть до снятия кандидатур с выборной гонки или нанесение непоправимого вреда имиджу оппонента. Эксперты – полит технологи считают, что технология «умной толпы» может являться одним из действенных и наглядных пропагандистских и агитационных средств, особенно в странах с контролируемыми СМИ или в условиях, когда информация в средствах массовой информации блокируется. Анализ показывает, что социальные технологии флэш-мобов с разной степенью эффективности использовались во многих странах, прошедших через этап «цветных революций» или там, где отмечены попытки их совершить. В тех странах, где антиправительственные или оппозиционные СМИ блокировались или были ограничены в подаче информации или распространении. Используя новейшие социальные технологии, в отличие от привычных форм массового протеста, организаторы добиваются высокой степени организованности, координации. А для успешного проведения подобных акций требуется выполнение нескольких условий – анонимность и мобильность участников. И, конечно же, наличие технических средств связи у каждого участника – будь то мобильный или сотовый телефон с выходом в Интернет.

Опыт использования силы «умных толп» имелся задолго до того, как череда «цветных революций» прокатилась по миру, накрыв собой страны с самыми разными видами правящего режима. Так, еще в 2001 г. сторонники оппозиции на Филиппинах свергли действующего президента страны, собрав на центральной площади с помощью смс-рассылки толпу численностью свыше одного миллиона человек, одетых в темные цвета. Часто встречающиеся сегодня технологии так называемого политического рейдерства самым активным образом используют флэш-моб при попытках захвата власти в отдельно взятом регионе или городе.

Одна из фундаментальных причин роста популярности флэш-мобов в условиях эверсионной борьбы заключается в том, что участники «умной толпы» могут не вызывать интереса правоохранительных органов на стадии ее формирования. Столкнувшись с проявлением каких-либо действий «умной толпы», органы правопорядка и действующего режима реагируют с запозданием или неадекватно на нетипичные поступки коллективного организма.

Действия мобберов трудно воспринимаемы и прогнозируемы их противниками. Ответственность за организацию эверсионного флэш-моба возложить, как правило, не на кого.

На стадии начала «цветной революции», когда еще не известен «масштаб трагедии» и возможные последствия для каждого отдельного участника протестных действий, флэш-моб является такой формой борьбы, в ходе которой личности нет необходимости брать на себя ответственность за совершаемые поступки. Психологические защитные механизмы гораздо сильнее работают в толпе и об этом всем давно и хорошо известно.

По мнению американского журналиста и аналитика Дж. Шуровьески, феномен децентрализации создает ощутимые преимущества участникам «умных толп», что имеет непосредственное отношение и к явлению флэш-моба. Так, Шуровьески утверждает, что если сформировать большую группу независимых друг от друга участников для решения какой-либо проблемы и заинтересовать их, вместо того, чтобы направлять усилия сверху, то совместное решение такой группы окажется более успешным. Этот принцип является основным при разработке мобберных технологий.

Следующей причиной популярности эверсионного флэш-моба является закономерность, которая ранее не просто не замечалась, но отсутствовала вовсе. Классики социальной психологии и социологии (Г. Лебон, Г. Тард, Х. Ортега-и-Гассет) убедительно доказывали в своих исследованиях, что толпа неуправляема, глупа по определению, не способна к рефлексии. Принцип организации эверсионного флэш-моба, его сущность и специфика функционирования создают принципиально иной тип толпы. Кроме принципов организации и коллективных действий, разумность массовому скоплению эверсионных мобберов придают социо-технические устройства, без которых невозможна организация флэш-моба.

В отличие от традиционных и привычных акций, митингов, шествий и демонстраций, в которых участвует большое количество людей и отличающихся слабой организованностью, участники эверсионных акций менее уязвимы. Нетрудно сорвать стихийный митинг или демонстрацию – технологии давно известны и хорошо отработаны. Есть те, которые получили название «мягких». С участниками флэш-моба все обстоит иначе. Мало того, что трудно обнаружить взаимосвязь между проводниками акции, невероятно трудно обнаружить организаторов и воздать виновным по заслугам. А то, что мобберы не знают друг друга в лицо, и, возможно, никогда, впоследствии, не узнают и не увидят друг друга вместе, делает возможность наказания ничто малой. Чаще всего во флэш-мобе участвует от нескольких десятков человек до нескольких сотен, что выгодно отличает эту акцию от многолюдной, в несколько тысяч человек, демонстрации, проходящей по центру

города. Мобильная группа участников флэш-моба будет более адекватной и готовой к различным сценариям внешнего противодействия. Так, при угрозе жизни многотысячная демонстрация поддается массовому психозу, приходит в состояние хаоса, впадает в панику и далее совершает неконтролируемые действия. Сотня – другая человек, участвующих в акции «умной толпы», при внешнем воздействии бесследно растворится в городской сутолоке. Более того, поскольку участники флэш-мобов должны в точности исполнять инструкции поведения при проведении акции, то и ущерб от вероятных столкновений с правоохранительными органами таких групп минимален.

У каждого отдельно взятого участника многотысячного митинга есть мотив, который заставляет индивида прийти в определенное место, вместе с десятками сотен таких же как и он, для демонстрации своего отношения к существующим порядкам, выражения протестных настроений либо иных действий. Пришедшие люди подчиняются законам, управляющим психологией толпы. Участники многотысячных акций, за редким исключением, не знают, как себя вести во время проведения акции, не организованы, не смогут, в случае возникновения конфликтов, к примеру, с правоохранительными органами, завершить протестные действия и выйти из них без потерь. Участники флэш- мобов хорошо осведомлены, как поступать в таких случаях.

Так чем же классический флэш-моб отличается от флэш-моба эверсионного? Во-первых, «традиционный» флэш-моб организовывается без привлечения внимания СМИ к своим акциям. Организаторы «цветных революций» не могут себе позволить такой роскоши. Всевозможные средства массовой информации заранее с помощью рассылки уведомляются о времени и месте проведении акции мобберов, указывается даже основной смысл и содержании предстоящего мероприятия. Более того, эверсоры могут даже «анонимно» поставить в известность сотрудников правоохранительных органов для того, чтобы СМИ впоследствии начали рассказывать о невиновных студентах и пожилых людях, укладываемых на асфальт бессердечным ОМОНом. Таким образом, заранее обеспечивается возможность классической провокации при проведении флэш-моба.

Во-вторых, флэш-моб предполагает добровольное участие в планируемых акциях, где все участники мероприятия выполняют одни и те же действия. При организации «умной толпы» в условиях «цветной революции», эверсоры могут сознательно ввести в заблуждение большинство людей, желающих принять участие в предстоящей акции. Например, в онлайн сетях и с помощью электронной рассылки может быть распространена информация о том, что на главной площади города будет проводиться флэш-моб, направленный в защиту экологии. Участникам необходимо собраться возле здания правительства (губернатора, мэра, президента и т. д.) в зеленых кеп-

ках и майках и громко прокричать пять раз «Я задыхаюсь», сделать соответствующее выражение лица и быстро разойтись. Казалось бы ничего противозаконного и криминального. Но в это же время небольшая группа людей, одетых так же, как и большинство участников акции, оказывается перед заранее оповещенными журналистами с плакатами «Нас душит правительство», «Пупкин – это грязь и коррупция» и т. д. В конечном итоге в СМИ появляются материалы о массовых акциях протеста против действующей власти. Сценарии подобных акций могут быть самими разнообразными.

В-третьих, традиционный флэш-моб не должен нарушать привычный ритм и уклад жизни горожан. Эверсоры в условиях разворачивающейся «цветной революции» могут устраивать акции, которые сознательно нарушают данное условие. Например, организовать многочасовое стояние на главной транспортной артерии города, лишая возможности людей добраться на работу и т. д.

В-четвертых, как уже было сказано, все акции «идейных» мобберов добровольны и уж тем более за участие в них не выплачиваются гонорары. В условиях относительно щедрого финансирования «цветных революций» любые массовые акции, в том числе и флэш-мобы, финансируются организаторами таких событий. Каждому участнику выплачивается разовое вознаграждение. Наиболее ярким примером таких событий является «оранжевая революция» на Украине. Ряд экспертов и журналистов, освещавших ее, в своих публикациях приводят факты, когда одни и те же люди, ради финансовой выгоды участвовали в массовых акциях каждой из противоборствующих сторон.

В-пятых, эверсионный политический флэш-моб предполагает значительно большее количество участников, чем традиционный. В случае, если в протестном флэш-мобе примут участие не более двух десятков человек, организаторы сочтут его неудачным, а общественный резонанс от такого мероприятия будет весьма незначительным.

В-шестых, так называемые «идейные» мобберы считают флэш- моб своеобразным социально активным интеллектуальным развлечением для городских жителей. Сам по себе флэш-моб не преследует никаких целей и не имеет смысла (разве что за исключением вызова реакции общества на нетипичные проявления каких-либо безобидных действий). Эверсионные мобберные технологии имеют ярко выраженную телеологическую направленность. Их основная цель совпадает с главной целью «цветной революции» – свержением правящего режима.

В-седьмых, время проведения классической мобберной акции, за исключением отдельных случаев, не превышает двадцати минут. Эверсионный флэш-моб может длиться часами в зависимости от целей предстоящей акции. Хотя, конечно, длительный флэш-моб в условиях революционных преоб-

разований – большая редкость. Он может быть осуществлен лишь в случае отсутствия внешнего давления на его участников.

Теперь остановимся непосредственно на процессе развертывания эверсионных толп с использованием мобберных технологий. Информация о готовящейся акции распространяется по эверсионным сетям с гораздо большей степенью конспиративности. Эверсионные технологи хорошо осведомлены о возможностях специальных служб в области фильтрации Интернет-трафика и телефонных переговоров. Поэтому инструкции о предстоящей акции распространяются по оффлайн сетям социальных связей или с помощью зашифрованных смс-сообщений, а также электронных писем. Под шифрованием в данном случае понимаются ничего не значащие выражения, например «Пьем пиво завтра в десять у зоопарка. Возьми с собой две бутылки». Под зоопарком могут пониматься любые административные здания, места большого скопления людей и т. д. Количество спиртного так же, как правило, подразумевает что-либо, необходимое для осуществления мобберной акции.

Обычно в инструкции, приходящий в виде электронного письма или sms-сообщения модераторы мобберных акций предупреждают, что организаторов у предстоящей акции нет, поэтому персональную ответственность будет нести каждый задержанный. Особенность флэш-моба заключается в том, что подобное массовое мероприятие не является формой несанкционированного властями протеста. Поэтому нет формального основания для привлечения к уголовной ответственности (это утверждение актуально только для некоторых постсоветских государств).

Эверсионные технологи заранее тщательно осматривают возможные места проведения акций, готовя возможные пути отхода. Для противостояния сотрудникам правоохранительных органов создается специальная группа, которая выполняет собственные функции во время акции. Так, например, внезапно «заглохший» автомобиль посреди улицы может на некоторое время задержать прибытие сотрудников милиции. В случае если правоохранительные органы заранее осведомлены о времени и месте проведения мобберной акции, на передний край могут выдвинуться пенсионеры, на которых вынуждены будут сконцентрироваться представители власти.

Организаторы эверсионных мобберных акций, проводящихся на начальной стадии «цветных революций», учитывают высокий уровень противодействия со стороны силовых структур. Чаще всего этим структурам заранее известен примерный сценарий предстоящей акции, время и место сбора его участников. Учитывая этот факт, организаторы акций все чаще прибегают к нетрадиционным способам сбора и передвижения участников. Так, например, в начале 2009 г. организация «Оборона» при проведении акции протеста в Санкт-Петербурге собирала своих сторонников под землей в метрополитене. Этот способ мог

позволить участникам перемещаться от станции к станции, скандируя при этом протестные лозунги и выйти на поверхность на любой станции.

Отдельные участники акции заняты фото- и видеосъемкой проходящего мероприятия. Как уже было сказано, в традиционном флэш-мобе категорически не приветствуется фиксация происходящего на любые записывающие устройства.

Одна мобберная акция может иметь несколько сценариев своего развития в зависимости от внешнего противодействия, количества пришедших участников и степени оказываемого воздействия на людей, оказавшихся свидетелями акции.

Условиями, определяющими успех эверсионного флэш-моба, являются:

наличие тщательно продуманного сценария действий во время акции и четких инструкций по поведению каждого отдельного участника;

абсолютная точность сбора участников акции. Для соблюдения этого условия обычно рекомендуется всем участникам заранее выставить точное время на часах и мобильных телефонах. При этом в большинстве случаев это требование полностью соблюсти невозможно;

внезапность сбора в заранее определенном месте;

слаженность и синхронность действий;

минимум общения между участниками акции;

наличие у каждого участника акции мобильного телефона. Как правило, организаторы подобных мобберных акций настоятельно советуют не пользоваться собственными sim- картами и мобильными телефонами;

Наличие у отдельных участников акции (на языке мобберов координаторы флэш-моба называются «маяками»)

карманных технических устройств идентификационного характера, беспроводных маршрутизаторов и т. д. Такие карманные устройства очень популярны у западной молодежи. Например, так называемый «брелок-сваха». Это устройство можно по заранее определенным параметрам настроить на поиск в большом скоплении людей своих сподвижников.

В зависимости от тактики, выбранной организаторами

эверсионной толпы, мероприятие может разворачиваться по двум сценариям.

Высокая интенсивность и низкая продолжительность

мероприятия с быстрым общим сбором и внезапным исчезновением участников эверсионного флэш-моба.

Размеренность и неторопливость акции (особенно с большим количеством участников), большая длительность и постепенное исчезновение толпы. Этот сценарий предполагает в большинстве случаев сознательный контакт с органами власти и охраны правопорядка.

При выборе места проведения эверсионной акции с применением мобберных технологий организаторы руководствуются следующими обстоятельствами:

доступность для участников акции места ее проведения;

наличие вблизи места проведения разветвленной уличной сети;

отсутствие вблизи места проведения акции органов охраны правопорядка;

отсутствие или минимальное количество вблизи места проведения акции объектов с камерами наружного наблюдения (если это условие соблюсти невозможно, то место сбора определяется на максимальной удаленности от таких объектов);

высокая интенсивность общественного транспорта в близи проведения акции;

большая проходимость людей в месте проведения акции.

Очевидно, что если мобберная эверсионная акция проходит в условиях активной фазы осуществления «цветной революции», в таком случае выбор места проведения акции определяется совсем другими обстоятельствами. Наиболее определяющим из этих обстоятельств является нахождение вблизи места проведения акции зданий и учреждений действующей власти. Это также могут быть и учреждения правоохранительных органов и служб безопасности государства.

Поведение участников эверсионной толпы во время проведения акции определяется внешними условиями и целями ее проведения. Анализ проведенных флэш-мобов в странах, где были осуществлены «цветные революции», позволяет предположить, что существует несколько общих рекомендаций для поведения участников мобберных акций.

Внутри толпы необходимо держаться как можно ближе друг к другу.

Оказывать сопротивление любыми способами при попытке
сотрудников правоохранительных органов вытащить
участника акции из толпы.

Каждому участнику наметить для себя путь отхода от места проведения акции после ее завершения.

Не смотреть постоянно по сторонам. Взгляд участника должен быть обращен внутрь толпы.

В случае силового разгона эверсионной мобберной толпы дистанция между участниками должна быть увеличена.

Не разговаривать с другими участниками акции.

При любых попытках сорвать эверсионный флэш-моб необходимо пытаться до конца соблюсти сценарий мероприятия.

Не позировать перед журналистами.

Каждый участник акции должен иметь включенный мобильный телефон для получения дополнительных команд с помощью смс-сообщений.

При выходе с места проведения акции пользоваться по возможности наиболее интенсивными транспортными артериями и пытаться раствориться в городской толпе.

Как и любой другой вид технологий, флэш-моб имеет ряд условий, при наличии которых его осуществление в эверсионном варианте невозможно либо весьма затруднительно.

Численность постоянно проживающего населения в населенном пункте, где проводится эверсионная мобберная акция, не превышает ста тысяч (иначе участники акции и те, кто им противостоит, будут знать друг друга, по меньшей мере, в лицо или их будет впоследствии легко вычислить).

В населенном пункте отсутствует либо полностью блокирована мобильная связь.

Отсутствует доступ в сеть Интернет.

Поведение эверсионных мобильных толп в странах, где были предприняты попытки «цветных революций», со всей очевидностью показывает, что основной движущей силой, идущей на сознательное противостояние с силовыми структурами действующей власти, была молодежь. Для того, чтобы подобные людские образования выделялись на общем фоне, участники акций были одеты в яркую одежду одинаковых тонов, что противоречит одному из условий неполитического флэш-моба – до начала акции ничем не выделяться из общей массы.

Сам характер флэш-моба, в том числе эверсионного предполагает высокую степень мобильности участников, а также способность противостоять силовому давлению. Молодежь как никакая другая возрастная группа удовлетворяет этим условиям. Сложные технологические устройства, используемые при организации и управлении эверсионной толпой, молодые люди осваивают быстрее всех. Мобильные текстовые сообщения, являющие обязательной составляющей эверсионного флэш-моба, также активнее всех применяет в общении между собой именно молодое поколение пользователей мобильных телефонов.

Важной составляющей эверсионной мобберной акции является, как уже было сказано выше, создание самим фактом ее осуществления информационного повода для средств массовой информации. Поскольку заблаговременное оповещение СМИ о готовящемся мероприятии повлечет за собой известность и в «соответствующих структурах», организаторы эверсионных толп готовят собственное информационное сопровождение. Отдельные участники флэш-моба выполняют функции журналистов, освещающих данное мероприятие. Собственные операторы получают инструкции о том, как создать

такой видеоматериал, который будет демонстрировать масштабность акции, но при этом отдельные лица участников будут трудноразличимы. После завершения акции материалы проходят цензуру эверсоров и рассылаются в СМИ. Если медийное пространство полностью контролируется противниками революции, ролик (или множество роликов) размещаются в глобальной сети на сайтах сторонников революции, в том числе за рубежом.

После завершения активной фазы мобберной акции всем участникам, как правило, рекомендуется некоторое время оставаться дома и не участвовать в активной общественной жизни. Другие формы, присущие традиционному флэш-мобу, такие как афтерпати (вечеринка после проведенного флэш-моба) также не предусматриваются эверсионными мобберными акциями.

На начальной стадии раскрутки «цветной революции», когда существует высокая вероятность отслеживания активности противников действующего режима, особое внимание эверсионные технологи уделяют сценарияхм мобберных акций. Их контент должен явно выдавать наблюдателям акции ее основной смысл, обладать провокационностью по отношению к действующей власти. В то же время в действиях мобберов пока не должно прослеживаться явных призывов к свержению существующего режима.

Сценарии мобберных акций во время активной фазы цветной революции определяются выработанной заранее стратегией и тактикой действий, а также текущим развитием ситуации.

Если рассуждать о будущем мобберных технологий и тех вариантах, в которые может трансформироваться флэш-моб в его классическом представлении, то здесь, как нам представляется, существует бесконечное множество вариантов, о которых необходимо думать уже сейчас.

Разновидностью мобберных технологий, так называемым sms- моб (управлением толпой только с помощью мобильных телефонов), уже сейчас активно пользуются разнородные политические силы во многих странах мира. В странах Запада (в основном в США) выявлению особенностей социального поведения и управления им с помощью мобильных технологий заняты целые исследовательские коллективы. М. Каневский заметил в связи с этим, что, как и в случае с flash-мобом, подобные действия реализуются в чьих-то интересах.

Анализируя скорость и периодичность, с которой появляются новейшие технологические коммуникационные разработки, завоевание ими популярности среди населения стран с самым разным социальным и экономическим уровнем развития, а также степень внедрения операторов сотовой и мобильной связи в повседневную жизнь граждан, можно смело утверждать, что технологии управления эверсионными толпами, основанные на использовании мобильной связи, будут иметь все большую актуальность.

4.4.1. Возможности форумов для обеспечения эверсионной деятельности

Веб-форум (или Интернет-форум) представляет собой площадку для общения пользователей определенных сайтов на основе специального программного обеспечения.

Функционирование форумов осуществляется в форме создания пользователями отдельных тем в различных разделах и дальнейшего обсуждения самих этих тем.

На разных форумах применяются различные формы доступа к сообщениям. Так, чтение и создание новых сообщений могут быть вполне доступны случайным посетителям; для доступа к другим необходима предварительная регистрация. Последнее является наиболее распространенным случаем. Могут использоваться и комбинированные варианты, «когда отдельные темы могут быть доступны всем посетителям, а другие – только зарегистрированным участникам. В Интернете существуют также закрытые форумы, доступ к которым определяется персонально для каждого участника администраторами форума. На практике также нередко встречается вариант, когда некоторые разделы форума общедоступны, а остальная часть доступна только узкому кругу участников». [362]

Для большинства форумов доступна система личных сообщений, позволяющая зарегистрированным пользователям общаться индивидуально. На ряде форумов при создании новой темы существует возможность голосования по ней. При этом другие участники или незарегистрированные посетители форума также имеют возможность голосовать, не создавая нового сообщения в теме форума. Форумы обычно обладают возможностью тематического поиска сообщений, оставленных отдельным пользователем.

Форумы подразделяются на следующие основные группы:

профессиональные форумы, где собираются специалисты различных областей знания и обсуждают общие для себя проблемы и темы;

форумы по интересам, например, спортивные, культурные, научные, а также форумы домохозяек, любителей дикой природы и т. д.;

общие форумы – чаще всего это большие городские форумы, где собираются различные люди, и обсуждается широкий круг вопросов, очень часто не связанных с жизнью конкретного города.

Как метко заметили Е. Юшук и А. Кузин, Интернет-форум – это своего рода клуб по интересам. Форумы, подобно блогам, позволяют организо-

---

362 С. С. Internet. История развития и принципы работы, протоколы передачи данных, система адресации. Сервисы Internet: электронная почта, форум, ICQ, файловая передача, среда World Wide Web, среда поиска информации. CoolReferat.com)

вать общение между людьми. Основное же отличие блога от форума состоит в том, что форум – это площадка для коллективного обсуждения. Именно этим форумы особенно ценны для организаторов и технологов «цветных революций».

Говоря об использовании Интернет-форумов технологами «цветных революций», необходимо классифицировать работу с аудиторией на этих площадках, которая проводится на различных стадиях осуществления «цветного» переворота.

На стадии подготовки к «цветной революции», когда создаются «независимые» информационные ресурсы, «Интернет-СМИ и других площадок такого рода, на них предусматривается возможность создания форума, где наряду с обсуждением обыденных новостей иногда осуществляется вброс необходимой эверсорам информации. Это делается для того, чтобы отследить реакцию на эту информацию, а также постепенно готовить аудиторию к будущим событиям.

На общих форумах, где собирается самая большая аудитория (до нескольких сотен тысяч человек) на стадии подготовки к цветной революции происходит внедрение своих пользователей, которые, ничем не выделяясь, зарабатывают рейтинговые очки (иногда это называется «карма»), говорящие об авторитете данного пользователя Зарабатывается авторитет количеством постов (размещенных сообщений), количеством приглашенных на данный форум других пользователей, а также качеством положительных откликов на посты конкретного пользователя. Осуществляется эта подготовительная работа для того, чтобы в период развертывания активной фазы революционных действий не распространять неоднозначную информацию как недавно зарегистрированный пользователь (новичок), поскольку это может навлечь вполне понятный гнев опытных пользователей (гуру, мегапостер, ветеран и т. д.), которые хотят остаться в стороне от политических событий и не желают засорять данный форум политически ангажированной информацией.»[363] Это делается потому, что обычно, как только опытный пользователь видит появление подобной информации или попытку вызвать дискуссию на интересующую эверсоров тему, он сразу же обращает внимание модератора раздела (или темы) на конкретного постера и тема, скорее всего, удаляется, а на ее автора накладывается бан (запрет на пользование Интернет-ресурсом).

Если на этапе подготовки к активным действиям в сети стороннику «цветной революции» удается стать модератором или администратором большого форума, это может считаться значительным достижением в сетевой войне. В таком случае раздел, который будет модерировать данный поль-

363 Кубякин Е. О Информационный экстремизм как феномен социокоммуникативной реальности XX1 в. – научный журнал «Гуманитарные, социально – экономические и общественные науки». В.№ 1-2011 г.

зователь, используется в целях сетевой войны наиболее активно. Когда его истинные цели раскрыты администрацией форума и его забанивают, особого эффекта это, как правило, не достигает, поскольку основные события разворачиваются уже не в сети, а в реальной жизни.

Тематическая составляющая постов на подготовительном этапе, выкладываемых на общих форумах достаточно разнообразна. Часто это риторические вопросы о том, как долго будет продолжаться несправедливость в той или ной сферах жизни общества. Иногда это публикации о злоупотреблениях и деяниях действующей власти, правоохранительных органов. Также встречаются и заведомо провокационные сообщения от постеров, обладающих якобы инсайдерской информацией, о готовящихся разительных переменах, которые затронут комфорт и качество жизни большинства населения. Иногда эти посты комментируют другие пользователи в русле, которое необходимо заговорщикам. Часто специально обученные постеры просят назвать источник информации или уточнить, что конкретно имел в виду автор сообщений. Таким образом, появляется возможность указать на некое авторитетное лицо, организацию, которые не равнодушны к происходящим событиям и ведут организованное сопротивление, а также на то, что в скором времени об этих лицах будут знать все и т. д.

При подготовке к «цветной революции» профессиональные форумы и форумы по интересам также представляют вполне определенный интерес для эверсоров. На них вербовщики ищут тех, кто может быть неравнодушен к революционным идеям. Работа на них ведется еще более осторожно, чем на общих форумах, поскольку здесь собираются люди чаще всего равнодушные к политической жизни. Иногда на таких форумах общается большое количество людей, знающих друг друга достаточно давно. Причем иногда они знакомы и в реальной жизни. Поэтому внедрение в такие сообщества происходит достаточно медленно. Больше всего потенциальных революционеров интересуют действующие и нынешние сотрудники правоохранительных органов, военнослужащие, журналисты, сторонники радикальных молодежных движений, студенты.

«Использование Интернет-форумов на стадии подготовки «цветной революции» обусловлено следующими целями:

поиск потенциальных сторонников осуществления «цветной революции»;

внедрение в сообщество Интернет-форумов пользователей, нацеленных на распространение необходимой эверсорам информации;

создание в сообществе форумов атмосферы недовольства отдельными действиями правящего режима или его представителями;

распространение информации, носящей инсайдерский характер о злоупотреблениях действующей власти или ее конкретных представителей». [364]

На стадии развертывания революционных событий на общих форумах наступает период активной работы. Здесь начинают комментироваться темы, созданные кем-либо задолго до этих событий и только сейчас приобретающие свою актуальность. Вновь зарегистрированные пользователи начинают активно общаться в рамках этих тем, а также создавать новые. Причем, например, на общегородских форумах все эти действия происходят не в разделах, связанных с политикой, поскольку они традиционно являются наименее посещаемыми. Чаще всего это темы связаны с безопасностью, коррупцией, развлечениями – то есть с разделами, где количество сообщений и соответственно посещений самое большое.

Содержание и технологическая подготовка таких постов заранее обсуждается на тренингах и семинарах, которые проходят активисты сетевой войны. Здесь мы не будем их обсуждать. Стоит отдельно остановиться лишь на том, что как на подготовительной стадии, так и на стадии развертывания «цветной революции» при работе на форумах бойцы сетевой войны стараются не пользоваться так называемыми спам-ботами – специальными программами для массового распространения информации и гиперссылок. Это делается для того, чтобы создать видимость живой дискуссии и массового обсуждения проблемы. К тому же, у многих форумов имеется достаточно неплохая защита против массового спама, распространяемого на их территории. Рассылки массового характера, с использованием программ для спама применяются на более поздних стадиях осуществления «цветных революций».

В тот момент, когда осуществление «цветной революции» уже сопровождается активными действиями в реальном мире, роль форумов не просто не снижается, а увеличивается. В это время на площадках форумов начинается активное обсуждение происходящих в реальном мире событий. В этот момент посты, распространяемые на форумах, создаются по всем канонам продвинутой рекламы и партизанского маркетинга. Здесь присутствуют и отсылки к авторитетным источникам, мнение которых однако большинство проверить не сможет, и к фото- и видеодоказательствам происходящего и многое другое.

«Действия, происходящие на форумах, на активных стадиях осуществления « [цветной революции» приносят наиболее ощутимый эффект в тех случаях, когда власть пытается ограничить доступ населения к реальной инфор-

364 Кубякин Е. О Информационный экстремизм как феномен социокоммуникативной реальности XXI в. – научный журнал «Гуманитарные, социально – экономические и общественные науки». В.№ 1-2011 г.

мации о происходящих событиях. Если деятельность Интернет-форумов не заблокирована (а блокируется она только тогда, когда форумы становятся самым популярным источником получения информации), они начинают вполне успешно играть роль «народных» средств массовой информации». [365]

4.4.2. Эверсионные технологии мобильной связи

Для России 2004 г. стал годом начала эксперимента по электронному голосованию. На последних региональных выборах (1 марта 2009 г.) в пяти регионах России был продолжен этот эксперимент, признанный весьма успешным. В странах Запада также активно проходят исследовательские опыты, связанные с электронными выборами.

Мобильный телефон и связанные с ним дополнительные возможности коммуникации эверсоры могут использовать не только при проведении различного рода эверсионных флэш-мобов. На стадии активного развертывания «цветной революции» возможности мобильных сетей связей могут быть самым активным образом использованы противниками действующего режима. Особенно этот тезис является актуальным в условиях тотального контроля действующей власти за средствами массовой информации.

Мобильные эверсионные действия относятся к конкретным технологиям, реализуемым в условиях «цветных революций». Многие из них могут задействоваться эверсорами как отдельно, так и в комплексе с другими технологиями. Более того, во многих случаях одни технологии неприменимы без использования других (например, флэш-моб невозможно организовать и управлять без мобильных телефонных технологий).

Массовая sms-рассылка

Во время осуществления украинской «цветной революции» использование массовой sms-рассылки различного рода сообщений активно использовалось предвыборным штабом В. Ющенко. Мобилизация населения в условиях киргизской «тюльпановой» революции и информирование местного населения об Андижанских событий в Узбекистане активно осуществлялись с помощью массовых sms-рассылок. Филиппинские события 2001 г. начались с того, что более 1 миллиона населения собралось на центральной площади столицы, узнав о предстоящей акции с помощью полученного sms-сообщения.

---

365 Кубякин Е. О Информационный экстремизм как феномен социокоммуникативной реальности XX1 в. – научный журнал «Гуманитарные, социально – экономические и общественные науки». В.№ 1-2011 г.

В последние годы в выборных кампаниях различного уровня все чаще используются технологии мобильной связи для агитации и пропаганды за отдельных политиков или политические партии. Нередки случаи использования sms-рассылки с целью дискредитации акторов политической борьбы.

Возрастающий интерес политтехнологов и эверсоров к технологиям мобильной связи, а также уровень распространения мобильной связи среди населения обуславливает интерес к данной технологии, которую можно использовать в самых широких целях.

Технологически процесс массовой рассылки sms-сообщений осуществить достаточно просто. Для этого существует целый ряд компьютерных программ, которые возможно найти в сети Интернет, такие, например, как Universe-sms, SMS Messenger и т. д. Обычно технологи, специализирующиеся на мобильном спаме, заранее определяются с тактикой предстоящих действий. Обеспечение массовой рассылки разного рода sms-сообщений возможно через сеть Интернет. Правда в этом случае существует вероятность того, что рассылка будет заблокирована оператором. Более надежный способ заключается в создании так называемых мобильных бригад, которые будут заниматься рассылкой текстовых сообщений со своего телефона, что значительно уменьшает скорость рассылки, увеличивая ее надежность.

Процесс рекрутинга агентов мобильного спама не требует особых усилий за исключением некоторого интсруктажа, особенности которого зависят от целей и задач планируемого мероприятия. Технически необходимо, чтобы телефоны мобильных спамеров были оснащены как можно большим количеством выполняемых функций, включая Bluetooth и ее аналоги. Более надежным и быстрым инструментом рассылки sms-сообщений является коммуникатор.

В тех условиях, когда политический режим позволяет существование легальной оппозиции, включая возможности ее сотрудничества с бизнес-структурами, гораздо проще договориться с оператором мобильной связи о предоставлении специальных номеров. Этот способ активно применялся сторонниками В. Ющенко во время украинской революции.

Говоря о контенте сообщений, рассылаемых с помощью технологий мобильного спама, необходимо отметить, что эверсоры стараются разрабатывать короткие, лаконичные и эмоционально насыщенные тексты. Если текст сообщения получатель не может получить сразу, без его обновления, эффективность воздействия значительно снижается.

Формат sms-спама также может быть весьма разнообразным: от перепечаток выдержек новостей с информационных сайтов, до тиражирования

статистики преступлений, совершенных за последнее время представителями власти и цитат лидеров оппозиции.

Эффективность технологии sms-спама зависит многих факторов, таких как уровень проникновения мобильной связи, материальное положение населения, информационная политика режима, степень свободы и открытости общества и т. д. Наиболее сильный эффект рассылаемые таким образом сообщения могут оказать в случае масштабной информационной блокады, когда население не имеет доступа к информации о происходящих событиях.

В среде экспертов, специализирующихся на «цветных революциях», довольно распространено мнение о том, что власть, в отличие от оппозиции, медленно и невнятно реагирует на имеющиеся раздражители, стремится ограничить доступ к объективной информации, достаточно часто открыто дезинформирует население о происходящих событиях и реакции на них. В таких условиях масштабный охват населения мобильной пропагандой может стать и источником дефицитной информации, и катализатором конкретных действий.

Вариаций технологического использования технологий мобильной связи достаточно много, и они продолжают возрастать. Так, sms-exit-polls, точнее его имитация, часто применяется в последнее время на выборах различного уровня. Особенно эффектным считается «информирование» о результатах опросов на выходе из участков членов избирательных штабов противника.

Мобильный спам также используется и как средство массовой дезинформации. Информация, которую невозможно оперативно проверить, вбрасывается с помощью sms-сообщений с самыми различными целями. В последнее время возрастает использование sms-технологий от имени противника для дискредитации или каких- либо других целей.

С помощью технологии Multimedia Messaging Service (MMS) стало возможным информирование о происходящих акциях с помощью передачи визуального изображения, включая их звуковое сопровождение. Технология MMS значительно увеличила возможности эверсоров в создании революционной ситуации и акцентуации ее эмоционального фона.

Видеоконтент, полученный при помощи MMS, отправляется на многочисленные видеопорталы, предоставляющие услуги хранения, размещения и показа различных видеосюжетов (Youtube, RuTube.ru).

Размещение различного рода видеосюжетов, снятых «случайными» свидетелями каких-либо событий с помощью мобильных телефонов и связанных с попытками захвата власти или влияния на нее, очень часто становится весьма популярным в Интернет-среде.

Организаторы «цветных революций» часто могут прямо поощрять и советовать снимать все события, свидетельствующие о тех или иных нарушениях действующего режима и попросту то, что может казаться человеку интересным и размещать это как на общеизвестных видеопорталах, так и на собственных ресурсах сторонников «цветных революций».

Вообще мобильный телефон становится одним из главных инструментов различного рода несогласных в борьбе с действующими политическими режимами. Его использование можно свести к следующим основным функциям:

координация и управление протестными массами;

информирование бригадиров протестующих о перемещениях и действиях правоохранительных органов;

координация и управление флэш-мобами (даже при блокировании самой мобильной связи);

получение и отправка информации в сервисы микроблогов (Twitter);

организация и управления различными мобильными акциями;

производство и распространение мобильного контента (от политической рекламы до вирусного видео).

Конечно, на этапе подготовки «цветной революции» учитываются уровень доходов населения, который оказывает прямое влияние на проникновение мобильной связи, ее качество, количество мобильных телефонов в семье (их уровень) и т. д. Так, например, в Киргизии далеко не у всех пользователей качество мобильных телефонов позволяло принимать или отправлять MMS, снимать на телефон видеоролики и т. д.

Современные мобильные телефоны позволяют не только осуществлять доступ в сеть Интернет, но и пользоваться программным обеспечением Windows, Java и др. Эти возможности в дальнейшем будут в полной мере использованы для производства разнообразного высокотехнологичного контента, который может быть использован в том числе и в попытках осуществления «цветных революций».

Вирусное видео

Производство и размещение вирусных видеороликов довольно давно считается эффективным маркетинговым и рекламным приемом. Вирусное видео являются одним из приемов вирусного маркетинга, который представляет собой систему трансляции различных сообщений, содержащих необходимую распространителям информацию. Одной из важнейших отличительных черт стратегии вирусного маркетинга является добровольное распространение информации. Форм продвижения вирусного маркетинга достаточного много. Сами популярными из них являются видеоролики, фото, флэш-анимация и т. д.

Сам термин вирусный маркетинг появился в США в 1996 г. Самым распространенным каналом передачи вирусного видео является Интернет. Сегодня в Интернете функционирует множество креативных рекламных агентств, специализирующихся на производстве и посеве (распространении) вирусного видео. Все большему распространению вирусного маркетинга способствует увеличивающаяся скорость доступа к различным интернет-каналам и социальным сетям, а также спектр предоставляемых услуг в этой области.

По оценкам абсолютного большинства экспертов и политтехнологов, в странах, где «цветные революции» имели успех, их организаторами создавалась иллюзия альтернативной реальности, в том числе с помощью методов вирусного маркетинга. Ярким примером использования технологий вирусного маркетинга в условиях «цветных революций» в оффлайне, явилась массовая «оранжевая истерия» во время украинских событий. Например, водители в маршрутных такси Киева осуществляли бесплатный проезд в день голосования тех пассажиров, на которых были оранжевые ленточки.

Все же более эффективной техникой вирусных технологий, особенно в условиях отсутствия доступа к официальным СМИ, является производство, посев и потребление вирусного видео. Анализ технологических и креативных аспектов производства политического вирусного видео не входит в задачи данного издания. Мы здесь остановимся лишь на функциях его использования в условиях «цветных революций».

Создание сильного эмоционального фона, который должен сопровождать революционные события.

Вызов ярких эмоциональных реакций на действия сторонников и /или противников «цветной революции».

Рекрутирование дополнительного числа сторонников осуществления «цветной революции».

Информирование о предстоящих акциях и мероприятиях.

Одним из преимуществ использования вирусного видео в «цветных революциях» является доступность проверки его эффективности, которую можно легко отследить с помощью количества просмотров, числа ссылок и т.д. Еще одной особенностью вирусного видео является относительная простота его производства и размещения, которая сегодня доступна любому пользователю персонального компьютера и сети Интернет.

Среди наиболее распространенных способов посева вирусного видео можно выделить следующие основные:

пересылка файла с видеороликом (если он небольшого размера) по электронной почте.

размещение ссылок на видеоролик на различных сайтах, блогах и форумах;

размещение информации о видеоролике и его характере в Twitter.

размещение видеороликов на известных и популярных файлообменниках;

размещение файла с видеороликом на наиболее известных и посещаемых видеопорталах;

распространение информации о видеоролике с помощью SMS и MMS.

В условиях развертывания революционной ситуации вирусное видео способно достаточно эффективно заменить телевидение, доступ к которому в силу очевидных причин для большинства оппозиционеров существенно ограничен.

Эверсионные технологии распространения и управления слухами

В каждом обществе обязательной составляющей межличностных неофициальных взаимоотношений будут являться слухи или неподтвержденная информация. Хождению и распространению слухов способствует множество прямых и косвенных условий, исследованных и проанализированных в научных изданиях по психологии, социологии и политологии. Слухам придается особый смысл, и они переходят на качественно новый уровень, когда население не доверяет государственным средствам массовой информации. Чем меньше в обществе и государстве возможностей законных способов обмена информацией, тем больше развиваются слухи, с помощью которых пытаются дать оценку текущим событиям и возможным их изменениям.

Чем большее значение в обществе играют личные и родственные связи, тем больше в таком обществе доверяют слухам. Благодатной средой для распространения слухов и непроверенной информации являются социальные сети. Даже в тех случаях, когда в средствах массовой информации дается только официальная или очень дозированная информация, подвергаемая жесточайшей цензуре, когда блокируются сотовая и мобильная связь и доступ к Всемирной паутине, слухи остаются необычайно эффективным и действенным оружием.

Примеров тому множество. Слухи стали определяющими в информировании населения и в Республике Узбекистан, где в ходе антиправительственных выступлений в Андижане, пытались реализовать сценарий «цветной революции», и в Кыргызстане, где «тюльпановая революция» состоялась. В обоих государствах хождение слухов и информация, которую они несли, по своим масштабам не шли ни в какое сравнение с новостными сообщениями официальных СМИ.

Ряд ученых, в частности, Дж. Масионис, выделяют следующие характерные особенности слухов.

Они процветают в атмосфере неопределенности. Слухи возникают тогда, когда люди не обладают точной информацией по важному вопросу. Например, отсутствие знаний о терроризме и угрозе заражения сибирской язвой при вскрытии писем привело к волне страхов после событий 11 сентября 2001 г. в США.

Слухи нестабильны. Передавая их, люди изменяют информацию обычно выгодным для себя способом. В результате появляется множество различных вариантов слуха.

Слухи трудно остановить. Число людей, которым стал известен тот или иной слух, возрастает экспонентным образом, поскольку каждый сообщает информацию нескольким своим знакомым. Со временем слухи угасают, однако единственный способ контролировать их – предоставлять ясную и убедительную фактическую информацию для заслуживающих доверия источников.

Утверждение о том, что существует только единственный способ контролировать слухи – спорно. Есть множество возможностей противостоять слухам или направить их в нужное русло и эти возможности известны современным политтехнологам. В современной социологии и ряде смежных наук налицо множество различных классификаций слухов. Они подчеркивают, выделяют те или иные стороны, элементы функционирования слухов. Такое значительное число разновидностей слухов может свидетельствовать как о распространенности данного явления в современном обществе, так и о недостаточно эффективном терминологическом аппарате, имеющемся в распоряжении у исследователей. Однако в задачу данного издания не входит теоретический анализ типологии слухов, а также механизмов их функционирования. В этой связи стоит отметить, что по данным многочисленных исследований, а также по данным исследований авторов настоящего издания, наиболее сильное эмоциональное воздействие на человека и, соответственно, на распространение слухов оказывают ситуации, угрожающие здоровью, безопасности или физическому существованию человека. Если на фоне данной ситуации у человека отсутствует достоверная и проверенная информация об ее характере, масштабе и потенциальных последствиях, эмоциональная насыщенность и важность слуха резко возрастает. Так, например, слухи о том, что после подавления волнений во время андижанских событий, последуют новые события, заставили значительное число людей сняться со своих мест и перебраться на юг Киргизии.

Исходя из технологических особенностей распространения слухов, важное значение имеет деятельность ЛОМов (или лидеров общественного мнения) и их личностные особенности. Чем с большими людьми взаимодейству-

ют ЛОМы, чем более неоднозначной является их позиция по актуальным общественным вопросам, тем больше внимания обращено к ним со стороны сообщества.

Для данного издания особую значимость имеют искусственно созданные, а не спонтанно возникшие слухи. В этой связи важно отметить, что для достижения желаемого эффекта перед кампанией по запуску слухов проводятся серии социологических замеров с помощью четырех основных методов: контент-анализа публикаций в СМИ, эксперимента, опросов, а также фокус-групп. В зависимости от целей распространения слухов и возможностей заказчиков используются как все перечисленные методы, так и некоторые из них. Задачей этих исследований является выявление лидеров мнений, типичных доноров и реципиентов слухов в данной среде, типичных коммуникационных стратегий населения и т. д.

Среди основных коммуникационных особенностей, делающих слухи важным средством передачи информации, можно выделить следующие:

Слухи, которые зачастую содержат информацию, трансляция которой официальными каналами коммуникации представляется нежелательной;

слухи, которые в концентрированном виде содержат информацию, проявляющихся в коллективных бессознательных ожиданиях отдельных личностей, социальных групп и общностей. Слухи заставляют перенести эти ожидания в сферу осознаваемого;

слухи, которые являются выражением коллективных притязаний, а не индивидуальных желаний.

В условиях «цветных революций» слухи активно используют на всех стадиях революционной борьбы. Но все же наиболее заметный эффект они приносят на стадии развертывания активных мероприятий. Именно в этот момент, когда значительная часть населения тем или иным образом задействована в революционном процессе, умело запущенные слухи становятся катализатором еще более активных событий.

На стадии подготовки к «цветной революции», слухи обычно не используют, чтобы не вызвать нежелательного интереса со стороны власти и правоохранительных органов. На стадии развертывания революционных масс начинается достаточно активное применение данной технологии. Это же относится и к основным стадиям «цветной революции».

Основными каналами распространения слухов в условиях цветных революция являются:

агенты влияния (в транспорте, местах массового скопления людей, очередях и т. д.);

официальные СМИ;

каналы виртуальной коммуникации (блоги, форумы, сайты и т. д.);

каналы мобильной коммуникации (мобильная связь, SMS, MMS и т. д.);
лидеры общественного мнения;
ближний круг общения (друзья и знакомые).

Специально подготовленные в рамках учебных тренингов и семинаров (задолго до основной фазы революционных мероприятий), «разносчики» слухов являются хоть и действенным, но достаточно дорогим способом распространения слухов. К тому же их деятельность обычно контролируется с помощью специальных групп, которые организаторы и вдохновители революций также вынуждены содержать.

Вместе с тем, именно деятельность таких специально подготовленных команд разносчиков слухов является наиболее эффективной в условиях массовых мероприятий. Часто политтехнологи и руководители подобных бригад отправляют их на массовые мероприятия противников для того, чтобы внести разлад в стройные ряды сторонников действующей власти. Иногда это бывает достаточно эффективным, особенно в случае, когда «массовку» согнали при помощи административного ресурса и, кроме сожаления о потерянном времени, эти люди ничего более не испытывают. На таких участников массовых мероприятий действия распространителей слухов оказывают наиболее сильный эффект.

Официальные СМИ являются достаточно труднодоступным каналом трансляции слухов. Особенно это характерно для начальных стадий их распространения, когда непроверенная информация еще не затронула широкие массы населения. Наиболее вероятно попадание слуха в официальные СМИ в том случае, когда информация, которую он передает, затронула широкие массы и власти вынуждены подключать официальные каналы коммуникации для опровержения этих сообщений.

Каналы виртуальной (или сетевой) коммуникации являются весьма эффективным способом распространения слухов. В этой ситуации специалисты, занимающиеся слухами, внимательно следят за тем, чтобы в процессе посева фрейм (основное содержание) слуха не изменился.

Каналы мобильной коммуникации наилучшим образом подходят для передачи аудиальных слухов. На начальных этапах распространения нужной информации этим занимаются специальные команды. В дальнейшем правильно построенный слух должен начать самостоятельное путешествие по каналам коммуникации.

Лидеры общественного мнения являются наиболее «авторитетным» источником трансляции слухов. Однако их всегда ограниченное количество, поэтому организаторы эверсионных мероприятий для ЛОМов оставляют всегда самые «тяжелые» слухи, которые не будут адекватно восприняты от других переносчиков информации.

Многочисленные исследования показывают, что именно ближний круг общения является наиболее восприимчивым к целенаправленному или случайному воздействию слухов. Этим пользуются не только технологи «цветных революций», но и специалисты по связям с общественностью на обычных выборах любого уровня.

Организаторы и технологи «цветных революций» хорошо понимают, что, когда на населения сваливается значительный объем информации, в том числе и засоряющей информационнокоммуникационное пространство, переизбыток слухов может привести к обратной реакции на их усилия. Поэтому объем, каналы передачи и смысловое содержание слухов меняется исходя из динамики развития революционной ситуации.

Эверсионные директ-технологии

Смысл и содержание директивных технологий в «цветных революциях» был заимствован из директивного маркетинга, цель которого заключается в максимизации процента положительных откликов клиентов на воздействия, основанные на прямой коммуникации.

К эверсионным директивным технологиям относятся мероприятия, осуществляемые в рамках подготовки и реализации «цветных революций», направленные на увеличение возможности влияния на население с целью его вовлечения в ряды сторонников революционных перемен. К таким мероприятиям относятся, прежде всего:

бесплатное участие в образовательных, информационных и развлекательных мероприятиях, осуществляемых

организаторами «цветных революций»;

предоставление информационной, консультативной, технологической, финансовой и иной помощи в создании общественных организаций и объединений, которые потенциально могут стать сторонниками революционных перемен в стране;

массовое тиражирование информационных сообщений, распространяемых в условиях наличия революционной ситуации.

Безусловно, наиболее распространенной формой директ- технологий являются массовые адресные или безадресные рассылки. Последнее является специфической чертой именно эверсионных технологий, поскольку традиционный маркетинг требует личного участия в процессе коммуникации получателя и отправителя информации.

Сегодня существует множество способов организовать как адресную, так и безадресную рассылку. Для этого существует целый ряд программ, имеющих характер спама, которые можно найти в Интерне-

те. Информационные рассылки в процессе управления революционными событиями организуются как с помощью Интернета и баз данных e-mail-адресов, так и с помощью мобильного телефоны и даже обычной почты. В последнем случае, для отправителя таких рассылок возрастает риск быть замеченным.

Те, кто занимается директ-рассылками в интересах организаторов смены режима, пользуется необходимыми приемами защиты и сохранения анонимности себя и данного вида деятельности.

Основные функции директ-рассылок в условиях «цветных революций» следующие:

оказание давления на противостоящую сторону (организация рассылки писем соответствующего содержания и характера сторонникам действующей власти и правоохранительным органам);

информирование общественности о происходящих событиях;

распространение информации о злоупотреблениях и нарушениях действующего режима (адресная рассылка по тематическим базам данных и безадресная рассылка с помощью спам-ботов);

привлечение дополнительных сторонников осуществления «цветной революции» (адресная и безадресная рассылка).

Применение эверсионных директ-технологий может быть ограничено как организационными и финансовыми возможностями организаторов «цветных» переворотов, так и возможностями противостоящих им сил.

4.4.3. Цели и методы «Новейшей теории войны»/«Emerging theory of war».

«Созданная адмиралом А. Сибровски и его коллегами теория подразумевает так называемую «сетевую войну» в которой вовсе не обязательно участие вооружённых сил как таковых. Изменилась эпоха, изменились и методы – оружием становится информация и агрессивное воздействие на массовое сознание.

По Эдварду Смиту центральной задачей ведения всех «сетевых войн» является проведение «операции базовых эффектов» (Effects-based operations – EBO), далее ОБЭ. Эта важнейшая концепция во всей данной теории. ОБЭ определяются как «совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны».

ОБЭ означает заведомое установление полного и абсолютного контроля надо всеми участниками актуальных или возможных боевых действий и тотальное манипулирование ими во всех ситуациях – и тогда,

когда война ведётся, и тогда, когда она назревает и тогда, когда царит мир. В этом вся суть «сетевой войны» – она не имеет начала и конца, она ведется постоянно, и её цель – обеспечить тем, кто её ведёт способность всестороннего управления всеми действующими силами человечества. Это означает, что внедрение «сети» представляет собой лишение стран, народов, армий и правительств мира какой бы то ни было самостоятельности, суверенности и субъектности, превращение их в жёстко управляемые, запрограммированные механизмы. За скромной «технической» аббревиатурой «ОБЭ» стоит план прямого планетарного контроля, мирового господства нового типа, когда управлению подлежат не отдельные субъекты, а их содержание, их мотивации, действия, намерения и т. д. Это проект глобальной манипуляции и тотального контроля в мировом масштабе.

Источник: kqduane.com

Карен Парфитт Хьюз

Как мы видим, эта война ведётся против всего человечества и направлена, как и всякая война, на покорение, подчинение и порабощение, в каких бы терминах это ни преподносилось. Традиционные заклинания, звучащие из Вашингтона общеизвестны – «продвижение свободы», «защита общечеловеческих ценностей» и «борьба за демократию».

Какими методами ведутся «тихие боевые действия» уже рассказывалось – вспомним о таких организациях как «Freedom House» или «Конгресс за свободу культуры». Последний был создан в 1950 году под эгидой ЦРУ, и его целью являлось прямое пропагандистское воздействие на европейских интеллектуалов в интересах США. Под эгидой «Конгресса» было создано известное радио «Свобода», но после серии разоблачений в прессе и обвинений организации в связях с американской разведкой в 1967 году он был переименован в «Международную ассоциацию за свободу культуры». Основная цель осталась прежней – воздействие на европейских деятелей культуры, в основном писателей и журналистов» [366].

Ясно, что публичное оглашение таких целей связано с ложным представлением о вседозволенности, безнаказанности и с ещё более необосно-

366 «Модулирование поведения» – война против всех. http://vlasti.net/news/79945

Источник: www.myshared.ru

Артур Сибровски

ванной уверенности в том, что «победа американской демократии неизбежна» (в СССР знаменитость обрёл лозунг «Победа коммунизма неизбежна» – поменьше бы такой самоуверенности и побольше реальных дел, и, глядишь, СССР не окончил свою историю позорным развалом).

Сеть НПО является идеальной с точки зрения осуществления главного принципа ведения современной сетевой войны, отмеченного вице-адмиралом А.К. Сибровски [367], а именно одновременного ведения войны в четырех сферах: физической, информационной, когнитивной и социальной[368]. Заметим, – достижение такой одновременности, обеспечивающий синергизм воздействия, присуще концепции геоцентрического ТВД (генерал Келер) при координации с помощью информационного оружия, а суррогат адмирала Сибровски не более чем усовершенствование традиционной и современной теории войны.

Им разработана приводимая логическая модель сетецентрическиз военных действий:

Данная теория подробно изложена в книге Эдварда Смита «Операции, основанные на модулировании поведения». Труд уникальный по своему цинизму. В нём прямо заявляется: союзников у США нет. Существуют исключительно враги. Объединённая Европа – один из них, как основной экономический конкурент. Ну, а как поступают США с врагами – общеизвестно. Европейцам есть чего опасаться. Угроза, к сожалению, не призрачна

Для достижения целей по организации информационно-управленческого превосходства через возможности НПО осуществляется формирование так называемых механизмов гражданского соучастия и сети раннего предупреждения, этнических и конфессиональных конфликтов, в рамках которых осуществляются:

– создание фокус-групп из местного населения для организации постоянного мониторинга и сбора информации;

– специальная работа с лидерами местных этнических сообществ;

– создание сети экспертов проекта, регистрация СМИ проекта, издание специальных брошюр;

– отбор молодежных лидеров из различных этнических групп;

---

367 Артур Сибровски – вице-адмирал в отставке, руководитель управления МО США по делам трансформации BC/Admiral Cebrowski is Director for Space, Information Warfare, Command and Control (N6). He previously served as Director for C4 Systems on the Joint Staff (J6) and as Director, Space and Electronic Warfare (N6)).

368 Бодвунов А. – НПО: сетевая война против России. Сетевые войны: угроза нового поколения. Евразийское движение. М., 2009, 200 с.

– оценка потребностей местных сообществ;
– организация специальных школ;
– общественные кампании;
– информационные кампании социальных проектов;
– организация эффективных коммуникаций.

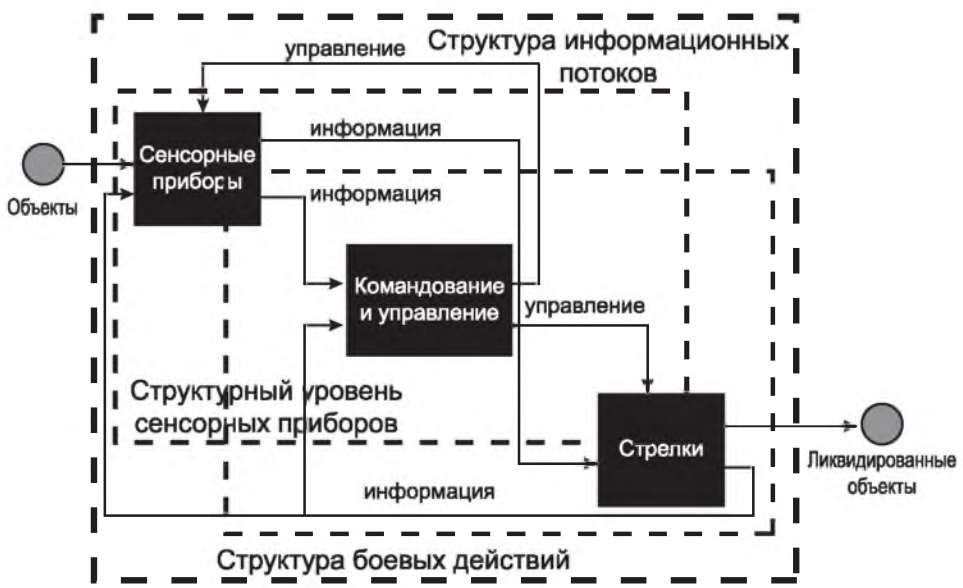
Данные мероприятия осуществляются на системной основе при помощи развития дисфункций определённого государства, склоняющих его руководство к принятию предъявляемых США и их союзников требований. При этом могут быть выделены следующие основные формы данной деятельности:

невооруженная конфронтация, приводящая к «демократической» переориентации государства (например, Грузия), осуществляется при опоре на невоенные воздействия (внешнеполитические, финансовые, научные, социально-экономические, иформационно-психологические), направленные на скрытое ослабление национального потенциала и невооружённое насилие.

В рамках данной формы используются непрямые военные воздействия (военно-стратегическая дезинформация, инициирование внешних и внутренних конфликтов и террористических актов на территории объекта воздействия силами третьей стороны).

Британские аналитики прямо называют «цветные революции» «демократическим шаблоном», универсальным и применимым к самым различ-

Логическая модель сетецентричных военных действий



Источник: Arthur K. Cerbowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future", Naval Institute Proceedings (January 1998) [http://www.usni.org/Proceedings/Articles98/PROcebrowski.html].

Источник: sprotivleniе.ws

На кладбище – поминовение героев

ным государствам, то есть универсальной и тиражируемой политической, психологической, финансовой и информационной технологией по экспорту «демократии» в другие страны, и в качестве следующего объекта её применения указывали Молдавию и государства Центральной Азии.

Важно отметить, что их прогноз сбылся: события апреля 2009 года в Молдавии явное тому подтверждение. По сути «цветные революции» – это качественно новые технологии совершения государственных переворотов, основанные на применении современных манипулятивных технологий психологического воздействия на массовое и индивидуальное сознание населения.

В технологической цепочке манипулирования сознанием следует выделять четыре звена: организация и управление молодёжным протестным движением; системная организация управляемой оппозиции и консолидация её вокруг полностью подконтрольного лидера; «параллельный подсчет голосов» в противовес официальным выборным процедурам; меры, которые сле-

Российская делегация на открытии и освящении памятника российским добровольцам, погибшим в боях за свободу сербского народа (Тучков, Спектор, Манчич, Дёмин, Руколеев).

дует предпринять, если действующая власть пытается отнять победу «бархатной революции» на выборах.

Организация мощного молодёжного протестного движения, внешне выглядящего спонтанным, но, на самом деле, являющимся строго организованным, – это первое звено, которое выделяют британские аналитики[369], в технологической цепочке психологической операции по принудительной смене неугодного США политического режима.

вооруженная конфронтация в ходе конфликтов и войн, приводящая к военно-силовому подчинению государства (например, Югославия);

постконфронтационное противоборство в формах оккупационно-силового и политического урегулирования, приводящее к военно-силовому подчинению государства (например, Ирак).

Американские правительственные организации/NIC (National Intelligence Council) и Институт национальных стратегических исследований/The Institute for National Strategic Studies, INSS совместно с Национальным военным университетом/National Defense University, США представили аналитический отчёт, в котором дали описание политической картины мира к 2015 году, спрогнозировав ключевые мировые тенденции и их влияние на основные регионы и страны планеты[370]. В указанном весьма тенденциозном и ошибочном документе отмечается, что до 2015 года новые нормы международного поведения будут развиваться через опыт новых кризисов, подобно событиям в Руанде и Боснии[371]. В Боснии, впрочем, несмотря на бесконечную цепь политических провокаций, лавину дезинформации и ложной информации о Балканской войне и навязчивый физический контроль правительства Республики Сербской, происходит консолидация общественных сил. В Республике Сербской символом сопротивления стало почитание народных героев и добровольцев, с оружием в руках защищавших сербский народ.

В ходе реализации форм информационно-управленческого превосходства особую роль играют СМИ и социальные сети. Не случайно с февраля 2001 года Госдепартамент США и американское Агентство международного развития инвестировали значительные средства в социальные сети, а также в открытие сайтов Twitter на арабском языке и языке фарси[372].

Однако повседневная практика международных отношений показывает, что кроме денег, в информационном противоборстве необходимо чувство

---

369 Чолиа. – Демократизация ...

370 GLOBAL TRENDS 2015: A Dialogue About the Future With Nongovernment Experts. [http://www.dni.gov/nic/NIC_globaltrend2015.html

371 Phillips W.R. – Civil-Military Cooperation: Vital to Peace Implementation in Bosnia. NATO Review. 1998, Vol. 46, № 1, p. p. 22-25

372 Сурков Н. – США проигрывают мировую информационную войну. Независимая газета, 04.03.2011

Источник: gramyelder.com

Билл Аэрс

меры, хотя бы минимальной воспитанности и проблесков здравого смысла, как у операторов информационного противоборства, так и у заказчиков информационных акций.

Вал дезинформации и самоуверенности в собственной правоте не только снижает эффективность провокаций американских СМИ, но и ведёт к недоверию в обоснованности политических решений США и, как отмечает в своей книге американский учёный-политолог и дипломат, д-р Глен Швайцер[373], к росту враждебности к США со стороны международного сообщества. На психологическом уровне оценка информационной политики США дана в Интервью проф. Билла Аэрса Российскому телевидению[374]:

«Наглость выкрикивания нашего мнения и нежелание ничего слышать в ответ ведёт к параллельной ситуации <…> Это уже создало проблемы для США, и они становятся всё большими <…> Нам необходимо вступать в обсуждения с уважением, – с уважением к себе, но и с не меньшим уважением к другим».

4.4.4. Сетевые технологии информационной войны в деятельности частных военных компаний и неправительственных организаций.

В настоящее время по оценкам экспертов, современная война в информационной сфере ведётся не только между государствами, но и между негосударственными или, точнее, неправительственными организациями и государством.

Информационная область в эпоху сетевых войн связывает между собой все уровни ведения войны и является приоритетной. Эта область покрывает системы передачи информации, различные механизмы её добывания, математические модели обработки информации и т. д. В свою очередь, среда сетевых войн выделилась в самостоятельную категорию и наряду с физическими средами приобрела важнейшее, если не центральное значение.

По сравнению с государством сетевые структуры имеют большую степень корпоративности, а, значит, соответственно, являются более целостными, высокоорганизованными, эффективными по управлению и достигаемым результатам. Сетевые структуры никак не скованы ни собственными размерами, ни всякого рода территориальными ограничениями. Наоборот, «сеть»

373 Schweitzer G. – America on Notice

374 Ayers Bill – US has to break with its superpower arrogance

стремится к расширению и распространению, ведущим к возрастанию её социальной значимости и, соответственно, влиятельности вплоть до полной монополизации контроля над социальной действительностью.

Исходя из этого обстоятельства, следует учитывать, что гражданство, декларируемая принадлежность к той или иной политической партии или религиозной конфессии «солдат» сетевых войн мало что значат и весьма условны.

Основой сетевой войны сегодня становится огромное разнообразие самоуправляемых НПО и частных военных компаний (ЧВК, PMC – private military company). Именно эти организации и превращаются в настоящее время в корпоративные объединения, связанные в одну сеть и дополняющие друг друга на различных уровнях. Частные военные компании, политологические фонды и НПО – новая сфера услуг.

ЧВК зародились в лоне производственных компаний, обладающих военным ноу-хау самого высокого уровня, на чью продукцию существует спрос, которая, правда, редко предназначена для эксплуатации на родине. В настоящее время их персонал насчитывает по некоторым данным 1,5 миллиона человек.

В интервью американскому телеканалу PBS директор британской частной военной фирмы «Erinys» Э. Менвил заявил: «То, чем мы занимаемся, – секрет. Мы не хотим, чтобы другие знали, кто наши клиенты, где мы осуществляем свою деятельность и как мы это делаем. Мы ничего не говорим без разрешения наших клиентов».

Возникает проблема правового характера, так как речь идет о частных контрактах в юридическом смысле, третья сторона не имеет возможности знакомиться с ними, даже парламентарии. В соответствии с американскими законами Конгресс может требовать официального ознакомления только с теми контрактами, сумма которых превышает 50 миллионов долларов. Такие контракты составляют небольшую долю, поскольку существует практика разделения контрактов так, чтобы сумма каждого их них не превышала подотчетной величины.

В настоящее время можно увидеть на сайтах некоторых компаний, например Science Applications International Cooperation, такие виды услуг, как «электронная война», «ведение информационной войны», «система планирования миссий». Заказы ЧВК получают по специальному защищенному каналу и адресам в Интернете. Свои знания, необходимые для выполнения работы, они также черпают преимущественно в глобальной сети, создавая так называемые центры моделирования боевых действий (фирма Cubic из Сан-Диего, Калифорния).

Сетевой принцип организации данных военных фирм позволяет им через Интернет организовывать широкую сеть обеспечения учебного про-

цесса, так называемых менеджеров риска (EUBSA – немецкая дочерняя фирма компании Paladin Risk) и осуществлять контроль подготовки в лагерях Англии, Франции, США.

Следующей важной сферой услуг частных военных фирм и компаний является разведка, включающая в себя сбор информации.

Во-первых, это весь сектор перехвата сигналов и подключения к сетям связи, в которых используются электромагнитные устройства – как наземные, так и спутниковые. С их помощью контролируется мобильная, стационарная связь, радиосвязь, связь посредством лазерных и видимых световых сигналов, а также связь посредством Интернета и электронной почты.

Во-вторых, это весь сектор услуг улавливания «графических» данных и информации фотографической, электронной, инфракрасной или ультрафиолетовой природы на суше, море, в воздухе или в космическом пространстве.

Обработка таких данных и анализ такой информации для нужд секретных служб составляют значительную долю деятельности частных военных фирм. Так, британская фирма «AKE Limited» рекламирует на своем сайте «консультации в отношении рисков в реальном режиме времени» в сфере разведки.

В сфере частного военного бизнеса можно увидеть определенную классификацию ЧВК, основанную на принятой в военных кругах «типологии острия копья»: сужающееся от основания к острию пространство символизирует, с одной стороны, удаление от «тыла» и приближение к «фронту», с другой – уменьшение численности личного состава, то есть соотношение личного состава, находящегося на передовой, и количества обслуживающего персонала составляет 1:100. Первыми идут «фирмы боевой поддержки» (непосредственное участие в боевых действиях), далее «фирмы военно-консультационные» (обучение и разработка стратегии), затем «военные снабженческие фирмы» (материально-техническое снабжение и обеспечение).

Многие фирмы и компании превратились в широко разветвленные холдинги: так, «Military Professional Resources Inc.» принадлежит американскому концерну по производству оружия «Lockheed Martin».

Концерны, в свою очередь, распространили диапазон своих военных услуг и получили доступ на национальные и международные рынки капиталов и финансов. Создаются так называемые «виртуальные фирмы», «виртуальные лоббистские офисы», «Интернет юридические офисы», «оперативные офисы». Таким образом, ЧВК сегодня являются глобальными игроками в сфере психологической войны.

Феноменом совершенно иного рода, способствовавшим возвышению ЧВК и ЧВФ, было изменение способов ведения боевых действий в таких концепциях, как «Revolution in Military Affair» и «Network Centric Warfare» (сетевые боевые действия).

В центре этого феномена стоит использование электронных и информационных технологий. В деятельности ЧВК произошли изменения в ведении боевых действий. Были приняты два новых понятия – «информационная война» и «командная война». Первое означает использование информации и информационных систем в наступательных или оборонительных целях, чтобы подключаться к компьютерным сетям и информационным базам противника, эксплуатировать их, выводить их из строя или разрушать.

Под командной войной подразумевается комбинированное использование электронных, физических, психологических и специальных средств для оказания влияния на командный состав противника, введение его в заблуждение и ослабление.

Эти методы были успешно использованы частной военной компанией «MPRI» при ведении операции «Буря» в Хорватии; в более крупных масштабах – в Афганистане и Ираке. Такие образцы высокотехнологичных вооружений как беспилотные самолеты (БПЛА), действующие с кораблей ВМС США, обслуживались сотрудниками ЧВК.

Из всего этого можно сделать вывод, что среди участников войн будущего, основывающихся на информационных технологиях, будут преобладать так называемые «новые наёмники» – представители разветвленной сети частных военных компаний, принадлежащих крупным корпорациям.

Это так, и не совсем так. Это справедливо для субрегиональных конфликтов, в том числе ведущихся в рамках современной концепции трёхмерной войны. Однако поддержание более крупных военных конфликтов и особенно войн на геоцентрическом ТВД с применением перспективных вооружений будет осуществляться с поглощением и подчинением единой цели войны, как ЧВК, так и «новых наёмников».

Возникает новый вид боевых действий – информационная война, включающая и выведение из строя компьютерных систем противника. В этих условиях первый удар может носить скрытый характер, предваряя военные операции с использованием обычных вооружений. Наносящий такие удары – а информационно-зависимые общества в этом отношении особенно уязвимы, – будет одновременно преследовать множество целей, стремясь ослепить, напугать, отвлечь или просто озадачить противника. Подобные действия опасны и тем, что они могут способствовать разжиганию конфликтов внутри атакуемой страны; таким образом, они выравнивают баланс сил для тех стран, у которых нет обычных вооружений дальнего радиуса действия – ракет и бомбардировщиков. Предвидеть, как именно будет разворачиваться война, начатая подрывом вычислительных систем противника, чрезвычайно трудно.

Сетецентричные силы – силы, способные реализовать концепцию сетецентричной войны (Network Centric Warfare). Сетецентричная война – вой-

на, ориентированная на достижение информационного превосходства. Это концепция проведения военных операций, предусматривающая увеличение боевой мощи группировки объединенных сил за счёт создания информационно-коммутационной сети, связывающей датчики (источники данных); лиц, принимающих решения; и исполнителей, что обеспечивает доведение до участников операций информации об обстановке. Таким образом достигается ускорение процесса управления силами и средствами, а также повышение темпа операций, эффективности поражения сил противника, живучести своих войск и уровня самосинхронизации боевых действий[375].

В настоящее время только Соединённые Штаты, оборонный бюджет которых в четыре раза превышает военные расходы ближайших конкурентов, способны внедрить сложные технические разработки и в полной мере пользоваться плодами военно-технической революции»

«В условиях перманентной сетецентричной войны США со всем миром на первый план выйдет новая элита – «бойцы информационного фронта», потеснив танкистов и летчиков, став главной кузницей кадров для высших звеньев военного командования[376]. Коэн – типичный представитель неоконсервативного направления в политическом спектре американской элиты: «перманентная война» – проекция на современность троцкистской «перманентной революции».

4.5. СОВРЕМЕННАЯ ВОЙНА – ВОЙНА ЗА ДУШИ ЛЮДЕЙ.

Редакция «Российского военного сборника» так оценивает современные цели военных действий в мире: «Надо отказаться от веками установившихся понятий о войне. Надо перестать думать, что война – это когда воюют, а мир – когда не воюют. Можно быть в войне, не воюя явно…

В прежних войнах важным почиталось завоевание территории. Впредь важнейшим будет почитаться завоевание душ во враждующем государстве. Воевать будут не на двухмерной поверхности, как встарь, не в трёхмерном пространстве, как было во времена нарождения военной авиации, а в четырёхмерном, где психика воюющих народов является четвертым измерением…»[377].

---

375 Net-Centric Environment Joint Functional Concept. DOD, 2005. Appendix B. Glossary

376 Элиот А. Коэн: военный историк, политолог неоконсервативного направления, член Совета по оборонной политике, профессор в Школе передовых международных исследований Университета имени Джона Хопкинса, профессор Гарвардского университета и Военно-морского колледжа США

377 Домнин И.В., Савинкин А.Е. – Асимметричное воевание. Игорь Владимирович Домнин – заместитель редактора «Российского военного сборника», полковник запаса; Александр Евгеньевич Савинкин – редактор «Российского военного сборника», кандидат философских наук, полковник запаса [http://www.strana-oz.ru/?numid=26&article=1135

Сегодня США делают ставку в военном деле на абсолютное превосходство. В документе «Национальная военная стратегия США», датированном апрелем 2004 года, разработано новое направление развития вооружённых сил страны на ближайшую и среднесрочную перспективу, описаны способы применения ВС в зависимости от военно-стратегической обстановки, силы и средства, необходимые для достижения превосходства над противником в военных операциях XXI века[378].

Фондом исторической перспективы (президент – доктор исторических наук Н. А. Нарочницкая) был подготовлен сборник Оранжевые сети: от Белграда до Бишкека (Под ред. доктора исторических наук. Н. А. Нарочницкой. Алетейя. Санкт-Петербург, 2008). Эта книга появилась, с большим опозданием. Появись она раньше, многое стало бы понятнее в тех политических катаклизмах, которые потрясали одно за другим государства посткоммунистического пространства последние несколько лет.

Интернациональная группа авторов сборника изучила одну из серьёзнейших проблем современных международных отношений – теорию и практику захвата власти в суверенных государствах проамериканскими политическими группировками.

«Теоретически корни этого явления следует искать в доктрине Монро, согласно которой США более века назад провозгласили своё право устанавливать верные Вашингтону режимы «к югу от Рио-Гранде», т. е. в Центральной и Южной Америке, и в родившейся на её базе мессианской модели мироустройства по имени «Пакс Американа» – мира, построенного по американскому образцу.

Очерк проф. Наталии Нарочницкой[379], открывающий сборник, рассказывает об истории возникновения в США в начале XX века системы «мозговых центров», think tanks.

Отличительной особенностью американских «think tanks» является даже не их прямая связь, сотрудничество и обмен кадрами с конгрессом, государственным департаментом, ЦРУ и другими учреждениями по сбору информации. Для этих «университетов без студентов», как их называли еще перед войной, «студентами» стали и правительство, и политический класс» США в целом. Наиболее яркий тому пример – созданный еще в 1916 году Совет по иностранным делам (Council on Foreign Relations – CFR). Его роль разработчика внешней политики США и связь с госдепом известна ещё с довоенных времён. Разработки Совета не раз служили

---

378 Олегин Александр, Сатаров Виталий – США: ставка на абсолютное превосходство. Журнал «Отечественные записки» №5 (26), 2005

379 Нарочницкая Н. А. – Американские «аналитические институты» – глаза уши и совесть Америки. В кн.: Оранжевые сети: от Белграда до Бишкека/Под ред. д. и. н. Н. А. Нарочницкой. Алетейя. Санкт-Петербург, 2008

основой для официальных внешнеполитических документов США. Именно СИД выработал ещё в начале XX века новую глобалистскую концепцию американской внешней политики, позволившей Вашингтону покончить с изоляционизмом и начать под флагом защиты демократии крестовый поход за мировое господство. И, хотя объявление «холодной войны» приписывают Уинстону Черчиллю с его знаменитой Фултонской речью, стратегию этой войны разрабатывали в СИД.

Именно в журнале СИД «Форин аффеарз» в 1947 году появилась под псевдонимом «Мистер Х» статья «Истоки советского поведения». Её автором был посол США в СССР Джордж Кеннан. В ней была сформулирована «доктрина сдерживания коммунизма», которая, по сути, легла в основу «холодной войны». Другие «think tanks» участвовали в разработке даллесовских доктрин «отбрасывания коммунизма» и «балансирования на грани войны».

Когда же в Вашингтоне убедились, что военная истерия информационной войны против СССР и социалистического блока контрпродуктивна, именно Дж. Кеннан в 1963 году поместил в том же «Форин аффеарс» статью «Полицентризм и западная политика», которая стала основой американской «политики наведения мостов». Её целью было обеспечить постепенный отход восточноевропейских участников Варшавского пакта от социализма и поощрить «ползучую контрреволюцию». В соответствии с этой концепцией США отказывались вести дело со всем Варшавским блоком, чтобы не повышать наднациональную роль СССР и его влияние, и даже пошли на смягчение закона о торговле стратегическими товарами в отношении фрондирующих партнёров в Варшавском пакте.

Доктрину эту пришлось пересмотреть после ввода войск в Прагу в 1968 году. С военной точки зрения такая операция была вроде бы абсурдной – советским танкам противостояли практически безоружные люди. Но СССР не стал ожидать, пока пражская «весна» перейдет в жаркое «лето», и Прага будет готова выйти из Варшавского договора. Он показал Западу, что готов – даже ценой очевидной потери престижа в общественном мнении и антирусских настроений в самой ЧССР, ценой нарушения международного права – подтвердить свой контроль над геополитической зоной ответственности, определённой ялтинскими соглашениями между Сталиным, Черчиллем и Рузвельтом, и не допустить распада военно-стратегического пространства.

США, проинформированные об акции самим советским руководством, признали тогда эту сферу, в отличие, скажем, от Афганистана, вход советских войск в который был воспринят как расширение зоны коммунизма и советского влияния.

В наше время, вспоминая об этом вторжении 1968 года, говорят только о последовавшем вслед за этим резким ухудшением отношений СССР с Западом в целом. Наталия Нарочницкая обращает внимание на другой аспект, немаловажный и для сегодняшних стратегов внешней политики России.

«Крах иллюзий на отрыв поодиночке социалистических стран от СССР привёл США к разрядке, – читаем мы в её очерке. – Прямыми результатами ввода войск в ЧССР были договоры ФРГ и СССР 1970 года, последующий договор между ФРГ и Чехословакией, в котором страны признали «Мюнхенский сговор» недействительным с самого начала, визит Р. Никсона в Москву, встреча во Владивостоке, весь комплекс договоров в области ядерного разоружения, включая его фундамент – Договор о противоракетной обороне 1972 года и Протокол к нему 1974 года». ОБСЕ также вряд ли пришло бы к завершению формирования без ввода войск, который побудил Запад подтвердить в Заключительном акте Хельсинки незыблемость послевоенных границ и реалий, в обмен на согласие СССР на сокращение вооружений в Европе.

Убедительное подтверждение того, что на Западе силу уважают. Но не всё так однозначно, о чём следовало бы сказать в сборнике. Положив под гусеницы танков «социализм с человеческим лицом», руководители стран Варшавского договора обрекли на застой, а затем гибель и «реальный социализм» в своих странах. С 1968-го по 1991-й прошло всего 23 года. В «мозговых центрах» скорректировали механизмы главных калибров, нацеленных на социалистический лагерь, что позволило США довольно быстро запустить механизм его развала с помощью своих агентов влияния.

В крупнейших мозговых трестах США в конце XX века была разработана идеология «единого бесконфликтного мира», в основу которой легла вильсоновская пацифистская идея «мира как концепции», которой должны быть подчинены интересы всех государств. Идея «Пакс Американа» не была выброшена на помойку, но её аккуратно загримировали под концепцию «глобализма» для поставок на экспорт. В этих целях проводились специальные акции «по поиску взаимопонимания» на разного рода международных форумах.

Первый опыт подобных диалогов представили американские «think tanks»[380], среди них Фонд Карнеги, американский Институт мира, и, конечно, СИД. Задачей таких инициатив сам государственный департамент называет «превентивную дипломатию». Они служат «либо дополнением к официальным действиям США, либо заменяют их, когда официальное американское присутствие невозможно». В отличие от конфиденциальных докладов

380 Spector V.N., Illiene I.A. – Think Tanks ...

Трёхсторонней комиссии, созданной в рамках идеологии СИД, призывы к совместному решению «проблем человечества» прямо адресовались мировой и в немалой степени советской элите.

«Советская интеллектуальная и номенклатурная элита, – отмечает Наталия Нарочницкая, – стала остро ощущать гнёт своей идеологии, но не потому, что та разочаровала её как инструмент развития собственной страны, а потому, что стала помехой для принятия в элиту мировую». Цена за место в мировой олигархии была названа в эпоху М. Горбачева» [381].

Нельзя игнорировать опасения значительной части российского общества, что у восходящих лидеров современной России, подобно бывшим лидерам СССР – М. Горбачёву, А. Яковлеву, Э. Шеварднадзе и другим, может возникнуть искушение войти в «мировую элиту» за счёт фундаментальных уступок в части жизненных национальных интересов России. Относительно удачной в этом смысле была попытка Т. Гайдара с его высказыванием о предпочтительности «России до Урала» и успешным развалом ВПК и попытка А. Чубайса с его разбойной приватизацией – их допустили в предбанник «мирового правительства».

«Одним из способов снятия или, по крайней мере, снижения остроты «синдрома неполноценности» российской и других элит, не допущенных в «Комитет 300», в «Трёхстороннюю комиссию» и их структуры, позиционирующиеся в качестве «мирового правительства», безусловно, может стать создание альтернативных структур того же конспирологического плана.»

Попытки отрицать теорию заговора могут быть и, скорее всего, являются частью самого заговора. Национальная элита любой страны, вырабатывая политический курс, должна не предполагать, а полагать наличие заговора того или иного уровня, направленного против интересов страны. В современном цивилизационном пространстве конспирология является неотъемлемой и естественной частью политологии, а политический заговор – способом достижения геополитических преимуществ за счёт непублично согласованных общих действий. Именно в непубличности, ergo, в возможности избежания ответственности состоит сила и отличие заговора от договора, который всегда подтверждён документально и обычно публичен, и от сговора, который может не подкрепляться формальными документами, но всегда публичен в своих проявлениях, например, в совместных акциях в бушующей информационной войне.

В качестве альтернативных структур «другого мирового правительства» может рассматриваться создание, например, «Комитета 500», куда будут входить лидеры национальных элит, не заинтересованных в вхождении в упо-

381 Владимир Большаков «Мир в оранжевых сетях», Столетие.Ru, 18.04. 2008

мянутые структуры действующего «мирового правительства»; «Четырёх- или пятисторонней комиссии», которая может быть сформирована на цивилизационном принципе или на конфессиональном принципе (Христианство: Православная церковь, Греко-римская церковь, Армянская автокефальная церковь, может быть, Католическая церковь; Ислам, Буддизм, Конфуцианство) и, например, Венский клуб, куда войдут ведущие учёные, политологи, социологи и аналитики заинтересованных стран.

Дело в том, что в странах так называемого «золотого миллиарда» существует выраженный дефицит природных ресурсов (менее 1/20 их общего запаса). Они существуют только благодаря «капиталократии»[382] – контролю капитала, не подтверждённого ни природными ресурсами, ни эффективными промышленными мощностями, их военный потенциал подтверждён исключительно дутыми финансовыми ресурсами – суверенный долг США, включая внутренние заимствования, превысил 16 триллионов долларов.

Лишись доллар положения мировой резервной валюты, его реальное обеспечение не стоит и одного цента, и вся военная машина США станет экспонатом в музее бесславия «Комитета 300». Осознание этого факта «крошкой Цахесом» с его манией «параллельного человечества»[383], оседлавшим США и погоняющим элиты стран, которым обещан рай «золотого миллиарда», является реальной причиной возросшей агрессивности США/НАТО в их безнадёжной попытке завоевать мировое господство, опередив надвигающийся системный кризис[384], сломив вооружённым путём сопротивление остального мира, к телу которого «крошка» присосался ненасытным хоботком «капиталократии[385].

Создание альтернативного мирового правительства могло бы защитить интересы 5 с лишним миллиардов жителей земли, не включённых в ареал «золотого миллиарда», на мировом рынке хотя бы за счёт создания альтернативной резервной валюты, не обременённой долгами и подтверждённой всеми материальными, природными и людскими ресурсами заинтересованных стран. Это может быть юань, это может быть рубль, это может быть «юанубль» или «рубюань», или, наконец, попросту «евраз».

Попытки начала такого движения уже делались. Например, Миланом Зецем была создана Международная академия «Элита народов мира», активность которой была ограничена отсутствием финансовой поддержки и пошла на спад после безвременной кончины учредителя. Концептуально

---

382 Субетто А.И. – Капиталократическая эсхатология и мондиализм. «Академия Тринитаризма», М., Интернет: Эл № 77-6567, публ. 10796, 05.11.2003

383 Барац Арье – Презумпция человечности (европейская культура в контексте иудаизма). Иерусалим. 1998

384 Спектор В.Н. – Ортодоксальный иудаизм ...

385 Субетто А.И. – Капиталократическая ...

менее определённой оказалась Международная академия духовного единства народов мира (учредитель – проф. Трапезников). Существенной ошибкой при организации Международной инженерной академии стало включение в её состав действующих руководителей государств-участников.

Однако на ошибках и неудачах учатся. В настоящее время, в условиях продовольственного и энергетического кризисов, инициированных мировой «капитолократией», решительное движение в направлении консолидации усилий стран, подвергшихся вооружённой и экономической агрессии, становится особенно актуальным. Эта задача облегчается кризисом доллара как мировой резервной валюты и отсутствием принципиальных противоречий со странами зоны евро, показавшими всему миру пример сопротивления всевластью управляемой из Манхэттена капиталократии (Вернер Сомбарт), ведущей не только информационную, но и финансово-экономическую войну с Евросоюзом. Интересен и может быть принят за основу первых шагов в таком объединении и подход иранского руководства, намеревающегося осуществлять торговлю своими энергоресурсами за евро и рубли.

Главным препятствием на пути к достижению этой цели является продажность национальных элит разобщенного мира, особенно на постсоветском и простюгославском пространстве.

Долларовые миллиардеры в России, которых с таким восторгом считает и персчитывает «Форбс» – агенты долларовой капиталократии, ограбившие Россию в соответствии с заговором «Комитета 300»[386] и при попустительстве всплывшей из глубин большевистского омута российской элиты и российского руководства. У сербов есть меткое определение: «проданные души», и оно применимо не только к постюгославскому пространству. Стоит только взглянуть на клику М. Саакашвили в Грузии и перед духовным взором предстанут «проданные души».

Устранение этого препятствия усилиями широкой общественности является необходимым и достаточным условием практической реализации

---

386 ***Справка о Комитете 300:*** *Activities of Committee 300 are financed via British East India Co and Dutch East India Co utilizing the spoils of China and «Golden Triangle» opium. It is under direct protection of the US National Reconnaissance Office (the NRO most secret PERMIDEX Intelligence) and GB MI6 enjoying support of the Anti Defamation Leage. Committee 300 directly runs Roundtable at the Rhodes Scholars (Oxford, GB) which coordinates activities of the British Royal Institute for International Affairs, Aspen Institute for Humanistic Studies, Trilateral Commission, the US Council on Foreign Affairs, Dutchey Foundation (Bankers), International Institute for Strategic Studies (IISS, since 1957) and indirectly Bilderberg Club via IISS and Canadian Institute for International Affairs, Union of Concerned Scientists, and what is most important Tavistock Institute (1921). Tavistock Institute is the most important element of the system. It has its own branched system of coordination with Institute for Social research; Princeton Institute for Advanced Studies; Harvard Psychiatric Clinic (Social Psychiatry); Stanford Research Institute; RAND Corp.; Club of Rome; Kissinger's Star Group, running Insurance, Banking, Real Estate, High Technologies (Cybernetics, HAARP, Communications, etc.), Entertainment; IPS (1963); Massachusetts Institute of Technology; National Training Laboratories; Wharton School of Economics (University of Pennsylvania); Hudson Institute; Brookings Institute directly, and CIA – MK-ULTRA – University of Rochester and 85 other Universities via RAND Corp.; Association for Human Psychology (1957) via Club of Rome.*

мер по консолидации дискриминированных стран в рамках альтернативного «мирового правительства», к которому, несомненно, в силу геополитических и геоэкономических причин в своё время присоединятся и страны зоны евро.

Американский «истэблишмент», создав СИД и ему подобные «мозговые тресты», с одной стороны, использует их для генерирования новых идей и разработки возможных сценариев развития политических и иных ситуаций, а с другой – попадает от них в зависимость, в своего рода интеллектуальную кабалу. Однажды созданные доктрины (вроде «доктрины Даллеса», «доктрины Трумэна» и т. д.), как компьютерные вирусы, определяют внешнюю и внутреннюю политику не только того политика, кто дал своё имя очередной доктрине, но и тех, кто сменяет его в Белом доме или госдепартаменте. Даже если они принадлежат к разным политическим партиям. Во главу угла при выработке внешнеполитических рекомендаций для президентов США мозговые тресты ставят даже не национальные интересы Америки, а узкокорыстные интересы нескольких финансово-политических групп влияния, которые, по сути, и владеют Соединёнными Штатами и претендуют на мировое господство от их имени.

При этом выход Америки на европейскую и мировую арену осуществляется с вызовом традиционному понятию национального интереса и суверенитета, с противопоставлением ему, как выражается Г. Киссинджер, «вселенской, основополагающей гармонии, пока что скрытой от человечества», но ясное дело ведомой ему.

В конце 90-х годов XX века Совет охватывает практически все важнейшие общественные институты и государственные структуры США. «В отличие от начального периода своей деятельности, Совет по иностранным делам сегодня кажется внешне растворившимся в американском истэблишменте, – пишет Н. Нарочницкая. – Скорее его можно сравнить с некой ложей посвященных, окармляющей американский истэблишмент идеологическими и мировоззренческими скрепами».

Дж. Лафлэнд в своей статье «Техника государственного переворота», одной из самых сильных в сборнике, приводит ряд конкретных примеров того, как в соответствии с этими «скрепами» США осуществляют прямое вмешательство в дела суверенных государств. Автор убедительно доказывает: «оранжевые революции» – это новая методика государственных переворотов, разработанная «мозговыми центрами» США совместно с ЦРУ. Эти «революции», имевшие место в Сербии, Ливане, Киргизстане, на Украине, в Грузии, и та, что не удалась в Узбекистане, преподносят публике, как народное волеизъявление. Но, как пишет Дж. Лафленд, «в действительности речь, как правило, идет о хорошо организованных операциях, зачастую о преднамеренных постановках для СМИ, оплаченных и контролируемых транснациональными сетевыми

организациями, которые также называют «неправительственными» и которые, в свою очередь, являются инструментами западного влияния». Эти инструменты используются всюду, где такое влияние ослабевает по тем или иным причинам. Координаты и социальные системы здесь значения не имеют.

Многие из тех, кто непосредственно осуществлял смены режима в латиноамериканских странах во времена Рональда Рейгана и Джорджа Буша-старшего, при Билле Клинтоне и Джордже Буше-младшем нашли применение своему ремеслу в странах бывшего советского блока. Лафлэнд рассказывает о двух сотрудниках ЦРУ и госдепа США, присланных в 1989 году в Панаму для ведения переговоров и организации государственного переворота для свержения генерала Норьеги[387]. Их звали Уильям Уокер и Майкл Козак. Уокер вновь «всплыл» в январе 1999 года в Косово, будучи главой верификационной миссии. Он следил за процессом искусственного созидания фиктивной картины сербских зверств, которые и послужили поводом для нападения на Югославию. Майкл Козак был назначен послом США в Белоруссии, где в 2001 году занимался организацией операции «Белый аист», имевшей своей целью свержение президента Александра Лукашенко.

В своем письме в английскую газету «Гардиан» в 2001 году Козак объявил, что в Белоруссии занимался тем же, чем и в Никарагуа и в Панаме, а именно «продвижением демократии».

Большой фактический материал о подрывном характере «оранжевых революций» содержится в статье И. Лебедевой «Брокеры «мусорных революций», в работе П. Ильченкова «Экспресс-революция» в Сербии». О роли финансируемых извне неправительственных организаций в тайных операциях западных спецслужб, о действиях на Украине других агентов влияния рассказывают Э. Попов в статье «Украинские НПО: от «оранжевой революции» к экспорту «демократии» в постсоветские страны» и С. Мирзоев («Украина сегодня: возможно ли второе издание «оранжевой революции»?») Марионеточный характер грузинской «революции роз» вскрывает А. Крылов в статье «Режим Саакашвили: диктатура вместо демократии»[388].

А. Арешев приводит множество ранее неизвестных фактов о методике действий поддерживаемой Западом оппозиции в Армении. Его статья «Оранжевые технологии» в Армении: внутренние факторы и внешняя обусловленность (2004-2007 гг.)» звучит весьма актуально в свете последних

---

387 Лафлэнд Дж. – Техника государственного переворота. В кн.: Оранжевые сети: от Белграда до Бишкека/Под ред. проф. Н.А. Нарочницкой. Алетейя. Санкт-Петербург, 2008

388 Лебедева И. – Брокеры «мусорных революций»; Ильченков П. – «Экспресс-революция» в Сербии»; Попов Э. – Украинские НПО: от «оранжевой революции» к экспорту «демократии» в постсоветские страны; Мирзоев С. – Украина сегодня: возможно ли второе издание «оранжевой революции»? Крылов А. – Режим Саакашвили: диктатура вместо демократии. В кн.: Оранжевые сети: от Белграда до Бишкека/Под ред. проф. Н.А. Нарочницкой. Алетейя. Санкт-Петербург, 2008

попыток противников избранного в феврале президента Саркисяна дестабилизировать ситуацию в стране[389].

Все помнят реакцию Москвы на заявление экс-госсекретаря США Мадлен Олбрайт о том, что Кавказ – это зона «национальных интересов США». Мало, однако, кто знает, что США заявляли об этом ещё в 1997 году. Именно тогда, пишет автор сборника А. Юнусов в своей статье «Запад как фактор дестабилизации Азербайджана», администрация США в лице президента Б. Клинтона, а также конгресс впервые публично объявили Каспийский регион не только «зоной жизненных интересов», но и «главным направлением» внешней политики США. Каспийский регион уже не рассматривался как «задворки бывшего СССР». В общей сложности несколько сот специалистов и экспертов в администрации президента, конгрессе, ЦРУ и научно-исследовательских центрах США занялись изучением ситуации в регионе и разработкой каспийской стратегии. Не случайно Збигнев Бжезинский открыто назвал Азербайджан «геополитическим центром» не только Южного Кавказа, но и всего Каспийского региона, государством, «заслуживающим мощнейшей геополитической поддержки со стороны Америки».

Об усилиях западных спецслужб по дестабилизации обстановки на Кавказе и в Южном федеральном округе в целом говорит и статья И. Добаева «Сетевые структуры «оранжевых» в ЮФО: угрозы национальной и региональной безопасности России»[390].

Несомненной удачей сборника следует признать очерк А. Ниязи «Бишкекский переворот: тюльпановое блюдо на азиатской кухне». Автор привел ряд малоизвестных фактов (например, о влиянии различных кланов на властные структуры), которые сыграли свою роль в том, что задуманная в госдепартаменте США «тюльпановая революция» не принесла тех плодов, на которые рассчитывали в Вашингтоне. Возросла эффективность участия Киргизской Республики в структурах СНГ и региональных организациях – ШОС, ОДКБ, ЕврАзЭс. Американская база имени Ганси стала предметом серьёзного торга, а на авиабазе в Канте наращивается военно-технический контингент ОДКБ-2.

В очерке А. Ниязи и в работах других авторов сборника прорисована вся инфраструктура, с помощью которой США осуществляют свой глобальный «крестовый поход за демократию»[391].

---

389 Арешев А. – Оранжевые технологии» в Армении: внутренние факторы и внешняя обусловленность (2004-2007 гг.). В кн.: Оранжевые сети: от Белграда до Бишкека/Под ред. проф. Н.А. Нарочницкой. Алетейя. Санкт-Петербург, 2008

390 Юнусов А. – Запад как фактор дестабилизации Азербайджана; Добаев И. – Сетевые структуры «оранжевых» в ЮФО: угрозы национальной и региональной безопасности России. В кн.: Оранжевые сети: от Белграда до Бишкека/Под ред. проф. Н.А. Нарочницкой. Алетейя. Санкт-Петербург, 2008

391 Ниязи А. – Бишкекский переворот: тюльпановое блюдо на азиатской кухне. В кн.: Оранжевые сети: от Белграда до Бишкека/Под ред. доктора исторических наук. Н.А. Нарочницкой. Алетейя. Санкт-Петербург, 2008

Практическая подрывная деятельность правительственных и неправительственных организаций США выстраивается на основе официально принятых концептуальных документов – «Акта о поддержке свободы» и закона «О продвижении демократии». Процессы глобальной демократизации курируют Бюро демократии, прав человека и труда госдепартамента США и Федеральное правительственное агентство США по международному развитию. Бюро поддерживает и продвигает программы «демократических реформ» с помощью созданного в 1998 году Фонда прав человека и демократии, избирательно финансирует те страны мира, которые выражают готовность к восприятию «демократических ценностей».

Речь идет не о некоей акции идеалистов от демократии, а о целенаправленной политике по обеспечению доминирующей позиции США на всех параллелях и меридианах. Всеми методами. Ну – а там уж не до демократии. (По материалам Владимира Большакова, «Столетие», 17.04.2008).

4 апреля 2008 года Международный уголовный трибунал для бывшей Югославии (МТБЮ) в Гааге оправдал бывшего премьер-министра Косово Рамуша Харадиная, в прошлом одного из полевых командиров сепаратистской «Освободительной армии Косова» (ОАК). В конце ноября 2012 года МТБЮ вновь оправдал террориста и бандита Хардиная и его подельников «за недостатком улик», хотя все улики и свидетельства содержатся в книге-покаянии бывшей обвинительницы МТБЮ Карлы дель Понте.

Харадинай обучался в одном из контролировавшихся албанскими спецслужбами лагерей террористов. Участвовал в контрабандных перевозках оружия из Албании в Косово, в 1998 году сформировал региональный штаб ОАК, отвечавший за операции в Метохии, а также террористическую группу «Черные орлы», активно сотрудничал с НАТО во время интервенции против бывшей Югославии. Харадиная обвиняли в этнических чистках населения, в убийствах косовских сербов, цыган и «нелояльных» албанцев во время вооруженного конфликта 1998-1999 годов. По оценкам сербских и международных экспертов, за 2 года под руководством Харадиная албанские террористы ликвидировали более 300 и похитили около 400 человек.

Власти в Белграде выдвинули против Харадиная обвинения по 108 эпизодам, связанным с такими преступлениями, как терроризм и убийства гражданских лиц. На следующий день, после того как 8 марта 2005 МТБЮ предъявил Харадинаю обвинения, он оставил пост премьера и добровольно сдался международному правосудию, надеясь получить оправдательный приговор.

Судьи не только выпускали Харадиная под гарантию, но и позволяли ему посещать Косово, где возможностей организовать «охоту на свидетелей» у него было более чем достаточно. Известно, что свидетели по делу Харадиная подвергались давлению, а некоторые из них лишились жизни.

Обвинительная сторона требовала для Харадиная 25 лет лишения свободы, но в итоге все 37 пунктов выдвинутых обвинений были сняты. Такой вердикт Гаагского трибунала позволит Харадинаю не только вернуться в Косово, но и продолжить там свою политическую карьеру.


Источник: ruskline.ru

Наталья А. Нарочницкая

В тоже время, бывший обвинитель МТБЮ Карла дель Понте, на заявлениях которой многие годы держалось негативное представление Запада о сербах, опубликовала сенсационную книгу «Охота: я и военные преступники», в которой привела доказательства того, что нынешнее руководство независимого Косово действительно делало состояние на торговле внутренними органами, изъятыми у похищенных сербов.

Два этих связанных между собой события обсуждены в статье[392] и в интервью доктора исторических наук Наталии Алексеевны Нарочницкой – депутата Государственной Думы Российской Федерации Четвертого созыва, ныне возглавляющей Российскую неправительственную организацию в Европе – Институт демократии и сотрудничества.

Она утверждает: «Как и следовало ожидать, международный уголовный трибунал по бывшей Югославии таки оправдал «полевого командира» – на деле настоящего бандита-боевика уже распущенной так называемой «Освободительной армии Косова» Рамуша Харадиная. Из заключения его освободили еще до начала процесса, хотя в свое время до начала суда не давали свободы даже тяжело больному Слободану Милошевичу.

Конечно, решение этого трибунала носит абсолютно пристрастный политический характер, всё это фарс. Так считаем не только мы в России. Институт демократии и сотрудничества, который я возглавляю, готовит к изданию исследование британского автора, написавшего о трибунале книгу, которая так и называется «Фарс».

Всё это звенья одной цепи, всё это было нужно именно для того, чтобы потихоньку превратить Косово в протекторат. Замысел этот зрел еще в 90-х годах, задолго до бомбардировок несчастного Белграда. Моделировался этот этнический конфликт просто по учебникам, в которых описывается управление такими ситуациями. Незадолго, лет за десять до всего этого, американские газеты откровенно обсуждали, как албанские боевики издеваются над сербами, и сербы вынуждены бежать, потому что жизнь в стране невыносима. Так что нынешние права человека и демократия – это страшное фарисейство.

---

392 Нарочницкая Н.А. – Карла дель Понте 5 лет молчала о злодеяниях албанцев в Косово. Православие и Мир. 8 апреля 2008 г.

Что касается Карлы дель Понте, я имела неприятный опыт встречи с этим человеком. Почти год назад на сессии Парламентской ассамблеи Совета Европы, когда она представляла свой доклад, я лицезрела ее лично. Мне пришлось стоять близко от нее и выступить, практически единственной, против трибунала, указав на серьезнейшие нарушения собственных процедур и международного права, опасную тенденцию формирования этим трибуналом собственной «зоны», где не действует международное право. Карла дель Понте – это чистый демон во плоти, я не побоюсь этого слова. Мне кажется, в ней заложена какая-то биологическая ненависть к правде, к чести, к достоинству, к традиции, к велики м ценностям.

Выйди её книга раньше – никогда Хашим Тачи не стал бы лидером самопровозглашенного квазигосударства «Косово», а оказался бы на скамье подсудимых. Всем известно, что он – боевик, замешанный в чудовищных зверствах.

Что касается похищения сербов, у которых потом вырезали органы, то выясняется, что она знала об этом пять лет и молчала. Более того, в её книге черным по белому написано, что об этом знали и некоторые сотрудники так называемых миротворческих миссий, и боялись за свою жизнь, и потому ничего не говорили. Значит, они прекрасно отдавали себе отчёт, что такое те самые албанцы, которых они мировому сообществу представляли как несчастных жертв, спасающихся от «демонов сербов». Это страшные данные. Есть даже карты, где указаны поселки, в которых вырезали почки у живых людей, и потом их уже добивали и разбирали на органы. Есть данные о том, что там было двенадцать русских женщин, гражданок России, которые были замужем за сербами. И надо этим заняться. Мы имеем полное моральное право, даже моральный долг это расследовать. В частности парижский Институт демократии и сотрудничества, которым я сейчас руковожу, уже объявил о том, что мы собираемся послать наблюдательную миссию выяснить не только эти вопросы, а вообще посмотреть, как же там все-таки соблюдаются права человека, религиозные права. На нашу инициативу уже откликнулся с радостью один британский журналист и правозащитник. Сегодня получили отклик от одного немца. Так что несколько человек наберем, и будем обязательно добиваться такой проверки.

Картина страшная, но я, честно говоря, сомневаюсь, что Европа когда-нибудь признается в этой чудовищной несправедливости и ошибке, в чудовищном преступлении, когда, демонизировав сербов, оправдали агрессию НАТО против суверенного государства в центре Европы, когда расчленили государство, которое подписывало Устав ООН, и Хельсинский акт Организации по безопасности и сотрудничеству в Европе, когда попрали международ-

ное право, сделав границы зыбкими[393]. Европейцам удобно спрятать голову под крыло и признать это всего лишь частной неправдой.

Что касается самой дель Понте, то она заслуживает того, чтобы на неё подали в суд. Она сознательно покрывала преступников, она не только окончательно подорвала репутацию трибунала, который, правда, в моих глазах никогда не имел никакой репутации, она, мне кажется, опозорила идею мировой справедливости в глазах даже тех людей на Западе, у которых ещё были какие-то иллюзии о трибунале. Карла дель Понте окончательно развенчала этот образ, если он хоть для кого-то ещё имел какие-то силу и обаяние»

На вопрос «Как Вы думаете, какой отклик в мире вызовут эти события?» Нарочницкая ответила: «Наша задача – следить за откликами и как можно больше продвигать эту информацию. Эта книга будет расходиться. Надо писать рецензии, задавать вопросы, устраивать обсуждения. Чем больше мы будем об этом писать, тем меньше шансов увернуться от каких-то ответов».

Вопрос – Если ей было выгодно молчать раньше, то почему вдруг она публикует эти признания? Новый хитрый ход?

Ответ: «Кроме всего прочего, циничная попытка заработать большие деньги. Недавно в газете «The New York Times» была опубликована очень большая и аргументированная статья об экономической и энергетической подоплёке целого «проекта» создания балканского кризиса. Ещё в середине 90-х годов разрабатывался проект нефтепровода Албания-Болгария-Македония (АМБОК). И фирма, зарегистрированная в Америке, так и называлась АМБОК. Для реализации этого проекта была необходима «зачистка» этой территории. Сейчас Албания и Хорватия войдут в НАТО, Македонию также туда тянут. Косово отделено. Косово – это единственная природная равнина на Балканах и по ней, в отличие от остальной части Балкан, могут пройти танки. Это прямая открытая дорога к Эгейскому морю, на Салоники.

Заказал этот проект ни кто иной, как британская дочерняя фирма нефтяной корпорации «Халлибертон», а юридическая контора, обслуживавшая её дела, стала местом работы самого Билла Клинтона, после того, как закончился его президентский срок, – того самого человека, который отдал приказ бомбить Белград. Чудесно все сходится».

Вопрос – зная всё это, что же можно сделать?

Ответ – «Всё это и грустно, и поучительно. Европа теперь имеет этот расползающийся по её телу нарыв, который специально ворошат, добавляя яда. И уже никто не может эту ситуацию сдерживать, кроме тех, кто всю кашу заварил. Тем самым, США обеспечивают потребность в себе. Им это нужно для того, чтобы дальше продвинуть свою военную инфраструкту-

393 Нарочницкая Н. А. – Границы становятся зыбкими: Косово – разменная фигура для США. Столетие. Ru. 25.02.2008

Источник: ruskline.ru

Владимир Хомяков

ру к Эгейскому морю, к Черноморским проливам, к нефтеносным районам, к Ближнему Востоку, к Ираку, Афганистану…

Сейчас появились данные о том, что уже несколько лет идут колоссальные нелегальные операции по снабжению старыми запасами произведенного ещё в Советском Союзе оружия марионеточным режимам Ирака и Афганистана, которые сейчас контролируют американцы. Всё это незаконно идет через Албанию, через Чехию… Счет ведется на сотни миллионов долларов.

Для того, чтобы связать всё это в единую работающую систему, в которой все звенья стянуты между собой, нужно принять их в НАТО, так это всё и происходит.

Мы не можем рассчитывать на справедливость всегда и везде. Евангелие нам этого, увы, не обещает. Но наш моральный долг, безусловно, кричать об этой неправде и бороться с ней». (интервью для портала «Православие и Мир» вела Валерия Ефанова[394]).

Практический интерес представляет обсуждение политическим аналитиком, журналистом В. Хомяковым доклада В.В. Путина на Госсовете по истечении его второго президентского срока. Работа Хомякова, безусловно, засуживает внимательного прочтения и изучения специалистами в области информационного противоборства.

В начале этого обсуждения он отмечает, что целью любого проекта, в том числе и сформулированного В. Путиным проекта модернизации страны, является не столько технология достижения поставленной цели, сколько её смысл. «Целью же и смыслом развития любой страны является счастье её народа, причем счастье именно в том смысле, как сам народ его понимает – в соответствии со своим мировосприятием, культурой и традицией». Далее Хомяков отмечает два важных момента из политических реалий, признанных В. Путиным: «…что Россия – «богатая страна бедных людей» и что «Единая Россия» «это – партия, составленная из той же «элиты», не имеющая (по собственному признанию Путина) ни идеологии, ни политических принципов».

В. Хомяков замечает: «что те, кто умиляется нынче, что, мол, «доклад Путина был адресован не набившейся в зал серой «элите», а нам, народу», выдают желаемое за действительное. Доклад был адресован именно ей, «элите», и именно поэтому содержал единственно понятную ей шкурную мотивацию развития».

---

394 http://www.pravmir.ru/article_2819.html

«Я даже готов предположить, что вскоре на каком-то более напоминающем народ форуме Президент выступит с речью, которая будет построена принципиально иначе – с упором на то, что является первостепенным для народа, а не для «элиты». Но означать это будет только одно: фактическое признание того, что «элита» и народ в России имеют принципиально разные жизненные мотивации, по-разному осознают цели развития и будущее своей страны. А раз так, то, в конце концов, выходов из этого тупика может быть только два: либо заменить народ, либо – «элиту» …».

В этом пассаже сказывается технократическое образование автора. При любом режиме, даже предельно автократическом, народ нельзя «заменить», он остаётся носителем власти, и элита вынуждена либо обманывать его, как это делали большевики, либо деморализовать нищетой или развращать его, как это делает современная «элита»[395]. Элиту, даже столь похабную как современная «элита», как часть народа, пусть худшую, тоже нельзя заменить – она не деталь машины, её можно лишь терпеливо и направленно формировать, опираясь на традиции народа[396].

Здесь можно только согласиться с утверждением Владимира Хомякова: «Время и огромные ресурсы, которые могли быть использованы на создание реального Гражданского общества, были бездарно растрачены на создание бесполезных и никого не представляющих симулянтов – от движения «Наши» до «общественных палат»[397] и с его выводом о том, «что «элита» и народ в России имеют принципиально разные жизненные мотивации, по-разному осознают цели развития и будущее своей страны».

Однако такая противоположность восприятия народом и элитой целей и будущего страны ведёт к критическому уровню уязвимости государства в условиях информационной войны[398].

Журналист считает, что «Самое неприятное обычно случается, когда власть, духовно и культурно оторванная от народа и понимающая счастье принципиально иначе, чем он, начинает формировать окружающую действительность под своё понимание счастья, которое считает «универсальным» и «общечеловеческим». И бывает искренне удивлена, когда вместо благодарности народ вдруг хватается за вилы…». А это именно то, что противник ожидает получить в результате своих операций в ходе информационной войны.

---

395 Родионов Ю. Н., Спектор В. Н. – Природа власти и проблемы безопасности государств как организованных человеческих сообществ. Труды МАН ПНБ. М., том 2, вып. 1, с. 47; Спектор В. Н. – Роль народных масс в истории. Лидер, партия, общество. Там же, с. 103

396 Курепина Н. С., Спектор В. Н. – Факторы сегрегации и агрегации национально-государственных социумов. Труды МАН ПНБ. М., том 2, вып. 4, с. 8

397 Хомяков В. – О чём не сказали ни Путин, ни Медведев. Интернет

398 Спектор В. Н. – Меморандум об очередном витке…

Источник: www.florida-rus.com

Кирилл Рябов

Российская элита, стремящаяся заслужить не доверие собственных народов, а признание западных идеологов, как во внутренней, так и во внешней политике склонна следовать «рекомендациям» и политике США в ущерб интересам собственной страны и её народа.

Последние события, связанные со скандальным фильмом «Невинность мусульман», показали, насколько прочно современные информационные технологии вошли в жизнь всей планеты.

История с этим фильмом имеет несколько характерных неприятных черт. Он был заготовлен в полном формате на английском языке более чем полгода тому назад, не получил аудитории и был вброшен в интернет-пространство в урезанном, но, тем не менее, в наиболее вызывающем виде в арабоязычной версии.

Он появился в сети именно тогда, когда хаотизация в странах, претерпевших «арабскую весну», пошла на спад и когда США, Саудовская Аравия не смогли получить в арабском мире достаточной с их точки зрения поддержки их сирийской аферы. Кроме того, довольно быстро и, безусловно, намеренно был высвечен факт продюсирования фильма Накулой Басел Накулой – коптом (национальное меньшинство в Египте, исповедующее христианство), осуждённым в США за мошенничество и лишённым права выхода в Интернет. Лихой поворот. Как говорится «И невинность соблюсти, и капитал приобрести» – и религиозный конфликт раздули, и от себя в какой-то мере бремя вины отвели, и дата выбрана надлежащая.

Кирилл Рябов справедливо замечает, что «вне зависимости от состояния этого «кинопроекта» реакция на него … уже привела к многомиллионному ущербу и десяткам человеческих жертв»[399]. Среди жертв возмущённых арабов, как-то кстати, оказался свидетель убийства Муамара Каддафи, активный протагонист затеянного США с союзниками по НАТО и поддержанного Аль Каедой кровавого переворота в Ливии, посол США Кристофер Стивенс (консульство США в Бенгази, 11.09.12). Кому нужен свидетель!

Продолжением с вариациями стала американская затея с Сирией как пролог к давно запланированным акциям, направленным на смену режима в Иране. Однако, несмотря на открытую информационную войну против Сирии, сопровождавшуюся направлением туда наёмников, включая боевиков из аль Каеды, руководимых спецназом США, администрация Обамы ещё более осторожна, чем в случае с Ливией.

---

399 Рябов Кирилл – Новая линия фронта: Интернет. 02.10.2012

Источник: ru.wikipedia.org

Кристофер Стивенс

Более того, и союзники США по НАТО, вовсю втянутые в информационную войну с Сирией, пока воздерживаются от прямых армейских провокаций. Теперь для этих целей определена Турция, готовая услужить, не безвозмездно, конечно.

Взаимоотношения Сирии с Турцией сильно напоминают отношения гитлеровской Германии с Польшей: снаряд, поставленный через турецкую границу и выпущенный, скорее всего, наёмником, перешедшим через ту же границу, перелетел через ту же границу в обратном направлении, попал в жилой дом и убил граждан Турции. Что тут началось в Интернете – тиражировались «жалобы» премьера Эрдогана – «борца за мир до полного взаимного уничтожения», раскручивалась спираль затеянной США провокации, раздувая конфликт с прицелом на его интернационализацию.

Вот уже и о 5 статье Устава НАТО заговорили, пытаясь запугать Иран и предотвратить его военную помощь Сирии. Опять Интернет используется как оружие грязной пропагандистской провокации. Россия как водится, как уже было в ситуации с Ливией, прос… рает эту информационную войну на интернетовской линии фронта, хорошо хоть в СБ ООН держится, и В. Чуркин не стесняется по полной отоваривать своих жуликоватых коллег.

Казалось бы, что проще – заявить о намерении защищать свои геополитические интересы в регионе и направить на рембазу ВМФ РФ ударную дивизию из морпехов и ВДВ, заявить в СБ ООН о предоставлении этой дивизии права участия в защите российских граждан и сирийского государства от иностранных наёмников и от иностранного вторжения, о намерении направить в поддержку нашему контингенту не гостевой авианесущий крей-

Источник: www.dni.ru

Источник: rus.azattyk.org

Живые и убиенные: *Муамар Каддафи.*

Источник: korrespondent.net

Акция группы «Война» «Х.. в плену у ФСБ».

Источник: www.liveinternet.ru

Первая акция группы «Война», 1 мая 2007 года.

сер, а 2-3 боевых авиагруппы и военные корабли с штурмовыми вертолётами и с комплексами С-300 и С-400 на борту. После такого заявления, поддержанного Китаем, всё бы в миг успокоилось – в администрации Обамы в канун выборов мало политических самоубийц, и нужда в такой акции отпала бы сама по себе.

Гораздо чаще скандалами вокруг контента (содержания текстовых и графических материалов) в Интернете оборачивается простой текст, посыл которого кого-либо не устраивает. За примерами далеко ходить не надо. Возьмём, например, самые свежие – отражение в Интернете ситуации вокруг Сирии и Pussy Riot/Бунт Пи… ёнок (кстати, здесь имеет место продуманное иноязычное название группы этих хулиганок – далеко не все в России владеют английским слэнгом, но все повторяют это мало приличное выражение, которое Путину не удалось заставить перевести на русский язык в прямом эфире его интервьюера – западного журналиста).

Ещё более примитивным, пещерным хулиганством стал «перформанс» группы извращенцев «Война», по-видимому, зашедших слишком далеко поклонников экзибиционизма Джигурды. «Напомним, государственная премия «Инновация» в номинации «Произведение визуального искусства» 8 апреля решением независимого жюри, состоявшего сплошь из новой российской элиты, была присуждена «арт-группе» «Война» за акцию «Х… в плену у ФСБ»[400]. Здесь обоснованное сомнение вызывают сразу два словосочетания: «независимое жюри» и «арт-группа». Акция, за которую «Войне» присудили премию в размере 400 тыс. рублей, была проведена 14 июля 2010 года на Литейном мосту: активисты «арт-группы» изобразили на нём 60-метровый фаллос, который после развода мостов «встал» напротив здания Федеральной службы безопасности.

400 Кобяков Константин – Оправдание «Войны». Интернет

Еще более неприличен проигрыш в затеянной западными фондами информационной войне вокруг неприличной группы мало приличных дам. На кой чёрт понадобилось придавать группе продавшихся девок не соответствующее их статусу идеологическое значение – вполне хватило бы обвинения в нарушении законов нравственности и в хулиганстве в общественных местах группой лиц по предварительному сговору по заказу неустановленных лиц и организаций. Сделать это надо было быстро, оформив приговор на 7-10 (по сумме преступлений) лет. Что же касается осквернения православных храмов, об этом можно было бы упомянуть вскользь на вполне понятном основании, что храмы – не место для немолитвенных перформансов (так теперь «отсиденты» и «досиденты» называют любое, даже самое непристойное действо, направленное на разрушение национальных традиций и традиционной культуры), также как музеи – не место для публичной демонстрации группового секса. Это нужно было сопроводить чёткой государственной информацией, в том числе размещённой в Интернете, как, в общем-то, это сделал президент Путин.

Источник: www.vz.ru

Андрей Ерофеев. ИСКУССствовед

Источник: www.nr2.ru

Бунт Pussy: поза «ожидание».

Забавно, хотя и омерзительно читать комментарии по поводу выдвижения этой, с позволения сказать художественной группы (примеры художеств приведены на рисунке) на международную премию Кандинского, данные в интервью представителя «новороссийской» творческой элиты её медийному рупору, газете «Взляд»[401].

Источник: www.nr2.ru

В Дарвиновском музее: Voina & Pussies.

В этом интервью «авангардный» искусствовед объяснил ретроградному российскому читателю о том, почему акцию Pussy Riot следует считать произведением искусства.

401 Ерофеев Андрей – В русле арт-активизма. Интернет. 13 августа 2012. Перепечатка

Источник: ru-casino.info, inosmi.ru

Хилари Клинтон воскликрула «вау».

Бывший госсекретарь Клинтон и ее партнеры по жизни и по работе .

Он утверждает, что «Акция Pussy Riot обучает формам художественного взаимодействия с обществом и властью».

Причинами таких «разборок» являются сразу две тенденции: широкое распространение доступа к Сети и следующее за этим повышенное внимание к Интернету со стороны различных государственных организаций. Так, к примеру, в США с середины прошлого десятилетия создавалась система так называемой цифровой дипломатии (Digital Diplomacy), то есть намеренного провоцирования в электронных СМИ с целью проверки реакции оппонента, что, в общем-то, является обычным приёмом публичной дипломатии.

Как очевидно из названия, целью этой системы является продвижение американского мнения и отстаивание интересов США на международном уровне, в том числе и с привлечением общественного мнения. Одним из авторов проекта являлась, занимавшая на тот момент пост госсекретаря США, Х. Клинтон. Именно при её активной поддержке несколько крупнейших корпораций, чей бизнес напрямую связан с интернет-сервисами, а также государственные структуры создали несколько специальных отделов.

Официально объявленными задачами этих отделов являются слежение за иностранными сегментами Сети и анализ текущих тенденций[402].

Необходимо заметить, что целью любой государственной информационной системы является именно продвижение национального общественного мнения и отстаивание интересов страны на международном уровне, в том числе и с привлечением общественного мнения. В СССР эти задачи были возложены на группу Печенева, с чем она вполне успешно справлялась, вызывая уважение и опасения зарубежных оппонентов. С тех пор всё изменилось не в нашу пользу, и никто в мире не опасается и не уважает российские информационные службы.

---

402 К. Рябов

В результате функции информационной борьбы, в том числе и в Интернете, обременяют высших должностных лиц государства, в первую очередь президента и министра иностранных дел.

Источник: viperson.ru

Анатолий Алексеевич Ноговицын

В ходе операции по принуждению Грузии в августе 2008 года, когда западные СМИ развернули самую широкомасштабную информационную войну с Россией, неожиданно чёткую и эффективную позицию в информационном противоборстве проявил Генеральный штаб Вооружённых сил Российской Федерации под руководством заместителя начальника Генштаба, генерала А. А. Ноговицина[403], на которого изливались Ниагары клеветы, сообщений о его отставке или даже о смерти.

Источник: www.slav-seti.ru

Андрей Петрович Девятов

Один факт остаётся непреложной истиной, которая, к тому же, подтверждена на практике. «Арабская весна» 2011 года наглядно продемонстрировала, что на первый взгляд стихийные события могут координироваться не только с помощью конспиративных квартир и прочих «шпионских хитростей». Для сбора достаточного количества людей можно просто создать соответствующие сообщества в социальных сетях или разрекламировать интернет-средствами отдельный аккаунт Твиттера, через которые и будут оповещаться потенциальные участники акций.

На фоне всех этих псевдореволюционных событий и так называемых «твиттерных революций» возникает специфический вопрос: точно ли египетские или ливийские «борцы за свободу» самостоятельно провернули схему с координацией через интернет-сервисы?

На самом деле для координации действий разнородных групп боевиков in situ в распоряжение инстигнаторов гражданских войн (СФРЮ, Киргизия и другие) и антиправительственных вооружённых акций («Арабская весна-2011», Сирия и другие) почти полтысячелетия совершенствовала свою подрывную деятельность британская служба внешней разведки, МИ-6. Она всегда готовая выполнить грязную работу не только по поручению своего

---

403 генерал-полковник Ноговицын Анатолий Алексеевич 24 апреля 1952 года. Армавирское высшее военное авиационное училище летчиков ПВО (1973), Военная командная академия ПВО (1980), Военная академия Генерального штаба ВС РФ (1994).

Елизаве́та I

Мария I Стюарт

правительства, но и так называемого «мирового правительства» – финансового банковского спрута, высасывающего кровь народов мира.

Об этом очень убедительно пишет в своей работе политолог, бывший полковник ГРУ Андрей Петрович Девятов (действительный член Российского отделения Международной академии исследования будущего, поверенный в делах войны смыслов Русского стратегического совета).

Он напоминает, что «создание МИ-6 (Military Intelligence-6), приписываемое Френсису Уолсинчену – подручному королевы Великобритании Елизаветы I [404], началось с провокации – казни Марии Стюарт [405] в 1600 году.

Таким образом, секретная служба «Её Величества» (Secret Intelligence Service – SIS) существует уже более 400 лет, но официально как бы и не существует, так как официального бюджета у службы нет.

Глава Министерства иностранных дел и по делам Содружества Соединённого Королевства, которому служба подчинена формально, реально выступает лишь государственным прикрытием выполнения службой внешних, по сути интернациональных функций в интересах мировой финансовой олигархии (Финансового интернационала).

Если секретная служба Моссад, будучи как бы «дочерней фирмой» МИ-6, опирается в основном, на еврейскую диаспору во всём мире, то МИ-6 опирается на международные масонские круги; транснациональные корпорации; оффшорные зоны, специально созданные в 1931 году для «свободы мировой торговли»; мировые банковские сети; организованную преступность; нелегальный оборот наркотиков и подобные организации[406].

Благодаря масонам, тамплиерам и банкам Ротшильдов, Англия стала первой страной мира эпохи индустриального общества. А, став лидером, уже не выпускала бразды власти до той поры, пока индустриализм не исчерпал

---

404 Елизаве́та I (7 сентября 1533-24 марта 1603). Королева Англии и королева Ирландии с 17 ноября 1558, последняя из династии Тюдоров. Младшая дочь короля Англии Генриха VIII и его второй жены, убиенной Анны Болейн.

405 Мария I Стюарт (гэльск. Màiri Stiùbhart; англ. Mary I Stuart) – королева Шотландии 14 декабря 1542-24 июля 1567, родилась 8 декабря 1542 года, казнена в Англии 24.07.1567.

406 Андрей Петрович Девятов - действительный член Россий¬ского отделения Международной академии иссле¬дования будущего, поверенный в делах войны смыслов Русского стратегического совета

себя в силу естественного прогресса технологий и доведения до пределов роста «пирамиды» финансового капитала, который на рубеже XXI века перестал приносить прибыль.


Источник: news-russia.info

Майкл Макфол

С незапамятных времен вся английская политика заключалась в том, чтобы ради выгоды английских (прежде всего, еврейских) банков постоянно создавать по всему миру проблемы, через финансирование решения которых финансовая выгода доставалась банкирам, а политический контроль ситуации – Британской короне.

Во главу угла британской политики всегда ставились лишь «дела и интересы», а обеспечение «дел и интересов» предполагало неслыханную аморальность, наглое предательство, свободу от обязательств перед друзьями и союзниками, заказные убийства. Такое беспринципное обеспечение «дел» и выполняла служба МИ-6.

Политическими и имущественными убийствами на международной арене англо-американские «денди» занимались со времён колониальных захватов. Стоило купить у английской королевы патент – и ты уже не пират-разбойник, а благородный служащий Британской короны с «лицензией на убийство и грабёж».

По законодательному Акту о разведывательных службах Соединённого Королевства сотрудники МИ-6 освобождаются от ответственности за действия, совершённые за пределами страны в рамках выполнения задания, даже если в Англии эти действия расценивались бы как преступные. Де-факто, МИ-6 ныне можно назвать секретной службой тайных операций «мировой закулисы», не связанной никакими законами и не подвергающейся никакому контролю» [407].

Если же вспомнить про американскую Digital Diplomacy и всё с ней связанное, то вопросов становится ещё больше. Появляются и первые подозреваемые в, как минимум, содействии повстанцам, например, тот же Кристофер Стивенс, по стопам которого с упорством, достойным лучшего применения, следует и посол США в Москве Майкл Макфол.

Первый пункт американской цифровой дипломатии, о котором стоит сказать, касается так называемой свободы Интернета. Американцы постоянно продвигают идеи свободы слова в других странах, и эти действия не могли не коснуться Интернета. На протяжении последних лет администрация США неоднократно выказывала своё беспокойство и осуждала блокирова-

407 А.П. Девятов Разведывательная служба «МИ-6», «Опиумная война» и безопасность Олимпиады – 23.08.2008

ние отдельных сайтов, а также различные законодательные акты, связанные с какими-либо ограничениями в Сети.

Конечно, свободный доступ к информации и свобода слова – это хорошо. Но возникает справедливый вопрос: почему осуждение ограничения доступа идёт как-то выборочно? Почему одним странам нельзя делать это ни под каким предлогом, а другие вольны ограничивать всё что угодно?

Кроме того, уже поднадоели обвинения в адрес Китая. Несмотря на почти полную самодостаточность китайского интернет-пространства, в котором есть свои почтовые сервисы, поисковики, энциклопедии и даже социальные сети, США продолжают обвинять Пекин в ограничении свобод граждан в Сети. Напрашивается соответствующий вывод: американцы, наверное, полагают, что тот самый свободный доступ должен осуществляться не вообще, а только в отношении ряда сайтов. Если этот вывод соответствует истинным целям борцов за свободу Интернета, то можно составить примерный список сайтов, через которые «цифровые дипломаты» продвигают свои идеи, а свои ли?

Второе направление продвижения взглядов США касается самой простой пропаганды. Этот вариант Digital Diplomacy подразумевает как прямое высказывание позиции страны, так и скрытое, включая провокационное. В первом случае «вещание» происходит через сайты посольств, официальные их группы в социальных сетях и т. д. Подобный подход позволяет не только информировать целевую аудиторию пропаганды, но и быстро фиксировать результаты последней, анализируя комментарии и реакцию людей.

Конечно, прямая связь местного населения с зарубежными дипломатами имеет свои минусы, – специфическое восприятие получаемой информации или вовсе недоверие к ней. В то же время, главным преимуществом про-

Источник: sholademi.livejournal.com

Посол США в Москве Майкл Макфол и его встречи с россиянами.

движения идей в социальных сетях является возможность быстрой обратной связи. Подобные сервисы, кроме того, позволяют, что называется, обкатывать методы и тезисы перед их «вбрасыванием» в полноценные средства массовой информации[408].

Следующая методика пропаганды является более привычной и касается применения средств массовой информации. Ещё в начале двухтысячных годов США стали организовывать трансляции своих теле- и радиостанций в Интернете. В последние пару лет, кроме существовавших СМИ, было создано ещё несколько новых медийных изданий. Большая часть новых каналов направлена на ближневосточный регион. Кроме того, некоторая часть программ этих станций время от времени распространяется при помощи популярных видеохостингов, например, Youtube. Стоит отметить, что данное направление «цифровой дипломатии» оказывается наиболее доходчивым и перспективным[409].

Главой государственной организации, которая курирует трансляции международных СМИ, была назначена Джил Макхейл, ранее занимавшая высокие посты в медиаконцерне Discovery/Открытие. Очевидно, она обладает достаточным опытом для выполнения задач по завоеванию интереса потенциальных зрителей. При этом интересны высказывания Макхейл по поводу текущих проблем цифровой дипломатии. По её мнению, главными загвоздками на пути продвижения американских идей в Интернете являются пропаганда и агитация международных террористических организаций и влияние крупных зарубежных государств на свои регионы (Россия влияет на СНГ, Китай на Юго-Восточную Азию, а Иран – на Ближний Восток).

Менее серьёзными проблемами является ограждение стран от вещания некоторых радио- и телеканалов. Так, сравнительно недавно Таджикистан и Узбекистан – эти страны по логике Дж. Макхейл входят в зону влияния России – запретили трансляцию «Радио Свобода» на своих территориях, в связи с чем вещание станции на узбекском и таджикском языках было перенесено в Интернет[410].

Третье направление цифровой дипломатии в некоторой мере касается второго, но использует другие каналы пропаганды. Как известно, для создания какой-либо группы лиц вовсе не нужно «приводить за руку» каждого. Достаточно найти нескольких активистов, что называется из народа, которые станут пропагандировать нужные идеи и находить новых сторонников.

Ещё осенью 2010 года такая методика получила официальное одобрение руководства США. Программа Государственного департамента под названием Civil Society 2.0 («Гражданское общество, версия 2.0») имеет довольно

408 К. Рябов

409 К. Рябов

410 К. Рябов

интересные цели. В ходе её воплощения американские специалисты находят активистов в других странах и обучают их азам пропаганды в социальных сетях и блог-платформах, в том числе и с использованием специального программного обеспечения. После этой подготовки активисты могут выполнять выдаваемые им задания, причём делать это в определённой мере эффективнее, чем американские специалисты.

Дело в том, что свежеобученные зарубежные «пропагандисты» по определению лучше знают обстановку в своей стране, чем заокеанские инструкторы или методисты. Согласно ряду источников, в программу обучения пропагандистским технологиям среди прочего входят и курсы по шифрованию передаваемых данных (то есть курсы «молодого шпиона»), по преодолению имеющихся виртуальных барьеров и т. д.

Как видим, идея «цифровой дипломатии» не так уж плоха, как кажется на первый взгляд. Интернет-технологии уже стали привычной частью жизни множества людей, и их распространение только продолжается. До определённого времени крупные государства не обращали должного внимания на новое средство связи, одновременно являющееся, как потом оказалось, ещё и хорошей платформой для пропаганды. Со временем понимание этих фактов дошло до ответственных лиц, и почти все ведущие государства в той или иной мере стали реагировать на новые аспекты жизни общества. Больше всех в этом деле преуспели американцы.

Что же делать другим странам? Ответ очевиден: догонять и при возможности перегонять Соединённые Штаты. Прошлогодние события в арабском мире полностью показали потенциал организации различных «мероприятий» при помощи возможностей, которые даёт Всемирная сеть. Поэтому всем странам, которые в перспективе могут стать местом очередных массовых беспорядков, плавно переходящих в государственный переворот, нужно в самом ближайшем времени заняться тематикой информационной безопасности, а затем начать формирование своих «ударных сил» в Интернете[411].

Практика показывает, что простое отключение доступа к тому или иному ресурсу не даёт должного эффекта: при желании и соответствующих возможностях неугодные существующей власти пропагандистские сайты могут появляться регулярно и в большом количестве[412]. Кроме того, возможности подобных «интернет-партизан» и «шпионов-«добровольцев», в отличие от властей, не ограничены законодательством и сложными бюрократическими процедурами по прекращению предоставления доступа к ресурсу[413].

---

411 К. Рябов

412 К. Рябов

413 Выступление заместителя секретаря Совета Безопасности РФ В. Соболева перед участниками II Международной конференции «Терроризм и электронные СМИ», Айя-Нап, Кипр, 6-11 ноября 2006

В связи с этим для обеспечения информационной безопасности необходимо создание соответствующих государственных структур, которые будут иметь связь и взаимопонимание с крупными национальными компаниями, работающими в сфере высоких технологий, а ещё лучше, по крайней мере, для Российской Федерации переосмыслить на современном уровне и оперативно внедрить опыт группы В. Печенева в области традиционного и современного информационного противоборства.

4.6. В КОСМОСЕ.

В настоящее время, по-видимому, особое внимание нужно уделить процессу завоевания доминирующего положения национальных технологий информационного противоборства на геоцентрическом ТВД с прицелом на достижение господства на гелиоцентрическом ТВД.

Россия (СССР), США и Китай на примере своих устаревших или исчерпавших ресурс космических аппаратов уже продемонстрировали техническую возможность уничтожения спутников на околоземных орбитах. России по наследству от СССР достались первичные технологии защиты от нападения самонаводящимися ракетами, лазерным или пучковым оружием космических аппаратов, размещённых на околоземных орбитах и в ближнем космосе. Подобные технологии были созданы и Соединёнными штатами в ходе выполнения работ по программе СОИ. Это, безусловно, ограничивает возможности быстрой полной дезорганизации таких, базирующихся в космосе информационных систем как GPS и Гланас, способных, в том числе обеспечивать информационную поддержку боевых действий на геоцентрическом ТВД. Эти технологии, правда, не предусматривают защиту от кинематического оружия, отстреливаемого электромагнитными средствами, но в силу физической природы не имеющего систем самонаведения.

В Соединённых штатах по программе СОИ был разработан беспилотный космический летательный аппарат Х-37В многофункционального назначения – передвижной космической платформы информационного управления и координации вооружений геоцентрического ТВД, истребителя спутников и космического разведчика.

В Советском Союзе с конца 50-х годов велись работы по созданию средств борьбы с американскими военными спутниками-разведчиками. 1 ноября 1963 г. на околоземную орбиту вышел первый советский маневрирующий спутник «Полет-1». 12 апреля 1964 г. стартовал «Полет-2». Эти КА были разработаны в конструкторском бюро Владимира Николаевича

Источник: 100big.ru

Валентин Петрович Глушко

Челомея [414] и служили прототипами автоматического спутника-перехватчика ИС истребитель спутников)[415].

«Собственно перехват в космосе спутником ИС был впервые успешно выполнен день в день пять лет спустя после пуска первого ИСа – 1 ноября 1968 года.

В 1960-80-е годы в СССР было выполнено несколько десятков испытаний истребителей спутников. Последнее такое испытание состоялось 18 июня 1982 года. Оно проводилось в рамках крупнейших учений советских ядерных сил, прозванных на Западе «Семичасовой ядерной войной». Учения, в ходе которых были запущены наземные и морские баллистические ракеты, противоракеты, военные спутники (в том числе и перехватчик), произвели на руководство Соединённых Штатов неизгладимое впечатление. «Семичасовая ядерная война» дала неопровержимые аргументы американским военным и политикам, требовавшим начать работы по созданию в США противоспутниковой и противоракетной систем нового поколения.

Решение о разработке и развертывании противоспутниковой системы Президент Рональд Рейган объявил уже через месяц после «Семичасовой ядерной войной» – в июле 1982 года. Затем, 23 марта 1983 года Рейган провозгласил Стратегическую оборонную инициативу (СОИ). Эту программу вскоре окрестили «Звёздными войнами» в честь популярного кинофильма.

В США работы по созданию боевых космических станций развернулись ещё в начале 70-х годов до объявления Рейганом программы СОИ. Предлагались самые экзотические проекты с использованием кинетического, лазерного и пучкового оружия. Так, например, рассматривалась возможность вывода на орбиту мощного рентгеновского лазера. Энергию для него обеспечивал бы ядерный взрыв. Однако на деле не всё оказалось так просто, как на бумаге. Серия испытаний лазерного и пучкового оружия выявили массу проблем, которые американским ученым так и не удалось решить вплоть до официального свёртывания работ по СОИ в 1993 году.

А что же Советский Союз? В середине 70-х гг. работы по ударному космическому оружию были начаты в НПО «Энергия», руководимом Вален-

---

414 Владимир Николаевич Челомей 17 июня 1914-8 декабря 1984 академик АН СССР, дважды Герой Социалистического Труда советский учёный в области механики и процессов управления.

415 Военный космос. Интернет. 28 октября 2010

тином Петровичем Глушко [416]. Головная роль «Энергии» была оформлена специальным Постановлением ЦК КПСС и Совета Министров СССР «Об исследовании возможности создания оружия для ведения боевых действий в космосе и из космоса».

В официальной истории РКК «Энергия» им. С.П. Королева, изданной в 1996 г, об этих работах говорилось следующее:

«..В 70-80-е гг. был проведен комплекс исследований по определению возможных путей создания космических средств, способных решать задачи поражения КА военного назначения, баллистических ракет в полете, а также особо важных воздушных, морских и наземных целей. При этом ставилась задача достижения необходимых характеристик указанных средств на основе использования имевшегося к тому времени научно-технического задела с перспективой развития этих средств…

Для поражения военных космических объектов были разработаны два боевых КА на единой конструктивной основе, оснащенные различными типами бортовых комплексов вооружения – лазерными и ракетными…

Меньшая масса бортового комплекса вооружения с ракетным оружием, по сравнению с комплексом с лазерным оружием, позволяла иметь на борту КА больший запас топлива, поэтому представлялось целесообразным создание системы с орбитальной группировкой, состоявшей из боевых КА, одна часть из которых оснащена лазерным, а другая – ракетным оружием. При этом первый тип аппаратов должен был применяться по низкоорбитальным объектам, а второй – по объектам, расположенным на средневысотных и геостационарных орбитах…».

Источник: golfs3.ru

***17Ф111 «Каскад»** – система с ракетным оружием*

416 Валентин Петрович Глушко, 20 августа 1908-10 января 1989 академик АН СССР, дважды Герой Социалистического Труда действительный член Международной академии аэронавтики, крупный советский учёный, один из пионеров ракетно-космической техники; основоположник отечественного жидкостного ракетного двигателестроения, Генеральный конструктор многоразового ракетно-космического комплекса «Энергия – Буран», лауреат Ленинской премии, дважды лауреат Государственной премии СССР.

Источник: ru.wikipedia.org

Александр Эммануилович Нудельман

Оба типа боевых КА разработки НПО «Энергия» было решено создать на одной конструктивной базе. Исходя из оценок массовых характеристик будущих боевых комплексов, в качестве базовой платформы была выбрана орбитальная станция типа 17К ДОС. НПО «Энергия» имела уже большой опыт эксплуатации аппаратов такого класса. На основе этой базовой платформы были разработаны два боевых комплекса: 17Ф19 «Скиф» – система, предусматривающая использование лазеров и 17Ф111 «Каскад» – система с ракетным оружием.

НПО «Энергия» была головной организацией по всей программе противоспутникового и противоракетного оружия космического базирования.

Головной фирмой по лазерному комплексу для «Скифа» стало НПО «Астрофизика» – ведущая советская фирма по лазерам.

Ракетный комплекс для «Каскада» разрабатывался в фирме А. Э. Нудельмана [417], известного советского конструктора оружия для самолетов и КА.

Выводить на орбиту «Скифы» и «Каскады» должны были на первом (экспериментальном) этапе РН 8К82К «Протон-К», а позже – орбитальные корабли 11Ф35ОК «Буран». Для большего срока боевого дежурства каждый из типов этих КА имел возможность дозаправки, которую должны были обеспечивать корабли «Буран». Кроме того, предусматривалась возможность посещения боевых станций экипажем из двух человек сроком до 7 суток на кораблях типа «Союз»» [418].

Ракетная станция «Каскад».

Меньшая масса бортового комплекса вооружения «Каскад» с ракетным оружием, по сравнению с комплексом «Скиф» с лазерным оружием, позволяла иметь на борту КА больший запас топлива, поэтому представлялось целесообразным создание системы с орбитальной группировкой, состоящей из боевых космических аппаратов, одна часть из которых оснащена лазерным, а другая – ракетным оружием. При этом первый тип КА должен был применяться по низкоорбитальным объектам, а второй – по объектам, расположенным на средневысотных и геостационарных орбитах.

---

417 Проф. Александр Эммануилович Нудельман, 21 августа 1912-2 августа 1996 Дважды Герой Социалистического Труда, Доктор технических наук, академик Академии космонавтики им. К. Э. Циолковского, советский конструктор, учёный и организатор в области вооружений и военной техники. Трижды лауреат Сталинской премии, дважды лауреат Государственной премии СССР, лауреат Ленинской премии.

418 «Звездные войны», которых не было http://www.buran.ru/htm/str163.htm

Для поражения стартующих баллистических ракет и их головных блоков на пассивном участке полета в НПО «Энергия» для комплекса «Каскад» был разработан проект ракеты-перехватчика космического базирования. В практике НПО «Энергия» это была самая маленькая, но самая энерговооруженная ракета. Достаточно сказать, что при стартовой массе, измеряемой всего десятками килограммов, ракета-перехватчик обладала запасом характеристической скорости, соизмеримой с характеристической скоростью ракет, выводящих современные полезные нагрузки на орбиту ИСЗ. Высокие характеристики достигались за счет применения технических решений, основанных на последних достижениях отечественной науки и техники в области миниатюризации приборостроения. Авторской разработкой НПО «Энергия» явилась уникальная двигательная установка, использующая нетрадиционные некриогенные топлива и сверхпрочные композиционные материалы.

Источник: www.buran.ru

Боевая космическая станция

Источник: www.buran.ru

Боевой модуль уходит на цель.

Для орбитальных испытаний ракет было решено установить их на грузовые транспортные корабли «Прогресс». На первом этапе в 1986-88 гг. были запланированы пять полетов таких кораблей в рамках программы «Каскад». На производственной базе НПО «Энергия» – Заводе экспериментального машиностроения (ЗЭМ) началось изготовление этих кораблей под бортовыми номерами 129, 130, 131, 132 и 133.

Для поражения особо важных наземных целей разрабатывалась космическая станция, основу которой составляла станция серии 17К ДОС и на которой должны были базироваться автономные модули с боевыми блоками баллистического или планирующего типа.

По специальной команде модули отделялись от станции, посредством маневрирования они должны были занимать необходимое положение в космическом пространстве с последующим отделением блоков по команде на боевое применение. Конструкция и основные системы автономных модулей были заимствованы с орбитального корабля «Буран». В качестве варианта боевого блока рассматривался аппарат на базе экспериментальной модели ОК «Буран» (аппараты семейства «БОР»).

Тот же базовый модуль, как на орбитальной станции «Мир», те же боковые (уже не секрет, что на «Спектре», например, предполагались испытания оптической системы обнаружения ракетных пусков. А стабилизированная платформа с теле- и фотокамерами на «Кристалле» – чем не прицел?), но вместо астрофизического «Кванта» – модуль с комплексом боевого управления. Под «шариком» переходного отсека – ещё один переходник, на котором висят четыре модуля (на основе «бурановского» фюзеляжа) с боевыми блоками. Это, так сказать, «исходное положение». По тревоге они отделяются и расходятся на рабочие орбиты, выбираемые из следующего соображения: чтобы каждый блок вышел на свою цель в тот момент, когда над ней будет пролетать центр управления.

Фюзеляж «Бурана» используется в этом проекте по принципу «не пропадать же добру»: большие запасы топлива в объединенной двигательной установке и очень хорошая система управления позволяют активно маневрировать на орбите, при этом полезный груз – боевые блоки, находятся в контейнере, скрытые от любопытных глаз, а также неблагоприятных факторов космического полета.

Что существенно в контексте стратегического сдерживания – эта система оружия нанесёт прицельный, «хирургический» удар даже в том случае, если будет уничтожено всё остальное. Как атомные подводные лодки, она способна переждать первый залп.

Военная целевая нагрузка для ОК «Буран» разрабатывалась на основании специального секретного постановления ЦК КПСС и Совета Министров СССР «Об исследовании возможности создания оружия для ведения боевых действий в космосе и из космоса» (1976 год).

Источник: klasnaocinka.com.ua

Военно целевая нагрузка «Бурана»

Боевые блоки, представлявшие собой, по сути, планирующие ядерные бомбы, должны были компактно размещаться в отсеке полезного груза боевого ударного модуля со сложенными консолями крыла в трёх-четырёх последовательно установленных револьверных катапультных пусковых установках.

Габариты отсека полезного груза «Бурана» позволяют разместить на каждой вращающейся катапультной установке до пяти боевых блоков, как это изображено на рисунке. С учётом возможного бокового маневра каждого боевого блока при спуске в атмосфере не менее плюс/минус 1100-1500 км один ударный модуль мог бы в короткое время своими двадцатью маневрирующими боевыми блоками стереть всё живое с лица Земли в полосе шириной до 3000 км.

Существуют сведения и о других военных аспектах применения орбитальных кораблей. В частности, в рамках «ассиметричного ответа» американской программе «звездных войн» (СОИ) рассматривались вопросы минирования с помощью «Бурана» околоземного космического пространства с созданием непреодолимой завесы для космического сегмента СОИ. Более того, в СССР проводились научно-исследовательские работы с наземной экспериментальной отработкой по созданию орбитальных бризантных облаков, быстро и полностью «вычищающих» от космических аппаратов весь околоземный космос до высот 3000 км. Конечно, после этого околоземный космос становился полностью недоступен в течение нескольких месяцев, но ведь эти меры предполагалось использовать только во время (или непосредственно перед) полномасштабного военного конфликта между СССР и США. А, как известно, «лес рубят – щепки летят» …

Однако куда дальше продвинулись работы над лазерным оружием. Поэтому о создании космического лазерного оружия стоит рассказать более подробно.

История проекта «СКИФ».

Борьба с баллистическими ракетами оказалась слишком сложной проблемой. Потому заказчик – Министерство обороны СССР, решило начать сначала разработку эффективного противоспутникового оружия. Ведь вывести из строя КА значительно проще, чем обнаружить и уничтожить летящую боеголовку. Тем самым в Советском Союзе стала разрабатываться так называемая программа «анти-СОИ». Эта система должна была уничтожать будущие американские боевые КА, тем самым лишая США защиты от ядерных ракет. Эти советские станции-«убийцы» хорошо укладывались в рамки военной доктрины СССР, предусматривавшей так называемый «упреждающий ответный удар», согласно которому сначала советские космические станции «анти-СОИ» должны были вывести из строя американские станции СОИ,

а затем уже стартовали бы советские баллистические ракеты для нанесения удара по территории противника.

«Решение было с первого взгляда достаточно простым: установить на КА уже созданный и проверенный лазер для испытаний его в космосе. Выбор пал на лазерную установку мощностью 1 МВт, созданную одним из филиалов Института атомной энергии им. И. В. Курчатова. Этот газодинамический лазер, работающий на углекислом газе, был разработан для установки на самолетах Ил-76. К 1983 г. он уже прошел лётные испытания.

История авиационного лазерного проекта, тесно переплелась с проектом космического лазера. Поэтому, несмотря на то, что она лежит за пределамиобсуждаемой темы, о ней стоит коротко рассказать. К тому же описание лазера на Ил-76 дает представление о лазере для испытаний в космосе.

Боевой лазер испытывался на самолете Ил-76МД с бортовым номером СССР-86879 (иначе его называли Ил-76ЛЛ с БЛ – летающая лаборатория Ил-76 с боевым лазером). Выглядел этот самолет своеобразно. Для питания лазера и сопутствующей аппаратуры по бокам носовой части были установлены два турбогенератора АИ-24ВТ мощностью 2,1 МВт. Вместо штатного метеорадара, на носу был установлен огромный бульбообразный обтекатель на специальном переходнике, к которому снизу был пристроен продолговатый обтекатель поменьше. Очевидно, там размещалась антенна системы прицеливания, которая крутилась во все стороны, ловя цель.

Оригинально было решено размещение лазерной пушки: чтобы не портить аэродинамику самолета ещё одним обтекателем, пушку сделали убирающейся. Верх фюзеляжа между крылом и килем был вырезан и заменен огромными створками, состоящими из нескольких сегментов. Они убирались внутрь фюзеляжа, а затем наверх вылезала башенка с пушкой. За крылом имелись выступающие за контур фюзеляжа обтекатели с профилем, подобным профилю крыла. Грузовая рампа сохранялась, но створки грузового люка были сняты, а люк зашит металлом.

Доработку самолета выполнял Таганрогский авиационный научно-исследовательский комплекс (ТАНТК) им. Г. М. Бериева и Таганрогский машиностроительный завод им. Георгия Димитрова» [419].

«Космический аппарат, предназначенный для установки на нём мегаваттного лазера с Ил-76ЛЛ с БЛ, получил обозначение 17Ф19Д «Скиф-Д». Буква «Д» обозначала «демонстрационный». 27 августа 1984 года министр общего машиностроения Олег Дмитриевич Бакланов подписал приказ №343/0180 о создании 17Ф19Д «Скиф-Д». КБ «Салют» было определено головным по его созданию. Этим же приказом была официально утверж-

419 «Звездные войны», которых не было http://www.buran.ru/htm/str163.htm

дена программа по созданию последующих военных КА тяжелого типа. Затем приказом по МОМ №168 от 12 мая 1985 года была установлена кооперация предприятий, изготавливающих «Скиф-Д». Наконец, в связи с тем, что противоракетная тематика была одним из приоритетнейших направлений, по «Скифу-Д» вышло 27 января 1986 года Постановление ЦК КПСС и Совмина СССР №135-45. Такой чести удостоивался не каждый советский КА. По этому Постановлению первый запуск на орбиту «Скифа-Д» должен был состояться во втором квартале 1987 года.

«Скиф-Д» был, прежде всего, экспериментальным КА, на котором должны были отрабатываться не только лазер, но и некоторые штатные системы следующих аппаратов, создаваемых в рамках программы «советской СОИ». Это были системы разделения и ориентации, система управления движением, система электропитания, система управления бортовым комплексом.

Аппарат 17Ф19Д должен был продемонстрировать также принципиальную возможность создания КА для уничтожения целей в космосе. Для испытаний лазера на «Скифе-Д» планировалось установить специальные мишени, имитирующие вражеские ракеты, боеголовки и спутники. Однако разместить такой мощный лазер на аппарате класса станции ДОС было невозможно. Выход нашелся быстро. К 1983 года стал виден «свет в конце туннеля» с РН 11К25 «Энергия». Этот носитель мог разгонять до скорости, близкой к первой космической, полезную нагрузку массой около 95 тонн. Именно в такую массу вписывался и аппарат с мегаваттным авиационным лазером.

Чтобы ускорить ход работ над «Скифом-Д» в КБ «Салют» было решено максимально использовать опыт прежних и ведущихся на тот момент работ. В состав «Скифа-Д» вошли элементы транспортного корабля ТКС и орбитального корабля «Буран», базового блока и модулей ОК «Мир», РН «Протон-К». Аппарат имел длину порядка 40 м, максимальный диаметр 4,1 м и массу около 95 тонн.

Конструктивно первый «Скиф-Д» (бортовой номер 18101) состоял из двух жёстко соединенных между собой модулей: функционально-служебного блока (ФСБ) и целевого модуля (ЦМ). ФСБ, разработанный на базе функционально-грузового блока 11Ф77 корабля 11Ф72 ТКС, использовался для доразгона «Скифа-Д» после его отделения от РН: блок добавлял необходимые 60 м/с для выхода КА на опорную низкую орбиту. В ФСБ также располагались основные служебные системы аппарата. Для их энергопитания на ФСБ устанавливались солнечные батареи от ТКС.

Целевой модуль не имел прототипов. Он состоял из трех отсеков: отсека рабочих тел (ОРТ), энергетического отсека (ОЭ) и отсека специальной аппаратуры (ОСА). В ОРТ должны были размещаться баллоны с CO2 для питания лазера. Энергетический отсек предназначался для установки

в нём двух больших электро-турбогенераторов (ЭТГ), мощностью 1,2 МВт каждый. В ОСА размещался сам боевой лазер и система наведения и удержания (СНУ). Для облегчения наведения на цели лазера было решено сделать головную часть ОСА поворотной относительно всего остального аппарата. В двух боковых блоках ОСА должны были располагаться мишени для отработки как СНУ, так и боевого лазера.

Однако создатели «Скифа-Д» столкнулись с целым рядом технических проблем. Во-первых, было совершенно неясно запуститься ли на орбите в условиях вакуума и невесомости газодинамический лазер на углекислом газе. Чтобы разобраться с этой проблемой на Заводе им. М.В. Хруничева было решено создать специальный испытательный стенд. Стенд занимал огромную территорию и включал в себя четыре 20-метровые вертикальные цилиндрические башни вакуумирования, две 10-метровые шаровые емкости для хранения криогенных компонентов, разветвлённую сеть трубопроводов большого диаметра. До сих пор эти строения на территории ГКНПЦ им. М.В. Хруничева напоминают о былой программе «советской СОИ».

Много проблем вызывала газодинамика мегаваттного лазера. При его работе был очень большой расход рабочего газа (CO2). Исходящая из лазера струя газа вызывала возмущающий момент. Чтобы его предотвратить решили разработать систему безмоментного выхлопа (СБВ). Специальный трубопровод, прозванный за свой внешний вид «штанами», шел от лазера в энергетический отсек. Там был установлен специальный выхлопной патрубок с газовыми рулями для компенсации возмущающего момента. СБВ разработало и изготовило НПО им. С.А. Лавочкина.

Серьёзные трудности возникли при создании системы энергоснабжения лазера, в особенности – ЭТГ. При их испытаниях были случаи взрывов. Работа турбин генератора тоже вызывала большие возмущающие моменты на аппарат.

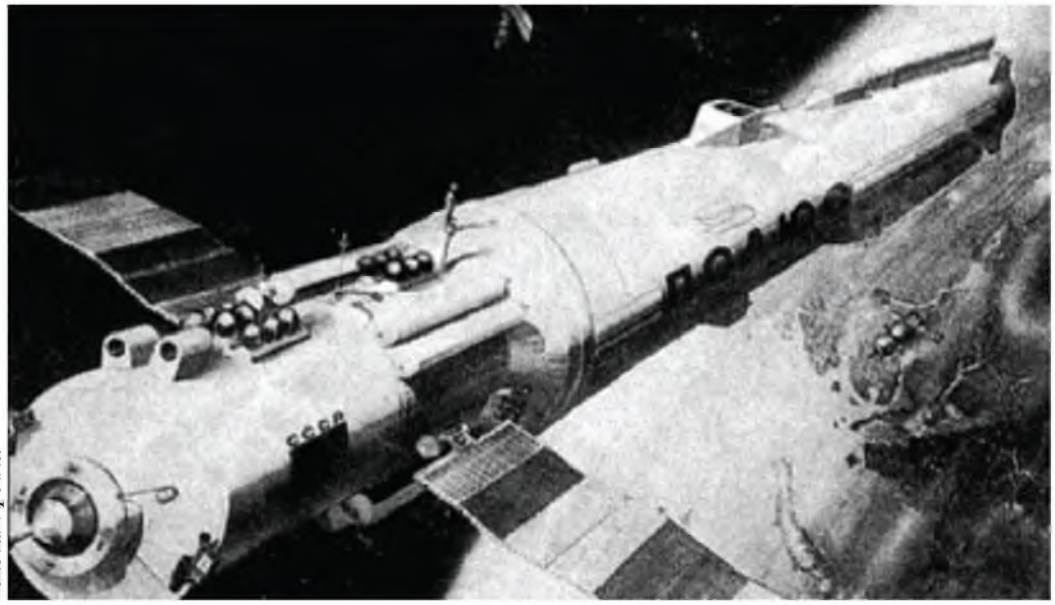
Очень сложной вышла система управления движением «Скифа-Д». Ведь ей приходилось производить нацеливание поворотной головной части и всего аппарата на цель, при этом компенсируя возмущения от работы генераторов, от выхлопа газов из лазера, да и от самих разворотов очень тяжелой, но при этом очень быстро вращающейся головной части ОСА. Уже в 1985 г. было ясно, что потребуется один испытательный пуск КА только для отработки всех этих вспомогательных систем. Поэтому было решено изделие «Скиф-Д1» вывести на орбиту без боевого лазера, и лишь «Скиф-Д2» полностью оснастить «спецкомплексом».

Проект «Скифа-Д» вяз во всех этих проблемах и сложностях. Конструкторы КБ «Салют» натыкались всё на новые и новые трудноразрешимые задачи. Конечно, со временем их можно было бы преодолеть, но не в те

сроки, которые устанавливали приказы МОМ и Постановления ЦК и СМ. В конце 1985 года, рассматривая планы на 1986-87 годы, старт «Скифа-Д1» N18101 планировался на июнь 1987 г, а «Скифа-Д2» № 18301 с лазером – на 1988 год.

Следующим за «Скифом-Д» в КБ «Салют» планировалось создать аппарат 17Ф19С «Скиф-Стилет». Это тоже был аппарат тяжелого класса, рассчитанный на запуск на РН «Энергия». 15 декабря 1986 года был подписан приказ МОМ № 515 о направлении работ в 1987-90 годах, где фигурировал и «Скиф-Стилет». На этом аппарате собирались установить бортовой специальный комплекс (БСК) 1К11 «Стилет», разработанный в НПО «Астрофизика».

«Стилет» для 17Ф19С представлял собой космический вариант земного «Стилета», уже созданного и проходящего в 80-х годах испытания. Это была «десятиствольная» установка инфракрасных лазеров, работающих на длине волны 1,06 нм. Однако, наземный «Стилет» не предназначался для разрушения или уничтожения техники противника. Этого просто не позволяла атмосфера и энергетика. Лазеры предназначались для вывода из строя прицелов и датчиков оптических устройств. На Земле применение «Стилета» было малоэффективным. В космосе за счёт вакуума радиус его действия значительно увеличивался. «Стилет – космический» вполне можно было применять как противоспутниковое средство. Ведь выход из строя оптических датчиков космического аппарата противника был равносилен гибели спутника. Для повышения эффективности действия «Стилета» в космосе был разрабо-



Источник: grok.net

Практическая реализация проекта.

тан специальный телескоп. В сентябре 1986 года электрический действующий макет «Стилета» был изготовлен НПО «Астрофизика» и поставлен в КБ «Салют» для испытаний. В августе 1987 года был изготовлен стендовый прототип кожуха телескопа.

В дальнейшем планировалось разработать целое семейство различных аппаратов тяжелого класса. Была идея создания и унифицированного космического комплекса17Ф19У «Скиф-У» на базе платформы тяжелого класса под РН «Энергия»»»[420].

В середине 1985 года в заключительную стадию вступила подготовка к первому запуску РН 11К25 «Энергия» 6СЛ. Первоначально запуск планировался на 1986 год. Поскольку орбитальный корабль «Буран» ещё не был готов, в Министерстве общего машиностроения было принято решение о запуске РН «Энергия» с макетом КА 100-тонной массы в качестве полезной нагрузки. В июле 1985 г. Генеральный конструктор КБ «Салют» Д. А. Полухин собрал руководящий состав фирмы и сообщил, что министр общего машиностроения О. Д. Бакланов поставил задачу создать 100-тонный макет для испытаний «Энергии». Макет должен был быть готов к сентябрю 1986 года.

После всех корректировок проектного задания появился проект аппарата «Скиф-Д макетный» или 17Ф19ДМ «Скиф-ДМ». 19 августа 1985 года вышел соответствующий приказ № 295 за подписью Бакланова.

Лётный экземпляр КА 17Ф19ДМ «Скиф-ДМ» состоял из двух модулей: ФСБ и ЦМ, имел длину 36,9 метров, максимальный диаметр 4,1 метра, и массу 77 тонн вместе с головным обтекателем.

К моменту разработки «Скифа-ДМ» в НПО им. С. А. Лавочкина была практически готова система безмоментного выхлопа. Поэтому решено было установить СБВ на 17Ф19ДМ для испытания газодинамики и определения величины возмущающего момента при выходе из неё газа. Однако если бы для этого использовался углекислый газ, то зарубежным аналитикам стало бы слишком очевидным назначение «Скифа-ДМ». А потому для испы-

Источник: newsland.com

Лётный экземпляр КА 17Ф19ДМ «Скиф-ДМ»

420 «Звездные войны», которых не было http://www.buran.ru/htm/str163.htm

таний выбрали смесь ксенона с криптоном. Эта смесь позволяла провести интересный геофизический эксперимент – изучить взаимодействие искусственных газовых образований с ионосферной плазмой Земли. Такое прикрытие испытаний СБВ было более или менее убедительным.

Реально было подготовить к сентябрю 1986 года и системы, используемые для наведения лазера «Скифа-Д» на цель и удержания цели в прицеле. Наведение осуществлялось в два этапа. Сначала для грубого наведения использовалась бортовая радиолокационная станция (БРЛС), разработанная в московском НИИ точных приборов. Затем точное наведение осуществляла система наведения и удержания (СНУ), использовавшая для этого маломощный лазер. Создавало СНУ казанское ПО «Радиоприбор» – ведущая в СССР фирма по системам опознавания.

Для обработки данных от БРЛС и СНУ и совместной работы этих систем с исполнительными органами системы управления движением в СУД «Скифа-ДМ» использовалась БЦВМ «Аргон-16», аналогичная такой же БЦВМ на базовом блоке станции «Мир». Для калибровки датчиков СНУ и испытания этой системы решено было использовать отделяемые мишени (типа надувных шаров и уголковых отражателей). Подобные мишени применялись при проведении военно-прикладных экспериментов с использованием комплекса «Пион» на ТКС-М «Космос-1686» в 1985 году и разрабатывались для комплекса «Лира» модуля «Спектр» станции «Мир». На надувных мишенях устанавливались бариевые плазмогенераторы для имитации работы двигателей баллистических ракет и спутников.

Снаружи весь «Скиф-ДМ» имел специальное покрытие черного цвета. Оно должно было обеспечить температурный режим аппарата. Внутри целевого модуля «Скифа-ДМ» стояло слишком мало тепловыделяющих устройств. Поэтому и нужно было максимально использовать солнечное тепло для обогрева. Черное покрытие позволяло это делать. Десять лет спустя то же самое покрытие с той же целью было использовано на Энергетическом модуле «Заря» (ФГБ) 77КМ №17501 для Международной космической станции.

Еще раз надо подчеркнуть, чтобы развеять массу слухов, ходящих о «Полюсе»/«Скифе-ДМ»: боевого мегаватного лазера на нём не стояло, впрочем, как и электротурбогенераторов, обеспечивающих его работу! И ещё, никакого поражения с борта «Скифа-ДМ» отстреливаемых мишеней не предполагалось: их просто нечем было поражать!

Комплекс, состоящий из РН 11К25 «Энергия» №6СЛ и КА 17Ф19ДМ «Скиф-ДМ» №18201, получил обозначение 14А02. Основной задачей для «Скифа-ДМ» стала проверка принципов создания КА 100-тонного класса, выводимого ракетой 11К25 «Энергия». Опыт создания 17Ф19ДМ должен был пригодиться при последующих работах над аппаратами тяжелого класса.

Впервые в отечественной космонавтике полезная нагрузка располагалась асимметрично на ракете, сбоку. Создавался ряд новых систем с развитием новых технологий и освоением новых материалов. Создавалась и новая кооперация предприятий, которая в будущем должна была работать над «советской СОИ». Кроме КБ «Салют» и Завода им. М.В. Хруничева в создании «Скифа-ДМ» принимали участие 45 предприятий Министерства общего машиностроения и 25 предприятий других отраслей.

Однако в ходе работ над проектом «Скиф-ДМ» первоначальная программа испытаний была значительно урезана. И причины этому были вовсе не технические. К этому времени «процесс перестройки пошёл» полным ходом. Ставший Генеральным секретарем Михаил Горбачев целенаправленно использовал тезис о мирном космосе и неоднократно публично поносил американскую программу СОИ и планы милитаризации космоса. И под действием этих новых веяний в верхнем эшелоне партийной власти сложилась группировка, выступившая против демонстрации лётных возможностей прототипа орбитальной лазерной станции.

На основании политических решений Госкомиссия по пуску «Скифа-ДМ» в феврале 1987 года отменила в программе полёта аппарата все отстрелы мишеней, испытания БРЛС и СНУ, выброс ксеноново-криптоновой газовой смеси через СБВ. Решили лишь вывести «Скиф-ДМ» на орбиту, а через месяц свести его в атмосферу над пустынным районом Тихого океана. Что подумали бы в США о таком огромном, но молчащем аппарате – трудно сказать. Пожалуй, здесь было бы не меньше подозрений, чем в случае отстрела мишеней и выброса газовых облаков. Теперь программа полета «Скифа-ДМ» включала в себя лишь десять наиболее «безобидных» экспериментов: четыре военно-прикладных и шесть геофизических.

И вот за несколько дней до запланированного старта 11 мая 1987 г. Горбачёв прилетел на космодром. 12 мая он знакомился с образцами космической техники, в том числе и военной. В итоге Генеральный секретарь ЦК КПСС остался очень доволен увиденным и услышанным. Время посещения-беседы с гостями в два раза превысило предусмотренное. В заключение М.С. Горбачёв посетовал: «Очень жаль, что не знал всего этого до Рейкьявика!»

13 мая во Дворце офицеров состоялась встреча Горбачёва с военными и гражданскими работниками Байконура. Горбачёв говорил долго, хвалил работников космодрома и создателей космической техники. Со стартом «Энергии» он не торопил, предложил сначала разобраться во всех проблемах и лишь при полной уверенности провести пуск такой сложной и дорогой системы. И ещё он заявил: «…Наш курс на мирный космос не признак слабости. Он является выражением миролюбивой внешней политики Советского Союза. Мы предлагаем

международному содружеству сотрудничество в освоении мирного космоса. Мы выступаем против гонки вооружений, в том числе и в космосе… Наши интересы тут совпадают и с интересами американского народа, и с интересами других народов мира. Они не совпадают с интересами тех, кто делает бизнес на гонке вооружений, хочет добиться через космос военного превосходства… Всякие разглагольствования о защите от ядерного оружия – это величайший обман народов. Именно с этих позиций мы и оцениваем так называемую Стратегическую оборонную инициативу, которую стремиться осуществить американская администрация… Мы категорически против переноса гонки вооружений в космос. Мы видим свой долг в том, чтобы показать серьёзную опасность СОИ всему миру…».

После этого судьба «Скифа», да и всей программы развития военно-космических систем стала ясна. И произошедший при запуске аппарата отказ, помешавший его выходу на орбиту, ускорил закрытие работ по данной программе.

«Некоторое время в КБ «Салют» ещё продолжались работы над аппаратом 17Ф19Д «Скиф-Д1» № 18101, старт которого в конце 1985 года был перенесен на июнь 1987 года. Однако после потери интереса к программе у руководства страны, средств на программу стали выделять меньше, сроки пуска стали отодвигаться. Лишь к началу 1987 года для «Скифа-Д1» на ЗиХе были изготовлены отсеки АФУ, ПСВ, ПСН, донный обтекатель, корпуса ПГО, ОДУ и боковых блоков целевого модуля. Корпуса остальных штатных отсеков целевого модуля планировалось изготовить к IV кварталу 1987 года.

Источник: www.arms-expo.ru

X-37B – космический беспилотный самолёт ВВС США возвращается из своей «загадочной СОИвой» миссии по управлению плазмоидами, генерируемыми наземным комплексом ХААРП. По данным ВВС США от 31 мая 2012, в настоящее время ведётся подготовка к запуску третьего прототипа беспилотника X-37B. Точная дата пока не определена; по предварительным данным запуск состоится осенью текущего года.

Возникли проблемы и с созданием в казанском НПО «Радиоприбор» системы наведения и удержания и фотооптической системы слежения. В связи с этим первый заместитель министра Общего машиностроения В. Х. Догужиев ещё 20 апреля 1987 года подписал решение о переносе сроков поставки стендовых комплектов СНУ и ССФО на 1989 год, а штатного комплекта – на 1990 год. С учётом этих сроков «Скиф-Д1» мог быть готов лишь к концу 1991 г. Проблемы с его системами решить не удавалось. По словам ведущего конструктора этой темы Ю. П. Корнилова, специалисты, работавшие над «Скифом», к тому времени подходили к этому аппарату с чисто восточной философией Ходжи Насредина: к тому моменту, когда придет срок готовности «Скифа-Д» «или эмир умрет, или – ишак».

Так, в принципе, и произошло. В сентябре 1987 года работы по теме 17Ф19Д в КБ «Салют» и ЗиХе были приостановлены, да так и не возобновились. «Новое мышление» в международных отношениях и начавшийся в то же время кризис в советской экономике привели к полному прекращению финансирования темы тяжелых боевых орбитальных станций в 1989 году. Закат «холодной войны» привёл и к закату советских «звездных войн».

А в мае 1993 года были прекращены все работы над РН «Энергия» и ОК «Буран»» [421]. Это стало последней точкой в истории создания космического меча Империи. Империи СССР, оставившей однако России знания наши возможностей в ближнем и открытом космосе, в том числе и на основе тяжёлых космических аппаратов (программа «Буран»).

Нужно заметить, что уже в середине 90-х годов XX века советским авиаконструктором Н. Матюком в противовес СОИ в четырёх вариантах (титановый или на основе силоксановых композитов, пилотируемый или беспилотный) был разработан гиперзвуковой космический истребитель с полуконформным барабаном, включавшим 12 ракет, запускаемых электромагнитным импульсом, с лазерной системой наведения и поражения, способный осуществлять управление наземными системами из космоса. К сожалению, заботами Н. И. Рыжкова этот проект был похоронен[422]. В пилотируемом варианте истребитель мог находиться в космосе, активно маневрируя, в течение 72-80 часов – время, достаточное для уничтожения 3-5 спутников, входивших в группировку СОИ. Такой разрыв в группировке требует 24-32 часа для её перестроения к уровню ограниченной эффективности, что позволяет беспрепятственно «прошнуровать» через него предусмотренное стратегическим планом (а в СССР он существовал, ведомый или неведомый Рыжкову и Горбачёву) число межконтинентальных ракет.

---

421 «Звездные войны», которых не было http://www.buran.ru/htm/str163.htm

422 Спектор В. Н., Спектор В. А. – Глобализация ...

Единственным, очевидным на то время недостатком пилотируемого многоразового космического истребителя Матюка в пилотируемом варианте была его уязвимость в режиме возвращения на землю из-за необходимости аэродинамического торможения при вхождении в плотные слои атмосферы.


Источник: www.xsp.ru

Жан-Клод Трише

Трудно сказать, возможен ли и целесообразен ли возврат к проекту Н.И. Матюка – с тех пор много воды утекло, но совершенно очевидна необходимость создания подобного аппарата для обеспечения эффективного противоборства на геоцентрическом ТВД. При этом, безусловно, наработки Матюка и программы «Буран» могут и должны быть использованы, так как они позволят значительно сократить сроки выполнения НИОКР и даже значительной части ОКР при создании такого многофункционального современного ЛА.

Учитывая, что США уже изготовили три прототипа подобных летательных аппаратов, России необходимо иметь в ближайшие 2-3 года как минимум 4 беспилотных и 2 пилотируемых ЛА такого класса.

4.7. В ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ СФЕРЕ.

В сентябре 2011 года тогда ещё премьер-министр России В.В. Путин заявлял, что Москва учитывает замечания рейтинговых агентств, хотя они часто допускают ошибки. Кто не глух, тот услышал истинное значение этих слов: Москва учитывает, что любые замечания американской тройки рейтинговых агентств являются злонамеренной ошибкой.

На самом деле злонамеренность ошибок Moody's, Standard & Poor's и Fitch Ratings является значимым информационным ресурсом в финансово-экономической войне Соединённых штатов с Евросоюзом, впрочем, и с Россией тоже.

Как сообщала газета «Взгляд», с начала мирового финансового кризиса 2008 года национальные регуляторы по всему миру пытаются уменьшить степень влияния «большой тройки» агентств – Moody's, Standard&Poor's и Fitch Ratings. На самом деле эти агентства являются информационными операторами финансовой стратегии международного банковского консорциума, в настоящее время направленной не только и не столько на извлечение максимальной прибыли, сколько на максимальный подрыв суверенитета[423] пока ещё относительно независимых государств за счёт разрушения их финансово-экономических институтов.

423 Спектор В.Н. – Стратегия десуверенизации как основная угроза национальной безопасности. Пленарный доклад на 1 секции Международного симпозиума Интерполитех-2011. М., 2011, 12 с.

В частности, представители стран Евросоюза не раз заявляли, что рейтинговые агентства подрывают восстановление экономики в Европе. В частности, глава Европейского центрального банка Жан-Клод Трише призвал остановить олигополию «большой тройки» международных рейтинговых агентств в лице Fitch, Standard & Poor's и Moody's. Как тут опять не вспомнить «дедушку Крылова: «А Васька слушает, да ест».

Действия трёх крупных международных рейтинговых агентств подверглись жёсткой критике со стороны Международного валютного фонда, Елисейского дворца и Европейской комиссии.

«В июле 2012 года панъевропейский финансовый регулятор – Управление по ценным бумагам и рынкам (ESMA) – инициировал проверку в отношении трёх крупнейших рейтинговых агентств мира – Standard & Poor's, Fitch Ratings и Moody's Investors Service. В рамках процедуры будут исследованы методы, которые аналитики используют для оценки кредитоспособности банковских организаций.

Глава ESMA Стивен Майор пояснил газете Financial Times, что проверка будет завершена к концу 2012 года, передаёт Forbes.

Вплоть до 2011 года деятельность агентств в европейских странах никак не регулировалась. Однако разрастание долгового кризиса и усиливающаяся зависимость настроений инвесторов от рейтинговых действий S&P, Fitch и Moody's заставили финансовые власти ЕС уделить особое внимание этим организациям. Их уже заставили проходить процедуру регистрации в ESMA, и впереди ужесточение контроля и надзора над их работой, уверены эксперты.

Банковские рейтинги привлекают особое внимание регуляторов, так как на агентства зачастую возлагают ответственность за чрезмерно оптимистичный взгляд на проблемный сектор. Организациям вменяют манипулирование настроениями инвесторов и введение их в заблуждение.

По словам Майора, рейтинги банков «имеют важный характер» в силу своей взаимосвязанности с суверенными рейтингами государств и гособлигациями.

Агентство S&P в ноябре 2011 года снизило рейтинги сразу 15 из 37 ведущих мировых банков в результате изменения методологии расчетов. Moody's предприняло аналогичный шаг в июне.

ESMA существует меньше двух лет, и до сих пор регулятору не доводилось принимать меры дисциплинарного характера. Однако заинтересованность управления в деятельности агентств может иметь далеко идущие последствия, предполагают эксперты. ESMA уже наделено полномочиями по инспектированию организаций на местах и оценке их соответствия требованиям в области управления, конфликтов интересов и прозрачности.

По мнению главы ESMA, массовое ухудшение рейтингов банков «создало риски того, что агентства не имеют достаточных аналитических ресурсов и квалификации, чтобы справиться с дополнительной нагрузкой». «Единоразовое изменение рейтингов может всего лишь служить предлогом для минимизации временных издержек. Важно сделать так, чтобы каждому отдельному рейтингу было уделено одинаковое внимание в части деталей и анализа», – констатировал Майор.

Он заверил, что его ведомство не пытается «рейтинговать рейтинги». «Мы не накладываем никаких ограничений на методологию агентств. Мы лишь просим, чтобы их решения имели экономический смысл и внутреннюю логику», – резюмировал глава регулятора.

Управление уже успело понять на собственном опыте, что такое дефицит рабочих рук: в департаменте рейтинговых агентств в ESMA работают 14 человек, которые контролируют деятельность 17 рейтинговых агентств. Майор в этой связи выразил надежду на то, что к концу года число сотрудников регулятора вырастет хотя бы до 20» [424]. Заметим, что количество сотрудников трёх американских рейтинговых агентств на несколько порядков превышают эту цифру. Так что рабочих рук и денег у них хватает.

Fitch Ratings

Тип: рейтинговое агентство
Год основания: 1913
Расположение: США: Нью-Йорк, Нью-Йорк (штат)
Ключевые фигуры: Джон Ноулз Фитч (15.02.1880-08.05.1943) – основатель
Отрасль: международное рейтинговое агентство
Сайт: Fitch Ratings

Moody's Investors Service

Тип: публичная компания
Листинг на бирже: NYSE: MCO
Год основания: 1900
Расположение: США: Бостон, Массачусетс
Ключевые фигуры: Джон Муди (1868—1958) – основатель
Отрасль: международное рейтинговое агентство
Оборот: $2 млрд (2010)

424 Европа не верит рейтинговым агентствам 03.07.2012 , Forbes Russia

Источник: www.im-plus.org

Герд Биллен

Источник: e-korrespondent.net

Михаэль Фукс

Источник: en.wikipedia.org

Кристиан Линднер

Standard & Poor's

Тип: публичная компания
Листинг на бирже: NYSE
Год основания: 1860, корпорация с 1941
Расположение: США: Нью-Йорк, Нью-Йорк (штат)
Отрасль: международное рейтинговое агентство
Оборот: $2,61 млрд (2010)

«Европе не до рейтингов. Создание европейского рейтингового агентства отложено… из-за нехватки денег. Консалтинговая компания Roland Berger, которой поручено проработать вопрос, объявила – набрать 300 миллионов евро в качестве стартового капитала не удалось, пишет Financial Times Deutschland.

Компания рассчитывала, что ради общего дела раскошелятся крупные немецкие и французские банки, но представители двух крупнейших экономик Европы идею восприняли весьма прохладно. Но полностью бросать начатое дело в Roland Berger не намерены: работу продолжит небольшая группа экспертов.

Необходимость появления европейского игрока на «оценочном» поле мотивировали тем, что рейтинговые вердикты от S&P, Moody's и Fitch зачастую вызывали у экспертов много вопросов и даже отчасти способствовали развитию долгового кризиса в Европе, сея панику на финансовом рынке, чего от них и ожидали заокеанские хозяева.

В Европе рейтинговые агентства обвиняют в непрофессионализме. В памяти инвесторов ещё свежа история с ошибкой S&P относительно кредитного рейтинга Франции, приведшая к панике на биржах.

Действия Standard & Poor's и Fitch вызывают волну недовольства среди европейских чиновников. Больше всего возмущения вызывает тот факт, что американские рейтинговые агентства практически неподотчетны регуляторам ЕС, из-за чего в Европе американская система выставления рейтингов кредитоспособности регулярно подвергает-

ся жесточайшей критике. Ну, точь-в-точь как неподсудность американских убийц Трибуналу ООН. Власти ЕС в последнее время регулярно заявляли о необходимости создания собственного европейского рейтингового агентства в противовес американским компаниям «большой тройки»»[425].

Так, глава Федерального объединения европейских центров защиты прав потребителей Герд Биллен называл поведение американских экспертов безответственным и требовал ускорить создание альтернативного европейского рейтингового ведомства. Идею горячо поддерживали и другие влиятельные политики. Заместитель председателя фракции ХДС в бундестаге Михаэль Фукс говорил, что в этом году «необходимо форсировать» создание такой организации. За образец он предлагал взять немецкий Фонд защиты интересов потребителей. Ограничить монополию «большой тройки» настойчиво требовал и Генеральный секретарь Свободной демократической партии Кристиан Линднер.

Европейское управление по ценным бумагам и рынкам ведёт пристальное наблюдение за «большой тройкой», проверяя правомерность и обоснованность действий Standard & Poor's, Moody's и Fitch Ratings. Чиновники ESMA обладают правом накладывать на агентства санкции при вскрытии каких-либо нарушений. Ведомство обещает вскоре опубликовать подробный доклад, в котором специалисты управления изложат свои выводы. Ранее глава ESMA Стивен Майор заявлял: «Мы не должны слепо перенимать регулирующую систему третьих стран». Он пригрозил агентствам из США отказом на лицензирование деятельности в Европе, если они не начнут придерживаться европейских норм.

Кроме того, повышенный интерес к делам экономических экспертов начали проявлять и европейские следственные органы. Так, в конце января прошёл обыск в миланском офисе Fitch. Инициатором проверки стала прокуратура города Трани, которая считает, что агентство могло распространять «недостоверную информацию» об итальянской экономике.

Ранее это же ведомство проводило следственные мероприятия в офисах S&P. Следователи хотели проверить, причастны ли сотрудники этого агентства к разглашению конфиденциальной информации и к биржевым спекуляциям.

И все же оценивать кредитоспособность и вероятность дефолта в европейских странах, похоже, по-прежнему будет «американская тройка», даже, несмотря на появившуюся ещё в конце февраля информацию о том, что Европарламент обсуждает законопроект, который позволил бы Евросоюзу запретить распространение информации о кредитных рейтингах. Ведь Moody's, Standard & Poor's и Fitch Ratings в совокупности занимают 95% мирового рынка[426].

---

425 Европейского рейтингового агентства не будет 16.04.2012 http://www.vestifinance.ru/articles/10354

426 Европейского рейтингового агентства не будет. [vestifinance.ru] Апрель 19, 2012. Интернет

В ноябре 2011 года Еврокомиссия одобрила новые требования к деятельности рейтинговых агентств. Осталось только добиться их реализации.

По определению рейтинговое агентство – коммерческая организация, занимающаяся оценкой платёжеспособности эмитентов, долговых обязательств, качества корпоративного управления, качества управления активами и т. п. Наиболее известный продукт рейтинговых агентств – это оценка платёжеспособности – кредитный рейтинг. Он отражает риск невыплаты по долговому обязательству и влияет на величину процентной ставки, на стоимость и доходность долговых обязательств. При этом более высокий рейтинг соответствует меньшему риску невыплаты.

В мире насчитывается более 100 рейтинговых агентств. В ходе мирового кризиса 2008 года традиционные рейтинговые агентства показали свою некомпетентность, присваивая высокие рейтинги эмитентам и ценным бумагам дефолтного уровня. В результате, США начали изменять законодательство для снижения зависимости при принятии инвестиционных решений от рейтингов. Впрочем, это вовсе не значит, что их некомпетентность или махинации попадут под юрисдикцию других стран, включая Евросоюз. В тоже время нельзя исключить, что мировой банковский консорциум будет делать всё от него зависящее, чтобы остальной мир действовал в соответствии с американским законодательством.

Как уже отмечалось, Евросоюз дозрел до понимания необходимости создания своих рейтинговых агентств. Пусть пока он не сумел реализовать своё понимание, но уже законодательно закрепил обязанность всех, включая американские, рейтинговых агентств получать лицензию Евросоюза.

Более решительно на исходящую из США финансовую и информационную агрессию отреагировали страны БРИКС.

Так, в России уже более 10 лет существует национальное, относительно независимое рейтинговое агентство «Рус-Рейтинг» [427].

Компании из Китая, России и США создают новое совместное рейтинговое агентство **Universal Credit Rating Group**, сообщил генеральный директор одного из участников проекта – рейтингового агентства RusRating Ричард Хейнсворт. Непонятно, правда, причём здесь США. Участие рейтингового оператора США может заметно снизить самостоятельность создаваемого рейтингового агентства и радикально уменьшить его информационную защищённость

«Владимир Путин предлагал создать некое общее рейтинговое агентство для всего евразийского пространства, а мы хотим создать всемирную сеть

---

*427 **Что такое «Рус-Рейтинг»** Год основания – 2001. Сфера деятельности – присуждение рейтинга банкам и исследование банковского рынка. Штат – 22 человека. Президент – Ричард Хейнсворт, 1996-2001 годы: представитель международного рейтингового агентства Thomson BankWatch в Москве.*

рейтинговых агентств, чтобы предложить мировому сообществу альтернативный взгляд на кредитные рейтинги стран и компаний. Проблема в том, что американские агентства считают Нью-Йорк центром вселенной и не учитывают сильные стороны других стран. Они присваивают американским компаниям более высокий рейтинг, чем азиатским, даже если азиатские компании показывает более высокие показатели», – сказал Хейнсворт в интервью RT.

Источник: www.hse.ru

Ричард Хейнсворт

Создатели агентства предполагают, что оно составит конкуренцию большой тройке – Moody's, Fitch и S&P» [428]. Но сторонний аналитик может увидеть в этом попытку поставить такую информационно беззащитную «всемирную сеть рейтинговых агентств» под контроль международного банковского консорциума. Так что выходит – Путин опять прав.

В создании новой структуры, помимо RusRating, участвуют китайское рейтинговое агентство Dagong и американское Egan-Jones.

Источник: telegraf.com.ua

Шон Иган

Dagong – ведущее китайское рейтинговое агентство, известное тем, что первым в мире снизило кредитный рейтинг США.

Egan-Jones Ratings, наряду со Standard & Poor's, Moody's, Fitch и рядом других компаний, входит в семерку «Национально признанных статистических рейтинговых организаций», которые зарегистрированы в этом статусе Комиссией по ценным бумагам и рынкам США.

Рейтинговое агентство Egan-Jones Ratings понизило суверенный кредитный рейтинг США Поводом для снижения рейтинга стало решение ФРС США о запуске третьего раунда покупки активов.

По мнению представителей агентства, действия Федрезерва будут иметь серьёзные негативные последствия для американской экономики в долгосрочной перспективе. В заявлении Egan-Jones отмечается, что программа ФРС по ежемесячной скупке облигаций, обеспеченных пулом ипотечных бумаг, на сумму в $40 миллиардов, а также сохранение процентных ставок на низких уровнях, не приведут к увеличению ВВП США.

По оценке аналитиков Egan-Jones, «действия Федрезерва окажут существенное давление на котировки американского доллара и приведут к росту

428 Россия и Китай создают рейтинговое агентство – «конкурента большой тройки» www.ziwa.org/.

цен на сырьевые активы. Увеличение цен на сырьё, в свою очередь, приведет к росту затрат и снижению прибыльности для компаний, повышению расходов для потребителей и снижению их покупательной способности».

Кроме того, в агентстве негативно оценили траекторию эволюции госдолга и дефицита бюджета США. В заявлении Egan-Jones Ratings отмечается: «с 2006 года по настоящее время объём госдолга США по отношению к ВВП увеличился с уровня в 66% до 104%. При сохранении текущих условий, к концу 2013 года соотношение госдолга к ВВП в США, скорее всего, составит 110%. Дефицит бюджета США составляет 8%. Для сравнения: соотношение госдолга к ВВП у Испании составляет 68,5% при уровне дефицита бюджета в 8,5%".

За Egan-Jones уже закрепилась слава «возмутителя спокойствия», в фарватере решений которого со временем движутся все остальные рейтинговые агентства. В своё время компания была первой, кто понизил кредитный рейтинг скандально известных компаний WorldCom и Enron. В июле прошлого года, почти за месяц до решения Standard &Poor's, агентство Egan-Jones Ratings, первым среди «Национально признанных статистических рейтинговых организаций», понизило кредитный рейтинг США с уровня «ААА» до «АА+»[429].

Американское рейтинговое агентство Egan-Jones сообщило о понижении кредитного рейтинга Германии на одну ступень. Агентство Egan-Jones не является мощным мировым ньюсмейкером: оно не входит в «большую тройку» отрасли, крупные фонды не бегут менять инвестиционную политику на основании его публикаций, а домохозяйки не бросаются обсуждать на кухнях «мировую закулису», прочитав очередную сенсационную заметку о зверствах рейтинговых «монстров»[430].

Так что новость о снижении суверенного кредитного рейтинга столпа Евросоюза могла бы пройти незамеченной, если бы не одно «но»: узкая трейдерская прослойка общества давно заметила, что рейтинги Egan-Jones чудесным образом предваряют решения «большой тройки» – S&P, Moody's и Fitch. Кто первым объявил о снижении рейтинга непотопляемых Соединённых Штатов Америки? Egan-Jones, которое тихо вывесило отчёт у себя на сайте ещё 19 июля. Вряд ли документ обрёл широкий круг читателей. Зато 6 августа мы проснулись уже в другом мире, в котором больше нет всесильной ААА-Америки, а есть только обычная АА+.

Героем месяца стало S&P, якобы первым решившееся поколебать основы мироустройства. Многие эксперты финансового рынка говорят, что Egan-

---

429 Агентство Egan-Jones понизило кредитный рейтинг США. Интернет 14.09.2012

430 Сарычева Мария – «Малыш» Egan-Jones снижает Германии кредитный рейтинг (Последуют ли этому примеру «монстры» S&P, Moody's и Fitch, как это было в случае с США?) Интернет, 19 января 2012

Jones наименее подвержено влиянию американского банковского и государственного лобби, поэтому его оценкам можно доверять в большей степени, чем оценкам «большой тройки». Внутри рейтингового бизнеса думают иначе.


Источник: r-conference.ru

Виктор Николаевич Четвериков

«Мне кажется, что Egan-Jones, пользуясь случаем, хочет заявить о себе на глобальном уровне, поскольку тема суверенных рейтингов стран Евросоюза находится на пике общественного внимания с одной стороны, а с другой стороны, критика в адрес «большой тройки» не ослабевает, – считает генеральный директор Национального рейтингового агентства (НРА) Виктор Четвериков. – Они пытаются набрать очки за счёт очевидных вещей. Потому что действительно надо приводить в соответствие рейтинги всех государств, но сейчас все этим занимаются. Мы, например, понизили Германию и Францию ещё год назад. Им и нам это проще сделать, чем крупным агентствам. Но говорить, что они более независимы, я бы не стал. Не думаю, что их оценка окажет сильное впечатление на инвесторов и государство, поскольку ящик Пандоры был открыт ещё до их решения.


Источник: www.finam.ru

Алексей Владимирович Логвин

По словам Четверикова, понизить кредитную оценку Германии надо было давно – экономики всех стран Европы дают сбои, и это касается крупнейших экономик региона. Теперь же, как считает гендиректор НРА, оценки ААА достойны только скандинавские страны, Австралия и Новая Зеландия.

Решение Egan-Jones было обнародовано в день, когда состоялся очередной аукцион немецких краткосрочных долговых бумаг. И прошел он вполне успешно, с понижением доходности относительно прошлых торгов. Главный экономист УК «Русь-Капитал» Алексей Логвин полагает, что это даёт основания думать, что решение Egan-Jones всё-таки было преждевременным.

«У Германии есть шанс получить снижение рейтинга только за компанию с кем-то ещё по политическим причинам, потому что экономической необходимости в таком шаге нет, – говорит он. – Те макроэкономические индикаторы, которые мы видим в последнее время, – промышленное производство, безработица – вполне адекватны и не внушают серьезных опасений».

Логвин полагает, что в тех условиях, которые сейчас сложились на европейских рынках, даже S&P, Moody's и Fitch не смогут внести серьёзную смуту,

Источник: russianexpert.ru

Дмитрий Андреевич Кулешов

Источник: www.bfm.ru

Алексей Викторович Вязовский

поскольку сильнейшим игроком стал ЕЦБ, который раздал евробанкам многомиллиардные кредиты. Причем вливания произошли в очень короткий срок. Поэтому пока эти деньги ищут себе путь в более-менее надёжные активы, опасаться резко негативной реакции рынка на любые действия рейтинговых агентств не стоит. Рынку трудно падать в таких условиях, какие бы новости ни выходили».

С этой точкой зрения согласен и аналитик ИК «РУСС-Инвест» Дмитрий Кулешов.

«Агентство в данном случае высказывает опасения, что Германии придётся оплачивать долги проблемных стран еврозоны, – говорит он. – Это принципиально отличается от опасений в связи с невозможностью государства обслуживать собственный долг. При этом доходность немецких облигаций, как считает Egan-Jones, останется на текущих низких уровнях. Именно это имеет определяющее значение для рынков капитала. S&P, кстати, уже сообщило, что понижать рейтинг Германии не собирается. Но даже если это и произойдёт, важна будет реакция на это событие со стороны портфельных управляющих, а не сам факт снижения».

С такой интерпретацией событий не может согласиться аналитик ФГ «Калита-Финанс» Алексей Вязовский. Он уверен, что снижать рейтинг Германии пора уже давно. Но принять такое решение «большая тройка» попросту боится: агентствам в Европе уже никто не верит, поскольку они выставляли Греции высшие баллы при вступлении в ЕС.

«Если же S&P, Moody's и Fitch все-таки решатся на такой шаг, то это вызовет, прежде всего, кризис на межбанковском рынке, – прогнозирует Вязовский – Европейские банки уже сейчас закрывают друг другу лимиты. И все идут за деньгами в ЕЦБ, который стал кредитором в последней инстанции. Но такое участие регулятора чревато инфляцией».

Вязовский считает, что столь активное использование печатного станка в скором времени может превратить Европу в подобие арабского мира, где люди выходят на улицы, потому что у них нет денег на покупку бешено подорожавшей еды. Разумеется, цивилизованный Старый Свет не будет лить кровь из-за удешевления евро, но социальная напряжённость, по мнению аналитика, неизбежна.

Dagong Global Credit Rating (大公国际资信评估有限公司; pinyin: Dàgōng Guójì Zīxìn Pínggū Yǒuxiàn Gōngsī) является кредитным рейтинговым агентством, базирующимся в Китае. Оно представляет собой одно из немногих заметных кредитных рейтинговых агентств, не базирующихся в США[431].

Дагонг присвоил американскому долгу самый низкий кредитный показатель (A+ с ноября 2010 года и A с августа 2011)[432] по сравнению с объявленными тремя традиционными рейтинговыми агентствами: Moody's, Standard and Poor's and Fitch. В настоящее время Dagong присваивает США такой же кредитный рейтинг как Испании. Комиссия США по ценным бумагам и рынкам отказалась признать рейтинг, определённый Dagong, в связи с отсутствием у Комиссии возможности осуществлять надзор за Пекинским агентством[433].

Dagong Global Credit Rating Co.

Industry: Financial Services
Founded: 1994
Headquarters: Beijing, China
Key people: Guan Jianzhong (Chairman)
Website: dagongcredit.com

Universal Credit Rating Group создаётся как «совершенно независимая рейтинговая служба» (или намеренная считаться независимой), которая «не представляет интереса той или иной страны или группы». Тогда ей следовало бы поискать остров Утопию в необъятном мировом океане.

4.8. В ФОРМИРОВАНИИ ЛОГИСТИКИ ОБОРОНИТЕЛЬНЫХ СИСТЕМ И СТРУКТУРЫ ВООРУЖЕНИЙ.

Анонсированное 5 января 2012 года Б. Обамой новое стратегическое руководство по обороне (defense strategic guidance) для Министерства Обороны, озаглавленное «Поддержание глобального превосходства: Приоритеты для обороны 21 века»[434] («Guidance») вызвало множество откликов.

Хотя новое руководство утверждает, что его разработка осуществлялась в рамках реализации стратегии национальной безопасности США,

431 http://finance.yahoo.com/banking-budgeting/article/112029/what-is-the-us-governments-credit-score?mod=bb-creditreports

432 Beaumont Peter – Chinese ratings agency threatens US with new debt downgrade. The Guardian (London). 11 November 2011

433 Dagong, the new Chinese bad guy or a fair player?»,SACR, 21 mars 2012

434 Department of Defense. Sustaining U.S. Global Leadership: Priorities for 21st Century Defense. Defense Strategic Guidance, Office of the Assistant Secretary of Defense (Public Affairs) January, 2012.

Источник: www.wilsoncenter.org

Барри Росс Позен

подготовка документа была осуществлена без мандата Конгресса и вне принятой процедуры и рамок разработки стратегических руководств для МО США[435].

Документ призван определить приоритеты военной политики и стратегии США на последующие десять лет в условиях сокращения военных расходов на $487 миллиардов долларов и изменения среды безопасности[436].

Представители Пентагона уже заявили, что если от них потребуют сократить бюджет еще на $500 миллиардов, то документ потеряет адекватность[437]. Руководство охватывает как геополитические, так и чисто военные аспекты новой политики.

Геополитические и геостратегические аспекты

В свое время Альфред Мэхэн (Alfred Mahan)[438] определил открытое море, обеспечивающее международную торговлю и коммуникации, как «общее пространство» (a wide common)[439].

Мэхэн не смог предугадать освоение воздушного и космического пространств, но, скорее всего, согласился бы с распространением концепции на воздушную среду, космос, кибер-пространство и с расширением термина до «глобального пространства» (a global common)[440]. Использование данного термина в документе свидетельствует о продолжении классической геостратегии морских держав и открытом возвращении геополитики в оборонную политику и стратегию США.

---

435 Согласно американскому законодательству Президент ежегодно представляет на рассмотрение Конгресса стратегию национальной безопасности (National Security Strategy); каждые четыре года министерство обороны представляет доклад «Четырёхлетний обзор обороны» (Quadrennial Defense Review (QDR), согласующийся со стратегией национальной безопасности и включающий в себя стратегию национальной обороны (national defense strategy); и каждые два года Председатель Объединённого комитета начальников штабов представляет национальную военную стратегию (national military strategy)

436 Арзуманян Рачья (эксперт ЦСОиП) – Новые задачи Пентагона в «Стратегическом руководстве по обороне». Глобальные проблемы, 25 января 2012. [http://www.csef ru/studies/defence/projects/new_military/articles/2590/

437 Department of Defense. «Defense Strategic Guidance Briefing from the Pentagon,» Presenter: President Barack H. Obama, Secretary of Defense Leon E. Panetta, and Chairman of the Joint Chiefs of Staff Gen. Martin E. Dempsey, January 5, 2012 («Guidance Briefing»)

438 Альфред Тайер Мэхэн (Alfred Thayer Mahan; (1840-1914) – американский военно-морской теоретик и историк, контр-адмирал, один из основателей геополитики. [ru.wikipedia.org› wiki/Мэхэн, _Альфред_Тайер]

439 Posen, Barry R. – Command of the Commons: The Military Foundation of U.S. Hegemony. International Security, Vol. 28, No. 1, Summer 2003, pp. 5-46. 12 January 2011, контроль которого, фактически, был равносилен «владению морем» [Kennedy, Paul M. – The Rise and Fall of British Naval Mastery. London: MacMillan, 1983

440 Posen.

Вторым важным моментом, относящимся к геостратегии, следует признать тезис, что США стоят перед «необходимостью перебалансирования/переориентации на Азиатско-тихоокеанский регион»[441]. Речь, идёт о геостратегической переориентации и формировании долгосрочных трендов, разворачивание которых будет происходить не только на протяжении последующих десяти лет, но всего 21 века.


Источник: riseofevil.ru

Арабское пробуждение по-американски.

На Ближнем Востоке среда безопасности во многом будет формироваться Арабским пробуждением (Arab Awakening).

США по-прежнему остаются гарантом безопасности Израиля. Первоочередной целью является воспрепятствовать ядерной программе Ирана и «противодействовать его дестабилизирующей политике». Решать свои задачи в регионе США намерены со своими союзниками, в первую очередь, Израилем, и в сотрудничестве со странами Совета по сотрудничеству стран Персидского залива (Gulf Cooperation Council). В документе не упоминается Турция. Хотя она и не упоминается, на практике, в ходе выполнения предусмотренных в документе мер по передаче ряда задач союзникам по НАТО, в соответствии с Балканскими агентурными данными сейчас решается вопрос о передаче Турции крупнейшей в Европе базы США в Косово – Бон Стил.

Изменения предусматриваются также в Европе и НАТО. В изменяющейся среде безопасности, сокращении ресурсов, которые могут быть выделены на оборону, США вынуждены сократить объемы своего военного присутствия на европейском ТВД.

Из классического геополитического инструментария стоит упомянуть намерение снизить размер ядерных сил, причем во всех компонентах ядерной триады. Хотя можно полагать, что одним из элементов ядерной триады полагается аэрокосмическая составляющая, в принятой США концепции геоцентрического ТВД прямо предусмотрено применение ядерного оружие в магнитосфере и в заряженных оболочках ближнего космоса (генерал Келер). Кроме того, в планах США по защите от метеоритной угрозы одной из мер является разрушение космического тела ядерными взрывами[442].

Из новых угроз среды безопасности 21 века, которым будет уделено особое внимание, важным представляется намерение противодейство-

---

441 Lee R. – The Far East between Russia, China, and America, Foreign Policy Research Institute. E-Notes, July 2012; Lukin A. – Russia and America in the Asia-Pacific: A New Entente? Asian Politics and Policy, 2012, Vol. 4, №2, p. 100

442 Рухлев В. Ф., Спектор В. Н., Пивоваров О. Н. и другие – Методы и пути решения кометно-астероидной и экологической безопасности России. Труды МАН ПНБ. М., том 2, вып. 1, с. 174

Источник: www.liveinternet.ru

Поль Джозеф Вейц

вать новым угрозам, исходящим от негосударственных акторов, неконтролируемых территорий, групп и личностей. Имеется в виду высокая вероятность вмешательства в киберкосмическое пространство США внешних (как негосударственных, так и противостоящих государственным) кибероператоров, что соответствует и мнению авторов, основанному на южно-кавказских данных [443].

Национальная безопасность, военное строительство и стратегия США.

В документе[444] определяются стратегические приоритеты, в качестве которых называются десять задач, которые должны решать Объединённые силы:

- контртерроризм и иррегулярная война;
- сдерживание и отражение агрессии;
- проецирование мощи, несмотря на вызовы, призванные блокировать доступ/территорию;
- меры противодействия оружию массового поражения (ОМП);
- эффективное оперирование в киберпространстве и космосе;
- поддержание безопасного, обеспеченного и эффективного ядерного сдерживания;
- защита внутренней безопасности и предоставление поддержки гражданским властям;
- осуществление стабилизирующего присутствия;
- проведение операций по стабилизации военно-политической обстановки и контрповстанческих операций/conduct stability and counterinsurgency operations;
- проведение операций по ликвидации последствий стихийных бедствий и катастроф, гуманитарных и прочих операций[445];

Оценивая среду безопасности и формулируя миссии, к выполнению которых должны быть готовы США, документ подчёркивает невозможность охватить все возможные угрозы.

В документе подчёркивается необходимость проводить различие между инвестициями, призванными сформировать отклик на проявленные

443 Спектор В.Н. – Служебная записка в СБ РФ, копия: в ФСБ РФ, ноябрь 2011, 3 с.

444 DoD ... «Guidance»

445 Позен, Кеннеди

и ещё не проявленные угрозы. Это предполагает способность изменять проводимый курс, формируя отклик на новые угрозы, то есть адаптабельность. Процесс адаптации может определяться различными факторами, которые могут быть как неизвестными и шоковыми по своей природе, так и результатом «эволюции в сферах стратегии, операционного искусства, экономики и технологии». В таких условиях любые нововведения должны бережно относиться к уже накопленному опыту и выстраиваться на принципе «обратимости» (reversibility) изменений[446], по принципу «конверсии – реконверсии».

Предполагаемые изменения не должны приводить к падению боеспособности вооружённых сил США. После завершения вывода войск из Ирака и затем Афганистана «мы должны будем предпринять дополнительные меры, чтобы сохранить и выстроить ключевые направления в сетевой войне (networked warfare)»….

Параллельно Минобороны и военное сообщество США в целом должны предпринимать усилия по разработке новых концепций планируемых операций. Это предполагает внедрение в Минобороны культуры изменений, балансируя между необходимостью снижать затраты и императивом устойчивого развития ключевых направлений в долгосрочной перспективе.

Краткий анализ. Геополитические и геостратегические аспекты.

Если геополитические тренды и намерения США хорошо исследованы, то смещение фокуса на Азиатско-тихоокеанский регион требует пристального внимания. Необходимость такой переориентации обосновывается, в частности, в работах военного геостратега Томаса Барнетта (Thomas P. M. Barnett). В конце 2011 года Барнетт предложил обновлённый взгляд на идеи и подходы, высказанные в известной работе «Новая карта Пентагона»[447], и новую «новую карту» лекций[448].

Однако, чтобы и далее обеспечивать доминирование в глобальном пространстве и осуществить переориентацию на новый регион, США должны расширять возможности глобального проецирования мощи, в первую очередь, военно-морской мощи. Каким образом можно осуществить столь масштабные изменения на фоне сокращения военных расходов не совсем ясно.

---

446 Позен, Кеннеди

447 Barnett, Thomas P.M. – The Pentagon's New Map: War and Peace in the Twenty-First Century. Putnam Publishing Group. 2004

448 «Мир согласно Барнетта. Новая карта Пентагона»/«The World According to Tom Barnett», brief, (Pentagon's new map))

Источник: en.wikipedia.org

Томас П. М. Барнетт

Кроме того, чтобы осуществить переориентацию на другой регион, США должны добиться стабильности на Ближнем Востоке и в дуге нестабильности в целом, что выглядит маловероятным, учитывая приход к власти исламистских режимов, несущих с собой угрозу для союзников США в регионе и для Европы, где становится крайне вероятным провал затеянного ещё Саркози проекта транс-средиземноморского сотрудничества Магриб – ЕС.

Сокращение американского присутствия и, как следствие, некоторых элементов зонтика безопасности США в Европе должны привести к изменению роли США в Атлантическом альянсе. Готовы ли США к такой постановке вопроса? Уменьшение удельного веса США на европейском ТВД должно сопровождаться увеличением военного потенциала других европейских стран. Да, сегодня Европа экспортирует безопасность, однако процессы на южном фланге НАТО далеки от стабильности. В состоянии ли будут европейские страны защитить себя без широкой поддержки США и без повышения военных расходов? Предлагаемая коренная трансформации системы безопасности Европы и НАТО это, помимо всего прочего, большие расходы, которые выглядят маловероятными на фоне финансового кризиса. Безусловно, США, продолжая финансово-экономическую, энергетическую и информационную войну с Евросоюзом готовы наложить дополнительное обременение передачей ему военных функций НАТО.

Национальная безопасность, военное строительство и стратегия.

Список миссий в руководстве[449], которым будет отдаваться приоритет, расширен и во многом совпадает со списком «Четырёхлетнего обзора обороны 2010 года/2010 Quadrennial Defense Review». Однако есть и очевидные изменения, наиболее значительным из которых является акцентирование понижения роли контрповстанческих миссий, являвшихся до этого главным стратегическим приоритетом Пентагона. Новая среда безопасности и мировой кризис вынуждают США отказаться от, как оказалось, столь дорогих и неподъёмных затрат на большие контрповстанческие операции.

В стратегическом руководстве отсутствует и конструкция «двух конфликтов», предполагающая способность США вести одновременно два

449 DoD ... «Guidance»

больших региональных конфликта. Документ придаёт особое значение проблемам гармонизации усилий ведомств и агентств, участвующих в решении задач национальной безопасности. В связи с несбалансированностью межведомственных взаимодействий Пентагон зачастую вынужден брать на себя задачи, которые должны были быть приоритетными направлениями деятельности других ведомств.


Источник: ja.wikipedia.org

Эрик Тор Олсон

Формирование отклика на угрозы новой среды безопасности требует создания сравнительно небольших, но хорошо экипированных вооружённых сил, развитие которых предполагалось в рамках «трансформации военной сферы». Большая часть приоритетных миссий стратегического руководства должна выполняться силами специального назначения, в первую очередь корпусом «морской пехоты», что довольно сложно реализовать. Помимо затрат на уменьшение численности вооружённых сил, изменения структуры вооружённых сил и её оптимизацию, количественный рост сил специального назначения не может превышать 3-5% в год и ограничивается организационной структурой, учебным процессом и пропускной способностью учебных центров[450].

Проведенный краткий анализ позволяет говорить о двух пластах, связанных с реализацией положений стратегического руководства, которые на самом деле являются «стратегической точкой разворота» (strategic turning point) в военной политике и стратегии США. Причём мышление, которое за ним кроется, не является революционным по своей природе, и не предлагает «рубить с плеча», как это имело место при переориентации Пентагона на контрповстанческие операции. Документ старается найти баланс и придерживается эволюционного подхода к развитию доктрин, идей, вокруг которых выстраивалась военная машина США на протяжении последних десятилетий.

Предлагаемые сокращения численности вооружённых сил предполагается компенсировать усилением остающихся войск передовыми военными технологиями, ВиВТ. Можно сказать, что подходы и концепции «революции в военном деле», «трансформации военной сферы», «сетевых сил» возвращаются. Другим важным моментом следует признать акцентирование процессов адаптации и целостного подхода к сфере национальной безопасности, необходимость гармонизации усилий всех элементов национальной

450 Olson, Eric T. (Admiral, USN, Commander, U.S. Special Operations Command) – Special Operations: Context and Capabilities in Irregular Warfare. Joint Force Quarterly (JFQ), Issue 65, First Quarter 2010, pp. 64-70

мощи при достижении целей национальной политики. Подход, который развивался в рамках сетецентричных концепций, базирующихся на достижении ожидаемых эффектов[451].

Таким образом, военные круги, понимая, что сокращения военного бюджета и вооружённых сил неизбежны, стараются сделать их наименее болезненными. Задача по сокращению расходов, скорее всего, была бы эффективно решена, будь поручена военным кругам. Тем не менее, без сомнения, команда, разрабатывавшая документ, ответственно подошла к делу и разработала добротный с военно-стратегической и геополитической точек зрения документ.

«Однако сама природа вопроса в данном случае является политической, и его решение будет диктоваться политическими факторами, предпочтениями и интересами. Проблемной частью документа является не текст и предлагаемые действия, а то, каким образом руководство будет инициировать выполнение положений документа, – шаг который является политическим по своей природе. Документ демонстрирует своего рода консенсус в военном истеблишменте США и подводит политиков к необходимости принятия решений, которые позволили бы США сохранять и далее свое военное и геополитическое преимущество в мире. Однако будет ли консенсус принят американским обществом или США выберут другой путь развития и другие приоритеты? Вопрос, который будет ставиться и решаться после президентских выборов, и уже не в военной сфере» [452].

4.9. ВНЕШНЯЯ ЭКСПАНСИЯ В ОБРАЗОВАТЕЛЬНУЮ СФЕРУ КАК СРЕДСТВО ФОРМИРОВАНИЯ ПЛАЦДАРМА ДЛЯ ПЕРЕФОРМАТИРОВАНИЯ БАЗОВЫХ ЦЕННОСТЕЙ

Качественный уровень образовательных процессов государства есть один из главных критериев его цивилизационного развития и позиционирования на мировой арене. Даже базовые знания граждан могут иметь узкую или расширенную интерпретацию, что существенно влияет на уровень подготовки и дееспособности специалистов и их КПД. Это касается отраслей знаний в фундаментальных науках. Гуманитарные и общественные науки в целом ряде случаев ориентированы на базовое, мировоззренческое восприятие обучаемого, связанное с историческими, этническими, геополитическими, конфессиональными и иными особенностями ареала. В данном слу-

451 Арзуманян, Рачья В. – Сложное мышление и Сеть: парадигма нелинейности и среда безопасности 21 века. Ереван: Научно-образовательный фонд «Нораванк», 2011

452 Арзуманян, Рачья В. – Сложное мышление и Сеть: парадигма нелинейности и среда безопасности 21 века. Ереван: Научно-образовательный фонд «Нораванк», 2011

чае процесс обучения призван сформировать гражданина, патриота, апологета принципов исторического развития и государственного строительства, являющихся, фундаментальными для данного государства, национальности, расы. Образовательные процессы в государстве – есть костяк его развития и идентичности. Принудительное переформатирование этих процессов равносильно переформатированию глобальных, фундаментальных, принципов, определяющих жизнедеятельность государства. Если данное переформатирование имеет целью разрушение исторической, идеологической, понятийной базы воспитательных, мировоззренческих связей в обществе, оно становится идеальным орудием агрессии против этого государства, цель которой – снижение его влияния на мировой арене, захват его ресурсов и рынков, смена геополитической ориентации, либо полное его уничтожение, как субъекта мировой геополитики.

Историко-патриотическое воспитание в образовательном процессе

История государства, литература, искусство, культура, этно-конфессиональная совместимость и терпимость (толерантность) в социально-общественных отношениях – вот неполный перечень того, на что позиционировано начальное образование. Патриотическое воспитание, до определенной степени, является гарантией сохранения идентичности государства. Не титульные нации, ни основные конфессиональные приоритеты не могут быть достаточной гарантией государственной идентичности, особенно в многонациональном и многоконфессиональном государстве, без национальной идеи, базирующейся на чувстве гордости за свою страну. Герб, флаг, гимн – данными символами государства можно обозначить «национальную идею», формирующую в сознании граждан устойчивый патриотический настрой. Данное чувство формируется на многофакторной основе. Особую роль играет незыблемость исторических событий в процессе формирования и становления государства, а фальсификация истории государства является тягчайшим преступлением. Фальсификация, инициированная извне, может расцениваться как акт неприкрытой агрессии. Массовое восприятие непосредственно зависит от образовательного уровня каждого гражданина, и в этой связи, начальное образование приобретает особое значение. Социально-экономический уровень развития общества формирует предпосылки для предоставления условий образовательного охвата слоев населения. В этой связи обязательное всеобщее начальное образование является предпосылкой к перспективному росту мощи государства. История развития государства, его роль в формировании глобальных исторических процессов, вклад в мировую культуру, литературу, искусство, достижения в области науки, роль армии и правоохранительных структур

в формировании мирового имиджа государства – вот те столпы, позволяющие форматировать мировоззрение новых поколений, призванных сохранить и усилить роль и имидж государства в мировом сообществе. Внешнеполитический курс государства, как правило, является одним из определяющих векторов в формировании мировоззрения молодежи и подрастающего поколения. В связи с этим популяризация национальных и государственных ценностей снизит риски влияния внешних культурологических и идеологических факторов на сравнительное сознание граждан.

Снижение контроля, частичное либо полное пренебрежение вышеозначенных параметров со стороны государства становится причиной внешней экспансии в эти процессы, последствия которой предсказуемы.

Этно-конфессиональный фактор в образовательном процессе

В многонациональном и многоконфессиональном государстве, важнейшую роль играет духовная ассимиляция и воспитание терпимости (толерантности) в обществе. Основы, конечно же, лежат в исторических, культурных и социальных процессах внутренней политики государства и заключается в уважительном, равноправном отношении к этно-культурным ценностям, в правильно регулируемых процессах миграции внутри страны, и взвешенном распределении административных и управленческих полномочий. Однако очень большую роль в данном случае играет образовательный процесс, и духовная ассимиляции на базе общих ценностей и государственного патриотизма. Важно выставить приоритеты обязательного ценза образования, с использованием государственного языка. Сохранение этнической идентичности это внутреннее дело этноса, и оно, несомненно, должно поощряется государством, однако оно не должно противоречить основополагающим принципам ареала совместного проживания. В условиях свободной миграции населения индивид, воспитанный в моноэтническом обществе, будет испытывать ряд существенных затруднений, более того он будет создавать затруднения в среде нового обитания. В этой связи образовательные процессы призваны нивелировать грань между этно-конфессиональной принадлежностью и патриотическим восприятием большого ареала обитания (государства) гражданином которого индивид является.

Нарушения баланса в этно-конфессиональной сфере в процессе воспитания гражданина, может стать плодотворной почвой для развития национал-шовинизма, сепаратизма, радикализма, смертельно опасных процессов для любого государства.

В ряду стратегически важных социальных процессов особую роль выполняют процессы сосуществования различных социальных, этнических,

конфессиональных групп. Цель государства – недопущение возникновения диссонирующих факторов в этих процессах. Потенциальный противник государства рассматривает те же процессы как плацдарм для катализации агрессивных реакций, способных нанести максимальный ущерб процессам государственного строительства. Посредством использования информационно-пропагандистских методов воздействия на сознание внешних и внутренних потенциалов влияния, финансовых, идеологических, административных рычагов, инициируется процесс либо претензии на приоритеты, либо недовольство своим положением и статусом в среде этно-конфессиональных образований единого государства. Радикальные толкования религиозных догм, образования новых агрессивных псевдо религиозных течений, в арсенале данных агрессий занимают основополагающее место. Как правило, основной отличительной чертой этносов является конфессиональная принадлежность, и именно этот спектр общественного консолидирующего фактора становится предметом информационно-идеологической агрессии.

Импорт образовательных и культурологических ценностей в стратегически важные социальные процессы

Каким образом осуществляется агрессивная экспансия в образовательные процессы государства? Во-первых, такого рода экспансия возможна только в государствах с нестабильной системой управления, или переживающих сложные времена, вследствие кардинального изменения стратегии развития. На примере развала СССР и двух с лишним следующих десятилетий можно выстроить классическую модель уничтожения государства и государственности. Влияние потенциального противника на процессы, происходящие в государстве, было чрезвычайно высоко. Под видом реформ, ангажированные реформаторы уничтожили основополагающие столпы государства – обороноспособность, промышленность, сельское хозяйство, национальный патриотизм, науку и образование. Школьные реформы были ориентированы на снижение образовательного уровня подрастающего поколения. Часы обучения истории, русского языка и литературы были сокращены в учебной программе до минимума, извращены и изменены многие факты, события и основополагающие принципы. Заказчик щедро платил, и в результате были уничтожены целые сегменты образовательного процесса. Профессионально-технические училища и техникумы были вычеркнуты из образовательного процесса. Вузы стали коммерческими предприятиями, которых и в настоящее время неоправданно много. Уровень образования в вузах не отвечал требованиям общества. Миллионы выпускников вузов не только не работают по специальности, но и по уровню знаний не соответствуют требованиям

работодателя. Культ гуманитарных наук нивелировал значимость и востребованность инженерно-технических, физико-математических и прочих точных наук. Миллионы юристов, экономистов, специалистов по связям с общественностью и управлению персоналом наводнили Россию.

Особого внимания заслуживает религиозное образование. Если с Русской православной церковью в плане подготовки кадров духовенства все имеет устоявшиеся основы, то в случае с мусульманской диаспорой все оказалось гораздо сложнее. Практическое отсутствие в СССР серьезных образовательных учреждений для подготовки исламского духовенства породило в данном процессе спонтанность. Этим не преминули воспользоваться противники России. В короткий срок во многих регионах России с достаточно большими мусульманскими диаспорами появились медресе (начальное учебное заведение), которые финансировались за счет средств поступающих из-за рубежа. В Башкирии, а затем и в других регионах России начали официально функционировать турецкие медресе и колледжи, профилированные на обучение духовенства. Все мусульманские духовные управления, а таковых было несколько сот, рекрутировали шакирд, (молодых людей от 13 лет, стремящихся стать священнослужителями), которые отправлялись учиться в страны исламского мира за счет зарубежных грантов. Параллельно в России возводились сотни и тысячи мечетей. Таким образом, исламское духовное обучение в России полностью контролировалось из-за рубежа. По истечению 2-4 лет, «специалисты», подготовленные и обученные за границей стали духовными пастырями многомиллионной диаспоры мусульман России.

Большинству обученных за рубежом духовных наставников мусульман России в процессе обучения прививались основы знаний не совместимые с веками формировавшейся в России идеологией. Учебные программы исламских вузов ряда стран, в которых обучались российские шакирды, были основаны на радикальном подходе и неприятии других конфессий. Вольно или невольно в сознание студентов закладывались, в том числе, крайне радикальные знания и экстремистские настроения. При полном отсутствии контроля со стороны российских властей стала развиваться чуждая тенденция развития ислама в России. На рубеже второго тысячелетия эта тенденция начала давать свои результаты. Сегодня мы имеем обширную сеть джамаатов от восточной Сибири до западных границ. Однако программа обучения, заложенная в сознание многих духовных пастырей ислама России, предусматривает множество различных вариантов направленности действий, в соответствии с изменениями социально-политических и иных тенденций развития ситуации в стране.

Таким образом, резкое снижение образовательного и воспитательного уровня населения России, переориентация приоритетов от исторических

и социально-политических устоев, бесконтрольность в сфере духовного воспитания и образования российских граждан, становятся плодотворной почвой для агрессивной экспансии извне. Цель этой экспансии – разобщение общественных связей, разрушение инфраструктур, и, в конечном счете, не военный захват ресурсов, которыми Россия, по мнению Запада, обладает не справедливо.

Частичное либо полное нивелирование роли государства в истории развития человеческой расы в образовательных процессах

Свободное интерпретирование исторических событий и фактов уже само по себе преступление против человечества, а когда оно касается отдельно взятого государства – это акт неприкрытой агрессии. Постперестроечный период в России был отмечен резким снижением, как уровня преподавания, так и контроля со стороны государства за его качеством. Учебники истории и географии утратили единый государственный стандарт, появилось новое явление – рекомендации изучения предмета по авторам. Порой в соседних школах изучали историю в интерпретации разных авторов, причем по рекомендации чиновников из министерства образования, Гороно или просто директора школы. Как и кем составлялись эти учебники, мало кого интересовало. Порой тендеры на составление и поставку учебников и методической литературы выигрывали организации, не имеющие никакого отношения к народному образованию и науке вообще. Этим активно пользовались потенциальные противники России. Так из школьных программ исчезали или сокращались до минимума наиболее важные и знаковые для российской истории события. В ряде случаев эти же события подавались в искаженной, занижающей роль России форме. В отличие от чиновников от образования, идеологический враг уделял формированию мировоззрения новых поколений россиян огромное значение и неограниченные средства. В том же русле шла атака на русский язык и русскую литературу. К 2014 году стало понятно катастрофическое положение преподавания русского языка и русской литературы в начальном, среднем и высшем образовании страны. Для того чтобы обратить на это внимание потребовалось личное вмешательство президента России В.В. Путина.

Мало кто связывает снижающийся уровень образования с безопасностью страны. Однако это один из самых важных аспектов разрушения перспективных потенциалов государства, и он должен рассматриваться в одной плоскости с развитием ВПК и вооруженных сил, с общественной и государственной безопасностью и контрразведывательной деятельностью. Наряду с мощным информационным потоком, популяризирующим западные ценно-

сти, агрессивная экспансия в сферу народного образования может оставить государство без апологетов уже в ближайшем будущем. Безграмотность, бездуховность, отсутствие национального, государственного патриотизма уже сейчас наводняют молодежную среду людьми, не разделяющими и не понимающими основы государственности. Культ материальных ценностей и псевдо демократии, культ насилия, как средства достижения своих меркантильных интересов поражает умы подрастающего поколения. Напрочь изжиты массовые молодежные патриотические движения, именно массовые, такие как всесоюзные октябрятские, пионерские и комсомольские организации. А именно массовость и непрерывная преемственность патриотического воспитания есть гарантия сохранения национальной и государственной идентичности и целостности.

Военно-патриотическое воспитание молодежи еще один аспект массового образования, который был нивелирован за ненадобностью. Вот только эта ненадобность выгодна совершенно конкретным кругам на Западе. Военно-патриотические клубы, ДОСАФ (добровольное общество содействия армии и флоту), предмет школьной программы «Начальная военная подготовка» (НВП) только к 2014 году стали возрождаться и то не повсеместно. На протяжении десятилетий в обществе формировалась устойчивая неприязнь к всеобщей обязательной воинской обязанности. Одним из следствий этого стало сокращение службы в армии по призыву до одного года. Молодой человек, не знающий даже азов военной подготовки, за один год не в состоянии стать воином, освоить сложную военную технику, и подготовиться к защите Родины. И это следствие разрушения образовательных процессов в государстве. Какую бы технику не создал возрождающийся ВПК России, без обученного солдата и сержанта это всего лишь железо.

Из выступления Аллена Даллеса перед сотрудниками ЦРУ США в 1945 году: «Мы бросим все, что имеем, все золото, всю материальную мощь и ресурсы на оболванивание и одурачивание людей. Человеческий мозг, сознание людей способны к изменению. Посеяв в России хаос, мы незаметно подменим их ценности, на фальшивые… Мы найдем своих единомышленников, своих помощников и союзников в самой России. Эпизод за эпизодом будет разыгрываться грандиозная трагедия гибели самого непокорного на земле народа, окончательного угасания его самосознания… Мы будем расшатывать, таким образом, поколение за поколением… Мы будем драться за людей с детских, юношеских лет, будем всегда главную ставку делать на молодежь, станем разлагать, развращать, растлевать ее. МЫ СДЕЛАЕМ ИЗ НИХ КОСМОПОЛИТОВ».

Последователи Аллена Даллеса дождались своего часа, сегодня мы близки к воплощению его идей в жизнь. Идеологическая война против России и ее

союзников ведется не первое столетие, технологии агрессии совершенствуются. В этой связи аспектам воспитательных и образовательных процессов необходимо предать государственный статус наряду с безопасностью и независимостью.

Образование за рубежом, чему мы должны научиться у них, и для чего?

Практика последних двух десятилетий – давать своим детям образование за рубежом, сформировалась в самых отсталых и малоразвитых странах. Мало того, что она ущербна и оскорбительна по отношению к своей Родине, она крайне опасна. Особенно прискорбно то, что своих детей на обучение за рубеж отправляют представители самых влиятельных политических и бизнес кругов России. Эти представители «элиты общества» своими действиями показывают презрение к уровню образования и воспитания, который может дать их Родина. На Западе с большим одобрением относятся к тому, что дети политиков, военных, бизнесменов, едут учиться к потенциальному противнику. Для российских абитуриентов созданы идеальные условия поступления и зачисление на обучение. Основной критерий не знания, и даже не платежеспособность, а положение родителей в российском обществе. Каждый такой студент – потенциальный материал для формирования угодных западу фигур влияния в России.

Тысячи западных компаний, осуществляющих свою деятельность на территории России, отдают приоритеты в кадровой политике претендентам, получившим образование за рубежом. Более того, подобная кадровая ориентация прослеживается и в российских предприятиях и учреждениях, в том числе и на самом высшем уровне. Дети высокопоставленных родителей, обучающиеся за рубежом, требуют больших финансовых расходов, обеспечения недвижимостью. Родители открывают счета в зарубежных банках, покупают недвижимое и иное имущество. Многие дети высокопоставленных родителей попадают в истории, которые могут повлечь за собой уголовную ответственность. Родители вынуждены спасать своих детей. Но людям, которые решают для родителей вопросы по спасению их непутевых детей, деньги не нужны… Как правило, такие истории не попадают даже в западную прессу. А продолжение этой истории может стать одним из тысяч эпизодов в схеме разрушения и уничтожения Родины этих студентов и их родителей. Выше уже был приведен пример импорта исламского образования – нам навязывают схемы обучения по западному образцу. Элитные лицеи и частные школы с гордостью декларируют, что преподавательский состав получил образование в Гарварде, Сорбонне и т. д.

Созданный Дж. Соросом в России институт «Открытое общество» в конце 1998 г. начал реализацию Мегапроекта «Развитие образования в Рос-

сии», который рассчитан на пять лет. На 1999 г. предполагалось на одну лишь целенаправленную переподготовку сельских преподавателей выделить от 100 до 150 млн. долл. Можно себе представить, какова «целенаправленность» этой переподготовки. Сельских учителей России, генетический аппарат нашей культуры, которую лелеяли Лев Толстой и Ушинский, теперь будут натаскивать культуртрегеры Сороса, ненавистники российской государственности.

И как следствие подобной экспансии в российское образование – в умах российской молодежи не осталось места педагогам русской школы. Постепенно забываются патриархи русской педагогической школы Ушинский, Пирогов, Толстой, Рачинский, Бунаков, Макаренко, Крупская, Стоюнина, Лазурский, Нечаев, Музыченка, Чехов, Фортунатов, Сухомлинский. Их место занимают Ж. Мажо, Л. Кро, Ж. Капеля (Франция), Г. Кэвелти А. Комбс, А. Маслоу, К. Роджерс (США) и др.

Информационно-психологическая агрессия – один из самых изощренных способов геополитического переустройства мира. Эта агрессия не предполагает апелляции к международному праву, от нее нет защиты извне. Противостоять подобного рода угрозе возможно только концентрацией внутренних усилий, путем переоценки экспортированных либо навязанных ценностей. В противном случае все возрастающая зависимость может перерасти в рабство.

ГЛАВА 5.
РОЛЬ РАЗВЕДКИ И КОНТРРАЗВЕДКИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БОРЬБЫ (ЗНАЧИМОСТЬ АГЕНТУРНОГО ПОДТВЕРЖДЕНИЯ ДАННЫХ НАЦИОНАЛЬНЫХ СРЕДСТВ КОНТРОЛЯ И НАБЛЮДЕНИЯ).

Значимость традиционных форм разведки и контрразведки перманентно снижалась с развитием информационных технологий. По мере перехода от парадигмы двумерной войны к трёхмерной и к её постепенному замещению пространственно-темпоральными средствами и методами ведения войны на геоцентрическом, а в относительно недалёком будущем и на гелиоцентрическом ТВД (конкуренция за освоение Луны, Марса и его спутников и за позиционирование космических станций на защищённых геостационарных орбитах) неизбежны и изменения как разведки, так и контрразведки.

Концепция ситуативной осведомлённости (situational awarness) поглотит все направления и виды как разведывательной, так и контрразведывательной деятельности, также как геоцентрический ТВД поглощает все домены современных вооружённых сил: сухопутный, морской, аэрокосмический и только народившийся кибернетический виртуальный домен современных вооружённых сил.

Разведывательные службы.

Роль разведывательных служб, во-первых, значительно расширится, включив в сферу стратегических интересов все области военной, хозяйственной, финансовой организации и социальной ситуации в большинстве государств мире, способных односторонне или в составе коалиций представлять угрозу безопасности страны. При этом необходимо учитывать, что в условиях геоцентрического ТВД в рамках концепции ситуативной осведомлённости информация перестаёт подразделяться на стратегическую и тактическую – она должна быть достижимо полной по всему объёму оперативного пространства. Это потребует освоения технологии генерирования

виртуальных агентов и атакующих средств (вирусов, закладок, виртуальных «бомб» и т. п.), внедряемых с помощью информационного и кибернетического оружия в компьютерные (связные и управленческие) сети потенциального противника, как для нарушения работы систем связи и управления, так и для прямого получения информации.

Важнейшей задачей всех разведывательных служб, как политических, так и военных становится установления способов генерации нуля, планируемого облика и смысла войны в странах, представляющих непосредственную угрозу национальной безопасности России, а также выполнение ранжировки вероятных угроз на основе научного анализа получаемых разведывательных данных.

Основным координирующим компонентом сил на геоцентрическом ТВД является информационное противоборство, использующее методы внедрения дезинформации и ложной информации в киберпространство. В связи с этим чисто инструментальные методы разведки так называемыми национальными техническими средствами наблюдения могут оказаться недостаточно надёжными, и резко возрастает значимость агентурного фактора для осуществления корректного и надёжного анализа реальных угроз национальной безопасности России.

Этот вывод подтверждается и тем, что ЦРУ США, традиционно отдававшее предпочтение национальным средствам наблюдения и контроля и анализу достижимо больших массивов публикуемых в открытой печати материалов и документов, вплоть до муниципального уровня, с 1985 года стало резко усиливать агентурный сектор, как за счёт собственных засылаемых агентов, так и расширением вербовки для создания национальных агентурных сетей в интересующих ЦРУ странах.

На органы военной разведки, по-видимому, будут возлагаться функции определения зон уязвимости потенциальных противников, как на суше и в мировом океане, так и в космосе и обеспечения информационных и иных стратегических контрударов по этим зонам, а также проведения направленных диверсий и актов саботажа на территории потенциальных противников, не исключая и использование террористических групп и организаций, враждебно настроенных по отношению к изучаемой стране (стратегическая военная разведка), с включением протестных настроений более или менее широких масс местного населения (совместно с СВР).

При этом, разумеется, в полном объёме сохранятся и традиционные задачи сбора информации, агентурной проверки данных, создания нелегальных резидентур, вербовки агентов и организации агентурных сетей, внедрение на месте в коммуникационные сети и другие виды разведывательной деятельности на территории стран – потенциальных противников.

Наиболее уязвимыми элементами всех видов разведывательной деятельности являются доставка потребителю добытой информации и необходимость организации постоянного оперативного контакта с завербованными агентами. Как нм странно, но правильно организованное использование технологий геоцентрического ТВД, включающее создание системы «электронных сит» на основе твердотельных или молекулярных сверхрешёток, резко снижает, в идеале сводя к нулю, уязвимость по этим элементам разведывательной деятельности, также как уже упоминавшееся снижение уязвимости по параметрам несанкционированного доступа к системам связи и управления.

Источник: www.pinterest.com

Лео Эсаки

Источник: coefs.uncc.edu

Рафаэль Тсу

Твердотельные сверхрешётки и технологии их получения и использования разрабатывались в Японии и США. Наиболее продвинутыми были работы японского исследователя, проф. Лео Эсаки[453] и проф. Рафаэля Тсу [454], ставших первооткрывателями твердотельных сверхрешёток [455]

В Википедии дается определение «В физике полупроводников под термином сверхрешётка принято понимать твердотельную структуру, в которой помимо периодического потенциала кристаллической решётки имеется дополнительный потенциал, период которого существенно превышает постоянную решётки. Различают следующие виды сверхрешёток:

композиционные сверхрешётки – эпитаксиально выращенные периодически чередующиеся тонкие слои полупроводников с различной шириной запрещённой зоны;

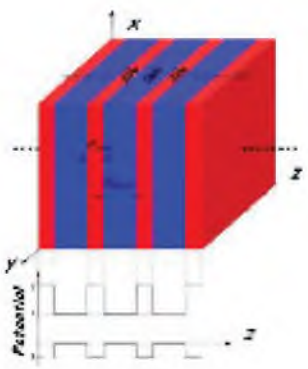
легированные сверхрешётки – периодический потенциал образуется чередованием ультратонких слоёв n- и p-типов полупроводника, которые отделяются друг от друга нелегированными слоями;

спиновые сверхрешётки – образованные периодическим чередованием слоёв одного и того же полупроводника: одни слои легируются

453 Лео Эсаки (яп. 江崎 玲於奈 Эсаки Рэона, известен также как Рэон Эсаки или Леон Эсаки; 12 марта 1925) японский физик, лауреат Нобелевской премии по физике 1973 года.

454 Рафаэ́ль Тсу (англ. Raphael Tsu) американский ученый китайского происхождения. Книга Р. Цзу Фамилию Тсу (Tsu) принял после переезда на запад из Китая, где имел фамилию Чжу (Zhu).

455 R. Tsu and L. Esaki (). «Tunneling in a finite superlattice». Applied Physics Letters, 1973, vol. 22, p. 562. DOI: 10.1063/1.1654509



Сверхрешётка GaAs/AlAs и профиль потенциала электронов проводимости и вакантных состояний вдоль направления роста структуры (z).

немагнитными примесями, а другие – магнитными – без магнитного поля энергетическая щель во всей сверхрешётке постоянна, периодический потенциал возникает при наложении магнитного поля;

сверхрешётки, сформированные в двумерном электронном слое (например в системе МДП: металл-диэлектрик-полу проводник) периодической модуляцией плоскости поверхностного заряда; сверхрешётки, потенциал в которых создаётся периодической деформацией образца в поле мощной ультразвуковой или стоячей световой волны.

Наряду со сверхрешётками из полупроводников, существуют также магнитные сверхрешётки и сегнетоэлектрические сверхрешётки».

Показателен уже упоминавшийся факт, что до середины 90-х годов XX века все патенты, связанные с получением и применением сверхрешёток, выкупались в собственность правительства США.

Молекулярные сверхрешётки изначально получались на основе комплексов типа слоистых ассоциатов с частичным переносом заряда средней силы[456] сокристаллизацией из раствора донорных и акцепторных компонент при термодинамически равновесных условиях (температура – T = const, давление – P = const, концентрации C_D и C_A = const) в специально сконструированном реакторе[457].

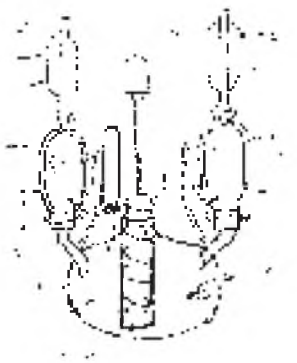
---

456 Спектор В. Н. – Константы нестойкости комплексов производных хинолина и акридина с солями производных хинолиния и акридиния. В кн.: Материалы Всесоюзной конференции по термодинамике органических соединений. Изд. ГГУ. Горький, 1973, с. 131; Соборовер Э. И., Мухина Г. Н., Пахомов Л. Г., Спектор В. Н. – Константы нестойкости комплексов производных хинолина и акридина с солями производных хинолиния и акридиния. Журнал физической химии, 1975, т. 49, № 7, с. 1696; Спектор В. Н. – Влияние внешних факторов на генерацию и движение носителей тока в органических полупроводниках класса комплексов с переносом заряда типа слоистых ассоциатов. В кн.: «Электроника органических материалов». Изд. «Наука». М., 1985, с. 218; Шкловер В. Е., Пахомов Л. Г., Спектор В. Н. – Структура акридинпроизводных – компонентов комплексов с переносом заряда типа слоистых ассоциатов. В кн.: «Электроника органических материалов». Изд. «Наука». М., 1985, с. 134

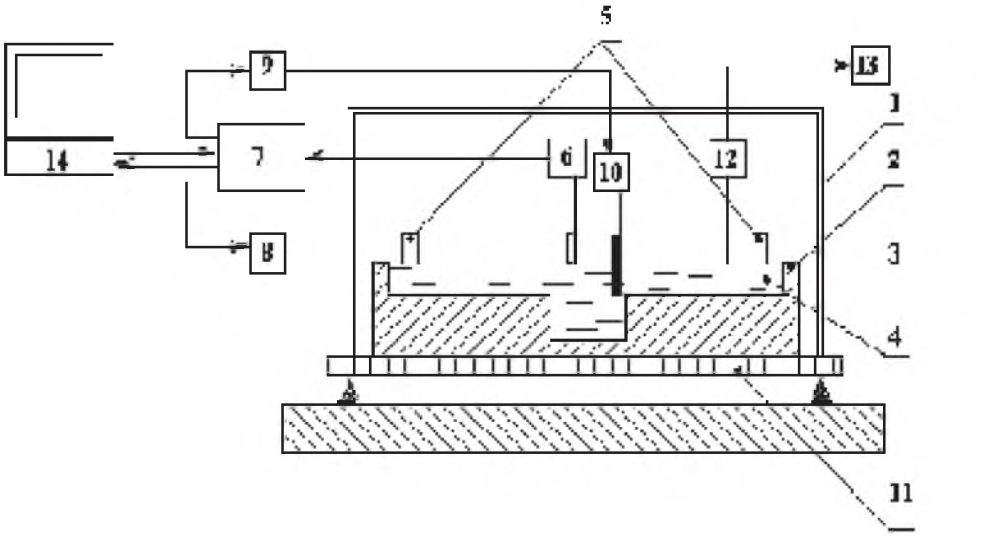
457 Спектор В. Н., Пахомов Л. Г – Устройство кристаллизации. Авторское свидетельство СССР № 1330791; Даценко Е. И., Пахомов Л. Г, Спектор В. Н. и другие – Способ очистки ароматических аминов. Авторское свидетельство СССР № 702004 от 14.08.79 с приоритетом от 19.10.77; Пахомов Л. Г., Спектор В. Н, Запольнов М К. и другие – Прецизионное производство органического полупроводникового материала КПЗ-01. Технологический регламент НИИ Химии при ГГУ-ВЗМИ-ОКТБ «Кристалл» при ЛТИ им. Ленсовета. Горький-М-Л, 1980. Государственный децимальный номер АЮВ 0.061.002 от 13.12.80, 9 с.; Пахомов Л. Г., Спектор В. Н., Запольнов М. К. и другие – Прецизионное производство органического полупроводникового материала КПЗ-02. Технологический регламент НИИ Химии при ГГУ-ВЗМИ-ОКТБ «Кристалл» при ЛТИ им. Ленсовета. Горький-М-Л, 1980. Государственный децимальный номер АЮВ 0.061.001 от 13.12.80, 9 с.; Спектор В. Н., Пахомов Л. Г., Михайлов В. М. – Разработка механизма образования и модели строения органических молекулярных комплексов с переносом заряда. Отчёт по НИР. ВЗМИ-НИИ Химии при ГГУ. Государственный регистрационный номер 01825023645, инвентарный номер 02822024385. 1981, 32 с.

Позже появилась возможность получения молекулярных сверхрешёток по методу Лэнгмюра-Блоджетт [458]и технологии молекулярного наслаивания[459].

Молекулярные сверхрешётки на основе органических КПЗ типа слоистых ассоциатов являются квазиодномерными или квазидвумерными твёрдыми телами, электронный спектр которых определяется преимущественно на молекулярном уровне, являются более совершенными электронными ключами. Однако они имеют существенный недостаток – низкую стабильность относительно воздействия внеш-



Реактор для получения кристаллов КПЗ *при T, P, c = const.*



Установка для получения моно- и мультислоевых органических структур методом Ленгмюра-Блоджетт Центра микротехнологий и диагностики Санкт-Петербургского государственного технологического университета.

1 – защитный колпак; 2 – симметричная двухсекционная фторопластовая кювета; 3 – подложка; 4 – граница раздела «субфаза – газ»; 5 – передвижные фторопластовые барьеры; 6 – электронный датчик поверхностного давления; 7 – блок управления; 8 – двигатель перемещения барьеров; 9 – привод; 10 – гидравлическое устройство перемещения подложки; 11 – антивибрационный стол; 12 – устройство очистки; 13 – насос; 14 – персональная ЭВМ.

---

458 Арсланов В. В. – Полимерные монослои и пленки Ленгмюра-Блоджетт. Политиофены. Успехи химии, 2000, том 69, №10, с. с. 963-980

459 Малыгин А. А. – Химия поверхности и синтез многокомпонентных оксидных наноструктур методом молекулярного наслаивания. В кн.: Труды XVII Менделеевского съезда по общей и прикладной химии. Казань, 2003. Доклад В239

Источник: www.nanoscopy.org

Микроскопия пленки Ленгмюра-Блоджетт.

них факторов (температура, влажность, пары органических растворителей, агрессивные газы и т. п.), что, естественно, резко ограничивает их практическую применимость, особенно в изделиях новой техники. Перспектива преодоления этого недостатка связана с совершенствованием технологии получения слоёв Лэнгмюра-Блоджетт, направленным на повышение чистоты и однородности структур на их основе.

Очевидно, что выполнение этих задач потребует расширения численности разведслужб, их глубокой модернизации, подготовки и переподготовки кадров высокой и высшей квалификации. Это, безусловно, потребует значительных средств, но никакая война не в состоянии отменить старую как мир мудрость: «Если страна не хочет кормить чужую армию, она должна содержать свою».

Службы контрразведки.

В ещё большей, пожалуй, мере следует ожидать усложнения работы всей системы органов контрразведки из-за появления системного виртуального агента трудно идентифицируемого противника с мультиплексностью, в пределе стремящейся к числу средств получения и отображения информации в стране,

$$\Lambda \rightarrow \sum n, m, \ell, \ldots,$$

где Λ – общая мультиплексность каждого виртуального агента,

$\sum$ – сумма средств получения и отображения информации в стране по видам:

$$n = n_1 + n_2;\ m = m_1 + m_2;\ \ell = \ell_1 + \ell_2,$$

n – общее число компьютеров, в том числе n_1 – общее число компьютеров в государственном секторе, в том числе в силовых структурах; n_2 – общее число компьютеров в личном пользовании, в общественных организациях и в корпоративных структурах;

m – общее число малых форм электронной связи и коммуникации (мобильные телефоны, в том числе спутниковые, смартфоны и другие), в том числе m_1 – общее число малых форм электронной связи и коммуникации в государственном секторе, в том числе в силовых структурах; m_2 – общее число малых форм электронной связи и коммуникации в личном пользовании, в общественных организациях и в корпоративных структурах;

ℓ … – общее число прочих, в том числе в нелегальных и криминальных структурах, и специальных средств связи и коммуникации.

Для понимания масштаба проблемы укажем, что, например, Глобальная информационная сеть Министерства обороны США включает около 7 миллионов компьютеров и более 15 тысяч различных компьютерных сетей. Часть из них содержит совершенно секретную информацию[460]. Наивно было бы предполагать функционирование единственного системного виртуального агента трудно идентифицируемого противника на территории страны. Исчерпывающий анализ требует исходить из аксиоматического предположения, что количество таких агентов стремится к некоторому пределу, например, к числу государств, в той или иной степени освоивших технологии информационной войны.

Наиболее продвинутые в этой области государства должны при этом предполагаться заинтересованными в функционировании более одного виртуального агента. В этом случае, каждый последующий виртуальный агент будет иметь более низкую мультиплетность, то есть он должен программироваться на определённую специализацию – сектор кибервойны (разрушение компьютерных и сетевых программ с целью нарушения систем связи и управления), сектор информационной войны (распространение дезинформации и ложной информации с целью провоцирования дестабилизации социума), сектор финансово-экономической войны, сектор разведки и т. д.

Однако сама множественность таких виртуальных агентов содержит заметный риск упрощения идентификации государственного или негосударстенного актора, обеспечившего генерацию такой серии виртуальных агентов по системе программирования и по общности предельной цели, то есть в таком случае виртуальной агент утрачивает характер случайной функции.

Элемент случайности функционирования виртуального агента может быть усилен генерированием по согласованной программе серии виртуальных агентов различными государственными или государственными совместно с негосударственными операторами с неочевидной общностью предельной цели.

Само по себе наличие в программах виртуальных агентов некоторой, пусть неизвестной точно, конечной цели позволяет отнести их к характеристическим функциям[461].

Характеристические функции обладают следующими свойствами:

– каждой случайной величине X соответствует определённая характеристическая функция, fx (t);

– распределение вероятностей для X однозначно определяется по fx (t);

---

460 http://www.neogeography.ru/ru/index. php? option=com content&view =article&id=168:24-&catid=2: news&Itemid=2

461 БСЭ. М., Советская энциклопедия. 1969-1973. Статья: Характеристические функции. [Яндекс. Словари>БСЭ, 1969-1978

– при сложении независимых случайных величин соответствующие характеристические функции перемножаются;

– при надлежащем определении понятия «близости» случайным величинам с близким распределением соответствуют характеристические функции, мало отличающиеся друг от друга, и, обратно, близким характеристическим функциям соответствуют случайные величины с близкими распределениями (например, можно с большой долей уверенности предполагать, что системный $\Lambda_{США}$ будет функцией, близкой к $\Lambda_{Британии}$, ***ergo***, можно ожидать близкого распределения величин мультиплетности).

Виртуальный агент, кроме того, может быть генерирован с использованием свёртки двух или более характеристических функций Λ_1 $\{f_1(x)\}$ и Λ_2 $\{f^2(x)\}$, тогда для комбинированного виртуального агента Λ^* свёртка двух используемых для генерации характеристических функций представляется в виде

$$f_1 * f_2.$$

Если f_1 и f_2 представляют собой плотности вероятности случайных величин X и Y, то $f_1 * f_2$ есть плотность вероятности X и Y:

$$\varphi(x) = -\infty\int\infty f_1(x-y)\, f_2(y)\, dy.$$

В целях затруднения распознавания и раскрытия свёртки пределы интегрирования могут выбираться произвольно

$$\varphi(x) = a\int b\, f_1(x-y)\, f_2(y)\, dy,$$

но интервал a….. b должен включать величины X и Y.

Свойства характеристических функций приводят к выводу предельных теорем[462]. Впервые вся сила метода характеристических функций ещё в 1901 году была показана академиком А. М. Ляпуновым [463] [464].

Понятие характеристических функций может быть обобщено, как на конечные, так и на бесконечные системы случайных величин, то есть на случайные векторы и случайные процессы. Это является дополнительным аргументом в пользу изучения возможностей развития методов практического применения характеристических функций для определения структуры виртуальных агентов и идентификации операторов, ответственных за их генерацию как инструментов информационной войны.

Безусловно, такая работа на перспективу должна вестись специалистами высшей квалификации совместно с академическими и вузовскими учёными в режиме повышенного уровня секретности, в том числе и по сокрытию

---

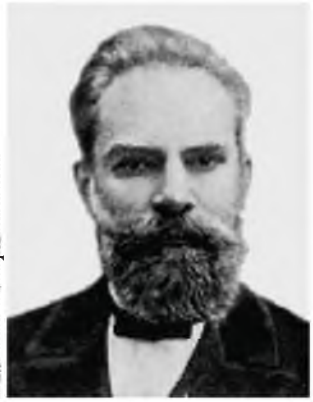
462 Гнеденко Б. В. – Курс теории вероятностей, 5 издание, М., 1969; Прохоров Ю. В., Розанов Ю. А. – Теория вероятностей, 2 издание. М., 1973

463 проф. Ляпунов Александр Михайлович (25.05.1857-03.11.1918) Академик Петербургской академии наук.

464 Ляпунов А. М. – Новая форма теоремы о пределе вероятности. Собрание сочинений, том 1, М., 1954, с. 157; Ляпунов А. М. – Избранные труды/Под редакцией В. И. Смирнова. Л., 1948

информации о специалистах, занятых в подобных исследованиях.

Приоритет борьбы с технологиями геоцентрического ТВД не может отменить повседневную работу органов контрразведки. Эта работа в настоящее время осложняется и тем, что компрадоры всех уровней являются вольными или неосознанными агентами зарубежных разведывательных служб, что целый ряд НГО, финансируемых зарубежными фондами и институтами, склонны видеть мир глазами западных структур, и тем, что иногда кажется, что в Москве и в Санкт Петербурге, число иностранных шпионов превышает число жителей этих городов.



Источник: www.kpi.kharkiv.edu

Александр Михайлович Ляпунов

К сожалению, в известной мере это является следствием ложно понимаемой политики «открытости», исповедуемой многими российскими государственными структурами. Открытость приемлема и даже хороша в межличностных отношениях, если, конечно они не затрагивают вопросы государственной, военной или технологической тайны. Она в определённых пределах необходима для успеха народной дипломатии. Открытость, как уже поняли многие крупные корпоративные структуры, совершенно недопустима в государственных структурах, и это относится не только к огрифованному документообороту, но и к любому обсуждению ведомственных вопросов вне установленных каналов.

Эта работа является или, скорее, являлась привычной для советских органов контрразведки до 1985 года. Правда, уже тогда в государстве был заложен системный порок – взяточничество. Нам на глаза как-то попалась книга конца 70-х годов «Наш самый страшный внутренний враг», изданная ЦК КПСС и ВЦСПС, в которой взяточник, особенно взяточник-чиновник, определялся как враг государства. Нельзя сказать, что тогда велась системная борьба с этим злом – оно постепенно распространялось, но было под контролем: разворовывалось примерно 2% ВВП страны, теневая экономика до 1985 года составляла не более 5% ВВП (правда, с 1985 по 1991 год она возросла до ~ 15%), уровень коррупции был очень высок в закавказских и среднеазиатских республиках и в Москве и также резко возрос с 1985 по 1991 год, выезды за рубеж были весьма и весьма ограничены, также как и визиты «диких» иностранцев. Бытовая преступность имела очень ограниченный выход на зарубежные каналы сбыта и поставки и чуралась контактов с иностранцами за исключением «общипывания» их в Москве, Киеве, Одессе и Ленинграде. Вспомним хотя бы знаменитую песенку из криминального фольклора: «Советская малина врагу сказала – нет».

Однако с развалом СССР вверх всплыла пена готовых и закалённых в неравной борьбе с государством кадров хозяйственного криминала, через границы плеснула волна новых «мешочников», которые подчас вербовку воспринимали как установление «деловых» контактов с зарубежными «коллегами». Одновременно деморосами – отсидентами и досидентами, у многих из которых было «рыльце в пушку» ещё из их советского прошлого, была разгромлена советская система государственной безопасности, в первую очередь структуры контрразведки и политического надзора.

Только к концу 1992 года из раздробленных кусков КГБ СССР, бессистемно разрезанного на ФСК, ФСО, ФАПСИ, ФПС и СВР, под надзором деморосов из ФСК, которая непонятно на кого лучше работала – на страну или на американское посольство, стал формироваться институт контрразведки, в конце-концов представленный ФСБ, в ведение которой лет через десять вернули ФПС.

В стране тем временем формировались и укреплялись структуры организованной преступности, консолидированной через так называемую «русскую мафию» с международной организованной преступностью, был налажен вывоз финансовых ресурсов (валюты, драгоценных металлов, алмазов и других драгоценных камней, стратегических материалов и технологий, включая изотопно обогащённые и особо чистые редкие и редкоземельные материалы, залоговых финансовых инструментов на землю, гарантированных федеральным правительством и правительствами субъектов Федерации). Страна была поставлена на ток пришедшими к власти экономическими бандитами, распродавалась оптом и в розницу. Организованная преступность завоевала контроль правительства, была широко представлена в органах представительной власти, скупила СМИ, создала свои силовые структуры, неподконтрольные федеральным силовым структурам. К концу «бурных девяностых» рейдерский разбой и заказные убийства пошли на убыль, замещаясь коррупционной организацией подбора кадров, отправления властных полномочий и осуществления хозяйственной деятельности. Такая ситуация привела к созданию принципиально новой «пятой колонны», в которой, в отличие от прошлого, все элементы этого антигосударственного сообщества, в большей или меньшей мере объединены зависимостью и приверженностью не какой-то определённой враждебной стороне, а надгосударственной структуре, часто именуемой «мировым правительством» – фантомом, выставляемым напоказ международным банковским консорциумом.

Надо отдать должное, – с начала 2000-ых в стране произошли заметные изменения, хотя борьбы с коррупцией, хищениями и незаконным обогащением только с 2012 перешла от слов к делу, но она постепенно становится ведущим трендом. Хотя в стране сильно влияние олигархов, компрадоров и пара-

зитического класса чиновничества, но и здесь наблюдается пусть и более медленная тенденция к изменению этой ситуации, создающей зияющие зоны уязвимости и угрожающей безопасности страны, несмотря на нарастающее давление со стороны западных структур, ведущееся преимущественно методами информационной войны.

Безусловно, решительный поворот власти к формированию гарантий суверенитета страны, подтверждённый укреплением военной организации и правоохранительных структур государства, предоставляет органам контрразведки возможности совершенствования своей деятельности и преодоления остаточных явлений влияния криминала и зарубежных разведывательных структур.

ГЛАВА 6.
ДОСТИЖЕНИЕ ПРЕВОСХОДСТВА В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ КАК ОСНОВНОЙ ЭЛЕМЕНТ ЗАЩИТЫ ГЕОПОЛИТИЧЕСКИХ ИНТЕРЕСОВ СТРАНЫ В ДОКРИЗИСНЫХ СИТУАЦИЯХ.

Вся мировая история стала подтверждением древнеримской максимы – «хочешь мира, готовься к войне», в том числе и к информационной войне. К сожалению, в этом элементе обеспечения национальной безопасности Российская Федерация утратила паритет с США в области информационного противоборства, в первую очередь в части технических средств его обеспечения.

Россия лишилась полигона в Багерово, оснащённого лучшими в мире стендами имитации всех компонентов ядерного взрыва и имевшего энергетическую обеспеченность, позволявшую поддерживать эксперименты по технологиям геоцентрического ТВД, в том числе и в киберкосмических вооружениях. Полигон отошёл к Украине и был разграблен до последнего метра кабеля.

Красноярская РЛС, способная поддерживать действия в киберкосмическом пространстве по требованию США (совершенно безосновательному, кстати) была разрушена по решению российского правительства.

Резервная РЛС «Дарьял-УМ» в Струнде, имевшая достаточную энергообеспеченность, но ещё не дооборудованная для ведения информационного и киберкосмического противостояния, была передана Латвии и уничтожена 5 мая 1995 года американской фирмой «Control Demolition Inc.» по требованию НАТО, а 2 РЛС «Днепр-М», некоторое время арендовавшиеся Россией, были уничтожены 19 октября 1999 года (были остановлены 31 августа 1998 года).

Габалинская РЛС была передана Азербайджану и находится в аренде РФ. Она полностью оборудована для ведения киберкосмического противоборства, но её функционирование за рубежом даже в мирное время сильно ограничено.

Российская станция «Сура», именуемая «Щитом Родины», введённая в строй в 1981 году, раньше аналогичной американской установки ХААРП, законсервирована, тихо разрушается, сильно разворована (кабели и медные детали).

В настоящее время российские возможности информационного противоборства ограничены в основном действиями в Интернете, и для достижения паритета по всей номенклатуре вооружений геоцентрического ТВД, координируемых и управляемых информационными вооружениями необходимо хотя бы срочно восстановить работоспособность комплекса «Сура».

Учитывая его неблагоприятное географическое положение (удалённость от полюса), как с точки зрения работы с заряженными оболочками Земли, так и с точки зрения наращивания мощности, необходимо начать работы по созданию современных комплексов на северных склонах Хибинского горного массива и на северных склонах Щучьих гор на Чукотке, что позволит обеспечить преимущество в противоборстве с комплексом ХААРП на Аляске и в Норвегии. В связи с необходимой высокой энергообеспеченностью таких комплексов (1,5-5,0 ГВт) возникают сложности с генерацией таких мощностей.

На Чукотке, также как на Аляске есть достаточные разведанные месторождения энергоносителей, но в отличие от ситуации на аляскинском комплексе ХААРП, где генерация на уровне 1,7 ГВт осуществляется на основе действующего комплекса по добыче природного газа, который позволяет планировать наращивание мощности антенных систем до 3,6 ГВт, эти чукотские месторождения ещё не разрабатываются.

Значительно проще в среднесрочной перспективе обеспечить энергоснабжение установки в Хибинах за счёт газовых месторождений севера Европейской части России. В докритической ситуации в режиме небоевого противостояния в геоцентрическом космическом пространстве достаточным уровнем энергообеспечения можно считать уровень $W \leq 2{,}0$ ГВт, что можно совместить с экспортными поставками газа по трубопроводу «Северный поток». В случае же военного конфликта газовый поток может быть перенаправлен на генерирующие мощности Хибинского комплекса.

Однако, как говорится «ложка к обеду хороша». Исторически это было подтверждено испытаниями ядерного оружия СССР, сразу охладившими пыл западных милитаристов. Россия должна заявить миру о своей технической возможности действий на геоцентрическом ТВД.

Решением вопроса срочного энергообеспечения комплексов на Чукотке и в Карелии может стать модификация российской программы утилизации АПЛ, снятых с боевого дежурства. Два кластера таких АПЛ, реакторы которых могут обеспечить суммарную выходную мощность $W \approx 2{,}0$ ГВт, могут быть перемещены от мест хранения АПЛ на максимально близкое расстояние к антенным комплексам. Они по временной схеме могут обеспечить работоспособность этих комплексов, вплоть до создания генерирующих мощностей на основе местных энергоносителей, способных выводить эти антенные комплексы на уровень излучаемых мощностей 4-5 ГВт.

Источник: www.nvmu.ru

Анатолий Иванович Хюпенен

Источник: vk.com

Сергей Игоревич Покладов

Эти же антенные комплексы могут решить ещё одну важную проблему. Большинство наиболее современных советских загоризонтных РЛС были размещены на территории Украины. Хотя не все они разорены и разграблены, России от этого толку чуть. Такие системы, регистрирующие пуски межконтинентальных ракет, локацию подводных лодок геополитических оппонентов и прямую связь с собственным подводным флотом, не должны арендоваться, а должны стоять на вооружении ВС РФ (ВМФ). Кроме того, они являются важным инструментом ведения информационной войны с использованием возможностей геоцентрического ТВД в интересах ФСБ, СВР, МВД, ФСО (ФАПСИ) и МО РФ.

Не менее важным мероприятием является подготовка операторов высшей квалификации для загоризонтных РЛС и для комплексов управления состоянием ионосферы и магнитосферы Земли, а также системных операторов управления всеми видами оружия геоцентрического ТВД и управления боевыми операциями на геоцентрическом ТВД.

Некоторым аспектам этого вопроса посвящена работа председателя Объединённого совета Союза ветеранов Войск ПВО, генерал-полковника в отставке, доктора военных наук, проф. Анатолия Ивановича Хюпенена [465] и полковника в отставке, члена Президиума Союза ветеранов Войск ПВО Сергея Игоревича Покладова [466]. Заметив, что в соответствии с Указом президента РФ от 1 декабря 2011 года созданы Войска воздушно-космической обороны, они пытаются довести до читателей «некоторые аспекты, связанные с таким важным вопросом, как организация и становление ВКО, а если быть конкретнее – рассмотреть сложившуюся обстановку вокруг подготовки специалистов для неё и определения головного военного вуза, который этим займётся».

Необходимо отметить, что существовавшее в то время руководство Минобороны России сильно подвело Президента страны. В сложившей-

---

465 проф. Анатолий Иванович Хюпенен 25 мая 1928 года, генерал-полковник в отставке, доктор военных наук, бывший командующий зенитными ракетными войсками ПВО страны, в 1972-1975 годах – старший группы советских военных специалистов в Демократической Республике Вьетнам.

466 Покладов Сергей Игоревич, полковник, служил в 392-м гвардейском зенитно-ракетном полку.

ся в мире ситуации нужно было решать вопрос о создании Военно-космических войск или «киберкосмических войск», одной из функций которых может быть и противовоздушная оборона.

Они, конечно, совершенно правы, говоря, что «В оценке современной военно-политической обстановки руководством нашего государства и его Вооружённых Сил отмечено, что, несмотря на позитивные перемены в мире, значение военно-силовых аспектов в международных отношениях продолжает оставаться существенным, а уровень и масштабы угроз в военной сфере возрастают[467].

Они частично правы, утверждая, что «В настоящее время коренным образом изменилось само содержание вооружённой борьбы. Её основой становятся действия сил воздушного нападения всех видов базирования при всестороннем их обеспечении из космоса в интегрированной системе управления. Именно поэтому в строительстве вооружённых сил ведущих стран мира сформировалась устойчивая тенденция приоритетного развития сил и средств воздушно-космического нападения. Анализ развития средств воздушно-космического нападения (СВКН) иностранных государств показывает, что уже в период до 2020 года произойдут коренные изменения, связанные с освоением воздушно-космического пространства как единой сферы вооружённой борьбы. Именно в этот период на вооружение основных иностранных государств поступят принципиально новые средства и системы, произойдёт интеграция средств разведки, связи, навигации и управления в единую информационно-разведывательную управляющую систему. Качественно изменятся формы и способы применения войск и сил» любого назначения.

Авторы работы[468] уверены, что «В этих условиях противник получит возможность наносить скоординированные во времени и пространстве высокоточные удары практически по всем целям на территории России». В тех условиях, которые имеют в виду и которые предлагают «ремонтировать, а не изменять эти авторы, то есть в условиях неготовности России к проведению масштабных боевых операций в космическом пространстве, а зацикливании на вопросах традиционной обороны, это может быть и так.

Само воздушно-космическое пространство станет единой, а порой и основной сферой вооружённой борьбы, а военные действия в нём приобретут главенствующую роль и глобальный размах. Успешное их ведение будет основой для достижения успеха в вооружённой борьбе на суше и на море.

---

467 Хюпенен Анатолий, Покладов Сергей – Кто организует борьбу на новом ТВД? Необходим военный учебно-научный центр ВКО. Общероссийская еженедельная газета «Военно-промышленный курьер ВПК»

468 Хюпенен ... Кто организует ...

С точки зрения авторов[469], не обязательно верной, впрочем, «угрозы СВКН являются наиболее значимыми в общей системе военной безопасности России. Это уже сегодня требует от нас адекватного совершенствования средств и систем противовоздушной, а в ближайшей перспективе – и воздушно-космической обороны Российской Федерации, предусматривающей объединение под единым управлением всех сил и средств, предназначенных для решения задач защиты от воздушно-космического нападения противника.

Таким образом, в настоящее время и, тем более, в будущем воздушно-космическое пространство становится новым театром военных действий (ТВД) и имеет абсолютно обоснованное право на такое же существование, как сухопутный и морской театры. Театр войны XXI века непременно будет иметь в своём составе три самостоятельных ТВД: сухопутный, морской и в воздушно-космической сфере». Возврат к принципам ведения войны по типу войн XX века, когда в основном принимаются во внимание способы вооружённой борьбы «на земле» и «на море», ведёт в тупик её организацию в воздушно-космическом пространстве.

В этом смысле авторы[470] сильно отстали от понимания стратегической реальности XXI века – самостоятельные операции сухопутных войск, ВВС и ВМФ в ходе масштабных военных конфликтов ушли в историю. Это вовсе не значит, что они утратили свою актуальность и не нуждаются в развитии и совершенствовании, но уже в настоящее время основной тенденцией военного строительства становится реформирование этих видов вооружённых сил на обеспечение возможности их участия в боевых действиях на геоцентрическом, а в перспективе и на гелиоцентрическом ТВД. Вместо трёх доменов вооружённой борьбы возникает единый, поглощающий их геоцентрический домен, в котором космос сам становится оружием.

Авторы[471] считают, что «сама по себе противовоздушная, а в современных условиях – воздушно-космическая оборона не создаётся[472]. Требуются объединение и координация усилий многих должностных лиц государства, Вооруженных Сил и ВКО, чтобы задачи, возложенные на новый род войск, были, безусловно, выполнены в военной обстановке».

В подтверждение своих выводов они приводят параллель с военными акциями США с союзниками против суверенной Югославии, против Ирака и совсем недавно – Ливии, начинавшихся «с проведения воздушной наступательной операции или авиационных ударов» и закончившихся «полной деморализацией вооружённых сил и населения защищающейся стороны.

---

469 Хюпенен ... Кто организует ...

470 Хюпенен ... – Кто организует ...

471 Хюпенен ... – Кто организует ...

472 Хюпенен А. И. и другие – Крах трёх академий. Военно-промышленный курьер. 2012

В результате исход военных действий был предрешён во всех случаях. Слабая противовоздушная оборона (не говоря уже об отсутствии воздушно-космической обороны) неизбежно ведёт к военному поражению и утрате государством суверенитета». Здесь авторы впадают в обычную профессиональную паранойю, сводя всю войну к ПВО, – есть и другие виды военного противостояния. Далее они показывают, что «есть и другие примеры. В частности, грамотное построение противовоздушной обороны в 60-70-х годах прошлого века (конечно, с помощью СССР) позволило небольшому государству Вьетнам выстоять в войне против Соединённых Штатов Америки и отстоять свою независимость». Здесь авторы[473] упустили сразу два крайне важных момента. Во-первых, в случае Югославии, Ирака, Афганистана, Ливии и Сирии всё началось с массированной информационной войны – вид военных действий, который эти авторы вообще не принимают во внимание. Во-вторых, вьетнамская война была традиционной войной, даже ещё не трёхмерной, в которой США и СССР проводили пробу сил и отрабатывали новые виды и типы традиционных вооружений с прицелом на возможности перехода к новой парадигме войны.

Они, безусловно, ошибаются в том, что «Руководством нашего государства на первых порах были предприняты абсолютно верные шаги, когда в апреле 2006 года была утверждена Концепция воздушно-космической обороны Российской Федерации до 2016 года и в последующий период, спланированы мероприятия, обеспечивающие совершенствование возможностей существующих систем противовоздушной и ракетно-космической обороны и создание на втором этапе интегрированной системы воздушно-космической обороны страны». Ошибкой является определение исключительно оборонительных мер и мероприятий – это прямой путь к капитуляции.

«Тем не менее, проблема определения ведущего высшего военно-учебного заведения для подготовки специалистов ВКО не решена и по сей день. Другой важной проблемой, как мы считаем, является то, что многие предложения ветеранов и учёных Войск ПВО остаются неуслышанными». Далее, в развитие своих претензий[474] авторы[475] обсуждают проблему оптимального выбора военного учебного заведения, в наибольшей мере приспособленного к подготовке кадров высшей квалификации для ВКО. Как обычно желание поддержать одно учебно-научное заведение они сопровождают мало обоснованной критикой возможностей других, вместо того, чтобы чётко показать преступность деятельности министра обороны А. Э. Сердюкова (в широких кругах известного под псевдонимом «табуреткин» – Интернет) и начальни-

473 Хюпенен ... – Кто организует ...

474 Хюпенен ... – Крах трёх академий ...

475 Хюпенен ... – Кто организует ...

Источник: opolichi.ru

Анатолий Эдуардович Сердюков

Источник: mk-turkey.ru

Николай Егорович Макаров

ка Генштаба ВС РФ Н.Е. Макарова, сделавших всё для недопущения готовности страны к противодействию на геоцентрическом ТВД, в частности практически уничтоживших Академию Жуковского ради красивого исторического здания.

В части ликвидации последствий доведенного до безумия разбоя в части практической ликвидации базовых военных академий, передачи высоко специализированного спецназа ГРУ ГШ ВС РФ, способного решать самые сложные оперативные задачи информационной борьбы, и финансовых художеств Сердюкова и иже с ним положительный сигнал дан нынешним Министром обороны РФ С.Г. Шойгу.

Нужно особо подчеркнуть, что и Военно-воздушная инженерная академия имени Н.Е. Жуковского – школа всех советских и российских космонавтов с Военным учебно-научным центром ВВС и с Научным центром по разработке проблем авиационной техники, её эксплуатации и боевого применения, и получившая статус базовой организации стран Содружества по подготовке военных кадров для объединённой системы ПВО (10 декабря 2003 года) Военная академия воздушно-космической обороны имени маршала Советского Союза Г.К. Жукова (Тверь), специалистами которой был подготовлен военно-теоретический труд «Стратегическая операция по отражению воздушно-космического нападения противника», основные положения которого были приняты Генеральным штабом и положены в основу стратегического планирования, а сама стратегическая операция по отражению ВКН противника длительное время сохранялась как официальная форма применения Вооружённых Сил РФ, и Военная космическая академия имени А.Ф. Можайского – должны ускоренно развиваться, а не подвергаться разрушительным экспериментам безответственных профанов с ускоренным экономическим «остепенением» и их подельников.

После разорения отечественными высокопоставленными саботажниками Военно-воздушной инженерной академии им. Жуковского, вероятно, можно согласиться с точкой зрения Хюпенена с соавторами в том, что ведущую роль в подготовке специалистов воздушно-космической обороны должна сыграть Военная академия ВКО в Твери как единственное учебно-

научное учреждение, имеющее государственную лицензию на подготовку специалистов воздушно-космической обороны, где сосредоточены знания по системам ПВО и РКО (а в целом, по системе ВКО), которая на научном уровне продолжает исследование вопросов воздушно-космической обороны, начатое ещё в 1988 году. Академия, обладает современной техникой (в том числе готовит специалистов на ЗРК С-300, С-400) и сетью новейших разноуровневых (от подразделения до оперативно-стратегического объединения), компьютеризированных и замкнутых в единую систему командных пунктов («Бастион», «Универсал» и «Байкал»). Этого, безусловно, мало для подготовки специалистов, способных участвовать в операциях на геоцентрическом ТВД. Однако начинать с чего-то надо, и быстро.

Можно согласиться с мнением Хюпенена с соавторами о необходимости создания для начала Военного учебно-научного центра воздушно-космической обороны на базе Военной академии ВКО им. Г. К. Жукова и включения в его состав Научно-исследовательского центра ПВО (Тверь) 4-го Центрального научно-исследовательского института Минобороны России, а в качестве филиалов – Ярославского института ПВО, учебных центров зенитных ракетных и радиотехнических войск в Гатчине и Владимире.

Целесообразно было бы прислушаться к мнению специалистов и ветеранов, положить конец принятию необоснованных решений в области обороны и дать возможность прославленным вузам Вооружённых Сил, которые не на словах, а на деле доказали высокий уровень вышедших из их стен специалистов, заниматься не борьбой за существование с невежественными бюрократами, а своим прямым предназначением – подготовкой руководящих кадров.

Приведём более обоснованную точку зрения на один из важнейших элементов противоборства на геополитическом ТВД – войне в концептуальном пространстве[476], по определению ведущейся консциентальным и информационным оружием.

«События «арабской весны», а также ряд успешных действий в ходе информационного противоборства США, Израиля и Ирана вновь возбудили интерес к проблеме обеспечения информационной безопасности государства.

В начале текущего года Министерство обороны Российской Федерации решило обозначить своё отношение к проблеме, опубликовав на официальном сайте документ под названием «Концептуальные взгляды на деятельность Министерства обороны РФ в информационном пространстве».

До последнего времени Минобороны старалось держаться в тени, явно не обозначая собственное отношение к проблеме информационного проти-

476 Гриняев Сергей (ЦСОиП) – Война в концептуальном пространстве. Открытый исследовательский и дискуссионный центр «Глобальная авантюра». Серия: «Глобальные проблемы», 15 марта 2012

воборства. Это во многом понятно – с момента принятия Доктрины информационной безопасности РФ в 2000 году не утихает спор между рядом российских ведомств за приоритет в этой сфере. Но, учитывая, что документ всё же был опубликован, тем самым обозначив отношение Минобороны к проблеме, он не мог остаться незамеченным среди специалистов, занимавшихся и занимающихся изучением вопросов организации и ведения информационного противоборства.»

Действительно, проблема организации и ведения информационного противоборства (по западной терминологии – «информационной войны») в последнее время актуализировалась. Причиной стало то, что многие положения современной военной науки, ранее бывшие исключительно теоретическими наработками, в последние месяцы получили практическую реализацию. Прежде всего, это касается успешной информационно-технической операции, проведенной против критической инфраструктуры ядерных объектов Ирана, а также проведенной иранскими силами против американского БПЛА. События же «арабской весны», уже не один месяц не сходящие с первых полос мировых СМИ, есть не что иное, как успешная стратегическая информационно-психологическая операция информационного противоборства. В обоих случаях имели место стратегические операции информационного противоборства, так как их результат привёл к изменению военно-политической обстановки в регионе и в мире в целом.

В этих условиях Минобороны РФ просто обязано было представить собственное отношение и собственное видение проблемы, обозначить готовность обеспечить сохранение информационной безопасности Вооружённых Сил и информационной безопасности государства.

Однако анализ документа показывает, что сделать этого не удалось. Более того, представленные «концептуальные положения» отбрасывают российскую военную науку на десятилетие назад – практически всё, что нашло отражение в обнародованном документе в той или иной форме обсуждалось (а многое отвергалось) ещё десять лет назад!

Самое простое, то, что лежит на поверхности и сразу бросается в глаза, – это терминологическая база. Такие общие термины как «информационный ресурс», «информационное пространство» и другие в документе трактуются собственным, уникальным образом, не связанным с трактовкой аналогичных терминов в иных государственных документах (например, согласно госпрограмме «Информационное общество 2011-2020 годов»), что подчеркивает общую несогласованность документа.

В большинстве данных в документе определений отсутствует глубокая теоретическая проработка, что ведёт к оторванности от единой теоретической основы военного строительства и понимания проблем информационно-

го противоборства, сложившегося за предыдущие десятилетия. Так, к примеру, в документе обозначен «военный конфликт в информационном пространстве», который есть не что иное, как «форма разрешения межгосударственных или внутригосударственных противоречий с применением информационного оружия». В этом определении, кроме спорности самого понятия «военного конфликта в информационном пространстве», особо насторожила готовность применения военной силы к разрешению внутригосударственных проблем, что является прерогативой МВД и ФСБ РФ и никогда не вменялась в задачи МО РФ (об этом, кстати, говориться и на официальном сайте Минобороны).

Давая определение информационной войне, авторы документа указывают на то, что это есть «противоборство между двумя или более государствами в информационном пространстве», при этом упуская из виду то обстоятельство, что сегодня важными акторами мировой политики являются надгосударственные структуры, которые подчас гораздо опаснее государств.

Кроме того, в документе отмечается, что раз решение на применение Вооружённых Сил РФ за пределами российской территории принимается Президентом РФ на основании соответствующего постановления Совета Федерации, то данное положение следует распространить также и на применение сил МО РФ в информационном пространстве. Это также весьма спорное утверждение. Получается, что в случае возникновения потребности в проведении операции, подобной внедрению вируса STUXNET, необходимо разрешение Совета Федерации?

Говоря о коалиционности действий, упоминая ОДКБ, ШОС и СНГ, авторы обходят стороной Союзное государство России и Беларуси.

В документе нет ни слова о новой структуре Вооружённых Сил, о том, кто же будет решать задачи по организации и ведению информационной войны в рамках военной структуры государства. Нет и чёткого понимания, как и каким образом следует увязывать подходы к организации и ведению информационной войны с теми принципами сетецентричности, которые сегодня так популярны в военной среде.

В общем, суммируя изложенное, следует отметить, что представленный Министерством обороны документ оказался типичным продуктом нынешней военной реформы. Он никак не связан с большим практическим и теоретическим пластом, наработанным российской военной наукой в предыдущие годы. Такое ощущение, что авторы оказались как бы первопроходцами, что немудрено – в результате проводившихся в последние годы реформ из Минобороны было уволено большинство специалистов, занимавшихся в течение многих лет разработкой проблемы организации и ведения информационного противоборства, а соответствующие научно-исследовательские

структуры внутри Минобороны перепрофилированы на другие направления. Так что опубликованный документ лишь дополнил и наглядно проиллюстрировал ситуацию со скандалом вокруг официального интернет-сайта Минобороны (кстати, одного из элементов инфраструктуры ведения информационного противоборства)[477]».

Помимо первоочередных задач подготовки кадров для выполнения задач на геоцентрическом ТВД, в первую очередь информационной борьбы, параллельно необходимо срочно решать вопрос восстановления вооружений и технической базы киберкосмических войск.

Для полного общего паритета в технологиях геоцентрического ТВД необходимо оборудовать 2-3 крупных корабля с мощными управляющими РЛС для фокусировки космических воздействий на наземных (океанических) целях и доработать систему космического истребителя Н. Матюка или «Буран» на возможности обеспечения в комплексе с наземными станциями успешного противоборства в космическом пространстве.

Необходимо изучить архивы группы Печенева (ЦК КПСС) и организовать на их основе и на основе научных и аналитических материалов МАН ПНБ подготовку специалистов высшей квалификации для достижения превосходства в информационном противоборстве в докризисный период. При этом необходимо заметить, что в силу консервативности мышления даже самых выдающихся военных учёных, может быть за исключением единиц, фундаментальные исследования в этой области и подготовка специалистов высшей квалификации должны осуществляться с привлечением академических (РАРАН, РАТН, РАЕН, РАМН и может быть РАН РФ) и вузовских учёных.

477 http://www. csef.ru/studies/defence/projects/theory_of_information_war/articles/2876/

ГЛАВА 7.
ДОСТИЖЕНИЕ ПРЕВОСХОДСТВА В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ КАК ОСНОВНОЙ ЭЛЕМЕНТ ЗАЩИТЫ ГЕОПОЛИТИЧЕСКИХ ИНТЕРЕСОВ СТРАНЫ В УСЛОВИЯХ ВООРУЖЁННОГО ПРОТИВОСТОЯНИЯ (ВМЕСТО ЗАКЛЮЧЕНИЯ).

Ещё раз необходимо напомнить научно обоснованную точку зрения, что переход от современного оружия, включая СМП, к перспективным вооружениям геоцентрического ТВД является более фундаментальным, чем переход от традиционных к ядерным вооружениям. Необходимо учитывать и тот факт, что в настоящее время российские возможности, как противостояния американским вооружённым силам на геоцентрическом ТВД, так и эффективного проведения на этом театре собственных военных действий резко ограничены, а достижение паритета в ближайшие 5-7 лет довольно сомнительно.

Исходя из этих начальных условий, необходимо срочно адаптировать как внутреннюю промышленную, сельскохозяйственную, военную, социальную и информационную организацию государства, его мобилизационный план и систему международных отношений к условиям нарастающей интенсивности информационной войны, способной уже в среднесрочной перспективе перейти в полномасштабную вооружённую конфронтацию.

Одной из причин такой проекции современной обстановки является быстрый переход от вяло растущей латентной внутриполитической нестабильности в США к довольно быстро развивающемуся системному кризису[478].

Осознание этой тенденции политическим и военным руководством США, понукаемым кликой неоконсерваторов как представителей «мирового правительства», уже в 90-х годах привело к безудержному экспансионизму, к радикальной милитаризации внешней политики и к отходу от международ-

478 Спектор В.Н. – Геополитическая концепция Договора о противодействии распространению ядерных вооружений, оружия массового поражения и средств их доставки. Лекция и семинар в Управлении информации и разведки Госдепа США. Вашингтон. США, 2006

ных обязательств[479]. Сейчас перед Соединёнными штатами остро встала проблема выбора: вернуться в русло следования нормам мирового сообщества наций и международных договоров или сделать ставку на победу в мировой войне, пользуясь временным преимуществом в наступательных информационных/киберкосмических технологиях, логистике и вооружениях геоцентрического (с началами гелиоцентрического) театра военных действий.

Учитывая груз накопившихся преступлений, возврат США к модели устойчивого развития в согласии с остальным мировым сообществом наций представляет значительные трудности, да и 17 триллионов национального долга делают такой шаг только труднее. В докладе[480], помимо обсуждения проблем, связанных с расползанием ядерных вооружений (приложение 1), был сделан прогноз возникновения и развития системного кризиса (2007/начало – 2012/пик – 2015-2018/распад или переход в разряд второстепенных региональных держав) государственности США. Судя по информации, поступающей от американских участников Академии, ситуация в США изменяется практически точно в соответствии с прогнозом.

Ergo, разумно ожидать усиления экспансионизма и агрессивности США, делащих ставку на «последний решительный бой». При этом необходимо учитывать, что стратегическими приоритетами неоконсерваторов, «правящих бал» в политической элите США, являются Россия, Германия (кстати, после распада СССР вышедшая на второе место в мире по освоению оружия геоцентрического ТВД) и при определённых условиях – Китай. Такая траектория развития политики США, как и во время холодной войны балансирующей на грани войны и мира, грозит к скатыванию в Третью мировую войну (многие военные аналитики уверены, что предпольные сражения этой войны идут уже довольно давно, может быть сразу после окончания «холодной войны»).

Американские политики стараются приготовить к ней американский народ и успокоить его заверениями о том, что информационная война будет вестись киберкосмическими средствами на внеземном, неком геоцентрическом ТВД, практически без человеческих жертв. Некоторая часть американского общества верит этому, несмотря на то, что цели оружия геоцентрического ТВД находятся на Земле/Гее и что каждая новая война связана с увеличивающимся числом человеческих жертв, в первую очередь мирных жителей, детей, женщи и стариков. Впрочем, уничтожение людей является одной из приоритетных целей неоконсерваторов, идеологов людоедского «золотого миллиарда», а убивать беззащитных куда как легче и дешевле.

---

479 Путин В. В. – Мюнхенское выступление

480 Спектор – Геополитическая концепция ..., 2006 (американские коллеги были предупреждены, что ни в лекции, ни в ответах на вопросы в ходе семинара опция мировой термоядерной войны не рассматривается

Неизбежна ли победа США в войне с большей частью мира? Безусловно, нет. Скорее можно быть уверенным, что в том случае, если США всё же решаться на такую авантюру, то либо они потерпят сокрушительное поражение, либо человечество перестанет своё существование на планете Земля. Значит ли это, что можно ничего не делать для изменения складывающейся ситуации? Безусловно, нет.

Рассмотрим, что может сделать Россия для своей защиты и для предотвращения всемирной бойни.

В области промышленной политики.

В рамках принятой государством программы диверсификации промышленного производства было бы целесообразно принять следующие меры:

– выделить в самостоятельный раздел программу реконверсии, устранив принципиальный недостаток Программы конверсии оборонного потенциала в области новых материалов и технологий Госплана СССР 1989 года[481], в которой в соответствии с указанием Политбюро ЦК КПСС не была учтена необходимость реконверсии производственных мощностей и, определив предприятия по направлениям реконверсии; подготовить и утвердить в установленном порядке нормативную документацию по обеспечению реконверсии;

– обеспечить приоритетное развитие машиностроительных и перерабатывающих предприятий, в первую очередь восстановление и модернизацию предприятий ВПК, назначенных на производство космической техники, систем и средств связи, электроники и электронного приборостроения;

– предусмотреть опережающее развитие отечественного производства товаров широкого потребления на международном уровне качества, имея в виду достижение полного самообеспечения товарами первой необходимости (в первую очередь фармацевтической продукции, одежды, обуви и бытовой химии), прогрессивно ограничивая их импорт (следует иметь в виду, что технология глубокой очистки органических веществ – полупродуктов в производстве лекарственных средств методом квазизонной плавки с недостатком растворителя[482]);

– предусмотреть восстановление предприятий местной промышленности на региональном и муниципальном уровне с целью максимально полного

---

481 Степанов Р. Ф., Спектор В. Н., Беликов Л. В. и другие – Программа конверсии оборонного потенциала в области материалов и технологий. Госплан СССР. М., 1989, в трёх томах

482 Пахомов Л. Г. – Автореферат докторской диссертации. ИХФ АН СССР. М., 1990, 48 с.; Пахомов Л. Г., Даценко Е. И., Камарицкий Б. А., Спектор В. Н. – Способ очистки олигоорганосилсесквиоксанов. Авторское свидетельство СССР № 1343783, зарегистрировано 8 июля 1987 г. с приоритетом от 25 декабря 1984 г. по заявке № 3831812; Даценко Е. И., Пахомов Л. Г., Спектор В. Н. и другие – Способ очистки ароматических аминов. Авторское свидетельство СССР № 702004

Источник: www.ccas.ru

Никита Николаевич Моисеев

самообеспечения товарами местного производства, обращая особое внимание на производство строительных материалов, строительной техники;

– повысить роль и ответственность региональных и муниципальных органов власти за осуществление мер по реализации полного самообеспечения товарами первой необходимости и создание их трёхмесячного резерва, учитываемого Госрезервом РФ, в условиях введения режима чрезвычайной ситуации;

– обязать органы национальной безопасности совместно с региональными и муниципальными органами власти обеспечить на всех предприятиях установку систем интранета с переходом на них из интернета в случае поступления предупреждения об угрозе атаки информационным/киберкосмическим оружием.

В области политики по развитию инфраструктуры:

– памятуя известное утверждение академика Н.Н. Моисеева о том, что России принадлежит совершенно особая роль инфраструктурного трансконтинентального моста в международной системе разделения труда и заявление В.В. Путина (2001) о готовности России обеспечить на своей территории строительство части трансконтинентальной инфраструктуры «Сеул – Париж», ускорить решение о реализации Программы транс российской консолидированной инфраструктуры (представлена в Совбез РФ в 1999 году – приложение 2);

– обязать органы национальной безопасности совместно с руководством всех инфраструктурных систем и предприятий обеспечить на них установку систем интранета с переходом на них из интернета в случае поступления предупреждения об угрозе атаки информационным оружием.

Сам факт строительства такой инфраструктуры явится мощным сдерживающим фактором относительно агрессии против России. Безусловно, при этом логистика прокладки трубопроводов, линий электропередачи и связи в экранирующих трубах резко повысит их защищённость относительно информационных атак даже самым перспективным киберкосмическим оружием и ЭМИ ядерных ударов. Кроме того, и работы по созданию и последующая эксплуатация такой инфраструктуры обеспечат появление 5-7 миллионов высокооплачиваемых рабочих мест, включая повышенную загрузку металлургических, машиностроительных и приборостроительных производств.

В области сельскохозяйственной политики:

– предусмотреть создание горизонтально интегрированных межрегиональных, региональных и субрегиональных сельскохозяйственных комплексов с замкнутым циклом производства на земельных угодьях площадью 5000-50000 гектар, включающих производственные мощности по переработке и предпродажной подготовки продукции (следует иметь в виду, что существует отечественная технология бакцерицидной упаковки продуктов питания, д. х. н. В.М. Мисин), а также мощности по текущему ремонту и обслуживанию сельхозтехники;

– предусмотреть опережающее развитие отечественного производства продуктов питания широкого потребления на международном уровне качества, имея в виду достижение полного самообеспечения продуктами первой необходимости;

– учитывая результаты долговременных исследований международного эксперта, д. б. н., проф. Ермаковой, ввести законодательный запрет на импорт/ввоз на территорию Российской Федерации любой генмодифицированной продукции в связи с её разрушительным действием на генофонд местной флоры и фауны, включая человека;

– повысить роль и ответственность региональных и муниципальных органов власти за осуществление мер по реализации полного самообеспечения продуктами питания первой необходимости и создание их трёхмесячного резерва, учитываемого Госрезервом РФ, в условиях введения режима чрезвычайной ситуации;

– обязать органы национальной безопасности совместно с региональными и муниципальными органами власти обеспечить на всех сельхозпредприятиях установку систем интранета с переходом на них из интернета в случае поступления предупреждения об угрозе атаки информационным оружием;

– для уменьшения уязвимости сельского населения предусмотреть предельно достижимое рассредоточение сельхозпроизводителей по территории страны, в первую очередь, используя ресурсы сельхозугодий Сибири и Дальнего Востока.

В области энергетики:

– осуществить неотложную оптимизацию структуры генерирующих мощностей и номенклатуры энергоносителей с целью создания альтернативной системы межрегиональных, региональных, субрегиональных и муниципальных (дизель-генераторы) генерирующих мощностей, работающих

Источник: ru.wikipedia.org

Николай Сергеевич Ениколопов

Источник: www.spfond.ru

Александр Евгеньевич Шилов

на местных энергоносителях (в целях расширения номенклатуры энергоносителей осуществить ускоренное внедрение технологии конверсии отходящих и попутных газов в спирты (ОИХФ РАН, академик А. Е. Шилов) и конверсии отработавших резинотехнических изделий в жидкие углеводороды (ИСПМ РАН, академик Н. С. Ениколопов));

– осуществить ускоренный переход с мачтовой системы ЛЭП на линии заглубленных экранированных и термостатируемых кабелей, устойчивых относительно атак киберкосмическим оружием и ЭМИ ядерного оружия;

– осуществить экранировку наземных технических сооружений линий электропередачи и трубопроводов энергоносителей (перекачивающих станций и т. п.), обеспечивающую их устойчивость к воздействию киберкосмического и информационного оружия и ЭМИ ядерного оружия;

– повысить роль и ответственность региональных и муниципальных органов власти за осуществление мер по реализации полного самообеспечения энергоносителями и создание их трёхмесячного резерва, учитываемого Госрезервом РФ, в условиях введения режима чрезвычайной ситуации;

– обязать органы национальной безопасности совместно с региональными и муниципальными органами власти и с руководством предприятий энергетического комплекса обеспечить на всех предприятия энергетического комплекса установку систем интранета с переходом на них из интернета в случае поступления предупреждения об угрозе атаки информационным оружием.

В области военной политики.

Вероятность достижения паритета с США в области вооружений геоцентрического ТВД в среднесрочной перспективе крайне низка, а ведение военных действий против них современными вооружениями обречено на провал. Однако уровень разработок в области геоцентрических вооружений не обеспечивает надёжность его эффективного функционирования при целом ряде условий, например, при минировании или «выжигании» околоземного космоса (с. 300).

В тоже время стратегические компоненты ВС США переориентированы и переоснащаются на ведение информационной войны киберкосмическими средствами (24 киберкосмическая армия и ещё более 20 упоминавшихся крупных подразделений ВВС и ВМФ США). Меняется, как было показано, и структура стратегического командования ВС США, ориентируясь на боевые действия на геоцентрическом ТВД. Особенность геоцентрического ТВД состоит в том, что не только оружие размещается в космосе, но и сам космос становится действующим элементом комплекса вооружений этого ТВД.

Исключение возможности прохождения оружия геоцентрического ТВД через зону околоземного космоса переводит любые мыслимые военные действия к традиционным двумерным с некоторыми тактическими элементами трёхмерной дистанционной войны, поддерживаемой лишь авиационными средствами. При этом обнуляются и возможности загоризонтных РЛС, а также межконтинентального ракетного оружия с его выходом в околоземное космическое пространство.

В таких условиях шансы вооружённого противостояния держав, обладающих традиционными стратегическими вооружениями, выравниваются. Это, впрочем, не значит, что у России есть значительный временной запас для радикальной, а не показной модернизации своих вооружённых сил, в том числе и для достижения паритета в информационном противоборстве и в вооружениях гео- и гелиоцентрического ТВД.

Опасным недостатком Вооружённых сил Российской Федерации является, во-первых, недооснащённость вооружениями повышенной точности (Великобритания – более 94%/опыт Фольклендской операции, США, Германия – около 90%, Франция – более 60%/, Россия – менее 15%) и, во-вторых, ещё большая недоукомплектованность офицерскими кадрами, способными к эффективному применению оружия повышенной точности. Это, в известной мере, стало результатом бессмысленных реформ и неоправданных, не обеспеченных компенсирующими мероприятиями сокращений численности.

В 1997 году МАН ПНБ был представлен в Совет обороны про Президенте Российской Федерации, согласованный с Академией Генштаба ВС России, Управлением тыла МО РФ, Главкоматом ВМФ России, Управлением внешних сношений ГРУ ГШ ВС России и рядом других заинтересованных ведомств и подразделений МО РФ, и одобрен 17.08.97 Советом проект реформирования военной организации России (приложение 3), предусматривавший радикальное сокращение контингентов, подчинённых МО РФ до численности, соответственной наличию кадров, способных оперировать современными стратегическими и прецизионными вооружениями трёхмерного дистанционного ТВД.

Подразумевалось, что роды и виды войск и специальные подразделения должны обеспечить стратегическими силами защиту интересов Российской Федерации в мире, а силами быстрого реагирования – эффективное противодействие любым видам агрессии.

Компенсация сокращения численности частей Минобороны для поддержания обороноспособности и обеспечения территориальной целостности Российской Федерации предлагалась за счёт формирований Федеральной службы национального резерва России общей численностью, доводимой в течение 3 лет до 6 миллионов человек, в подразделениях постоянного состава (силы МЧС, внутренние войска и другие) и в подразделениях переменного состава (формирования гражданской обороны, казачьи формирования, охранные предприятия и другие) с общей численностью военно-обученного запаса ФСНР РФ ~ 60 миллионов человек, военная подготовка и переподготовка которых может осуществляться в кадрированных частях.

Прошло более 15 лет, ситуация и в стране, и в мире претерпела значительные изменения, и подобный проект, разрабатывавшийся в условиях низходящей ветви развития страны, безусловно, должен пересматриваться в соответствии с этими изменениями. К сожалению, они в большинстве своём неблагоприятны с точки зрения национальной безопасности.

Помимо чисто военных аспектов необходимо учитывать необходимость минимизации зон уязвимости на территории страны и предусматривать с этой точки зрения проведение опережающей военной экспертной оценки всех макроэкономических проектов, представляемых на рассмотрение руководству государства. Например, большое сомнение вызывает проект Минэкономразвития по формированию мегаполисов. Не вдаваясь в содержательную часть этого проекта, можно утверждать, что его реализация в настоящее время несёт угрозу территориальной целостности страны, а сами мегаполисы, за исключением Московского мегаполиса, станут зонами повышенной уязвимости.

Учитывая тот факт, что на вооружении вероятного агрессора находятся климатические и кибернетические вооружения в исполнении, приспособленном к применению как на геоцентрическом ТВД, так и на современном дистанционном трёхмерном ТВД, зонами уязвимости становятся в первую очередь плотины ГЭС (массовая гибель гражданского населения и уничтожение электрогенерирующих мощностей), элементы инфраструктуры в первую очередь железные дороги и мачтовые ЛЭП, а также экосистемы, необходимо осуществить комплекс мер по снижению их уязвимости (повышению устойчивости) на основе существующих разработок, например, представленных в работе[483].

---

483 Спектор ... – Глобализация

Кроме того, предполагая имеющийся запас времени, в качестве защиты от атак кибероружием, осуществляемых при посредстве Интернета, необходимо, используя накопленный опыт Северной Кореи и Китая, самостоятельно создать дублирующий домен Интранета, способный обеспечить безопасное управление не только вооружёнными силами, но и упомянутыми народнохозяйственными структурами, в первую очередь критическими объектами.

Можем ли мы выстоять в развёртывающемся глобальном противоборстве, защитить свою Родину, свою землю, свои семьи? Вопрос не корректен – мы не можем не выстоять в этом противоборстве..

Много раньше русский философ Иван Ильин уже дал ответ на этот вопрос: «Мукою четырнадцати поколений научились мы духовно отстаиваться и в беде, и в смуте; в распадении не теряться; в страдании трезветь и молиться; в несчастии собирать силы; умудряться неудачно и творчески расти от поражения; жить в крайней скудости, незримо богатея духом; не иссякать в истощении, но возрождаться из пепла и на костях; все вновь начинать «ни с чего»; из ничего создавать значительное, прекрасное, великое… и быстро доводить жизнь до расцвета».

С тех пор ещё более 6 поколений русских людей прошли через испытания большевизмом, гражданской войной, войнами против врагов Отечества и смутой, и не может быть сомнения в том, что русский народ преодолеет и эти испытания и Россию ждёт счастливое будущее.

СПИСОК ЛИТЕРАТУРЫ

Shannon C. – The Bandwagon, Trans. IRE, 1956, IT-2, №1.

Шеннон К. – Работы по теории информации и кибернетике (пер. с английского, под ред. Р.Л. Добрушина и О.В. Лупанова) – Изд. иностранной литературы, М,, 1963

Shannon C.E. – Communication in the presence of noise. Proc. Institute of Radio Engineers. Vol. 37,. №1, 1949

Бриллюэн Л. – Наука и теория информации, М., 1960; Научная неопределенность и информация, М., 1966

Королев А.Н., Плешакова О.В. – Об информации, информационных технологиях и о защите информации. Постатейный комментарий к Федеральному закону. – М.: Юстицинформ, 2007.

Колмогоров А.Н. – Комбинаторные основания теории информации и исчисления вероятностей. УМН, 1983, т. 38, вып. 4

Колмогоров А.Н. – Проблемы теории вероятностей и математической статистики. Вестник АН СССР, 1965, №5

Седов Е.А. Одна формула и весь мир (книга об энтропии). М., 1982

Новик И.Б. – Негэнтропия и количество информации. Вопросы философии, 1962, №6

Новик И.Б. – Кибернетика. Философские и социологические проблемы. М., 1963

Урсул А.Д. – Природа информации. М., 1968

Проблема информации в современной науке. М., 1975

Вяткин В.Б. – Введение в синергетическую теорию информации. Информационные технологии, 2010, №12

Чернавский Д.С. – Синергетика и информация (динамическая теория информации) – М., Едиториал УРСС, 2004

Шкляр Я.Е. – Кибертерроризм и информационные войны как средство достижения экономических и геополитических интересов. Центр прогнозирования конфликтов (Методические материалы). Терроризм, часть1, 2006,

Спектор В.Н. – Письмо Председателю Президиума Верховного Совета СССР А.А. Громыко «Замечания к Закону «О государственном предприятии» от 30 июня 1987 года». М., 1987 г.,

Спектор В.Н. – О геополитических последствиях распада СССР и внутриполитической обстановке в России. Выступление на семинаре Политического комитета НАТО. Брюссель. 1992;

Спектор В.Н. – Интервью ЦТ СССР по проблемам конверсии. 1988

Материалы международной конференции «Моноцентровная модель глобализации и её деструктивная роль на Балканах и во всём мире». М., 2008;

Спектор В.Н. – Системный кризис в зеркале национальной безопасности. Труды Всероссийской конференции «Россия: государство и общество на пороге XXI века». М., 1997

Spector V.N., Walters M.B. – In: Joint Declaration on Dual Use Technologies of the delegations of the US National Academy of Sciences and Russian Academy of Sciences. NSF-NAN. Washington, D. C., USA, 1994;

Спектор В.Н., Симонов М.П., Пахомов Л.Г. – Материалы и техника снижения ЭПР за счёт рупорных элементов авиационных комплексов. ИХФ АН СССР – ОКБ Сухого – ГГУ. М. – Горький. 1988

Овчинников А.А., Спектор В.Н. и другие – Полимерный ферромагнетик. Письма в ЖЭТФ (СССР), 1986, том. 43, вып. 6.

Ovchinnikov A.A., Spector V.N. et al – Organic Polymer Ferromagnet. Nature (L), 1987, vol. 326.

Овчинников А.А., Спектор В.Н., Боженко К.В. – Кластерный механизм возникновения отрицательного обменного взаимодействия в продуктах неполного сгорания углеводородов. Известия АН (Россия). Сер.: физическая. 1997, т. 61, №5.

Пахомов Л.Г., Спектор В.Н. – Экологическая катастрофа в Европе уже началась. Независимая газета. 23 июня 1999 г.;

Manning Jerry – Wars are human inventions Коммерсантъ, 7.03. 2000

Manning Jerry – We get what we deserve – we deserve what we get. Proc. IAS PNS. Moscow. 2007, vol. 2, issue 1

Саакашвили. М – «Вероятность возобновления войны снизилась». Информационно аналитический портал «Грузия online», 11.03.2009.

Killing Eternity: Spiritual Genocide in the Territory of the Former SFRY/Library of the Publishing House NIP

Расторгуев С.П. Информационная война. – М: Радио и связь, 1999.

Белая книга Российских спецслужб. – «Обозреватель». М., 1996

Ахо А., Ульман Дж. – Теория синтаксического анализа, перевода и компиляции. Том 1. «Мир». М., 1978,

Налимов В.В. – Спонтанность сознания: Вероятностная теория смыслов и смысловая архитектоника личности. «Прометей». М., МГПИ им. Ленина, 1989

Гриняев С.Н. – Информационная война: история, день сегодняшний и перспектива. *http://itblogs.ru/blogs/donskoy/archive/2006/10/20/8132.aspx*

Гриняев С.Н. – Война в концептуальном пространстве. Открытый исследовательский и дискуссионный центр «Глобальная авантюра». Серия: «Глобальные проблемы», 15 марта 2012

Пивоваров О.Н., Пивоваров И.О., Кудрина Л.И. – Природа живых систем. НИА-Природа, 2002

Н. Винер – Кибернетика, или управление и связь в животном и машине. Советское радио. Наука. М., 1983

Molander Roger C., Riddile Andrew S., Wilson Peter A. – Strategic Information Warfare: a New Face of War. National Defense Research Institute/Report MR-661-OSD prepared for the Office of the Secretary of Defense/RAND. USA, 1996

Михайлов В.М., Спектор В.Н. – Комплекс материалов и технологий для выравнивания поверхностной проводимости в изделиях новой техники. ИХФ АН СССР – ОКБ Сухого. М., 1986;

Прохоров А.М. – Генерация устойчивой гасимой плазмы в заантенных пространствах авиационных комплексов. ИОФ АН СССР – ОКБ Сухого. М., 1986;

Sergiy Pozniy – За что Комитет по международным отношениям ненавидит Путина..»CounterPunch», США, 23.01.08 [*http://www.counterpunch.com*] и *Майк Уитни* – За что Journal Мердока любит Каспарова. «CounterPunch»: STRATEGiUM: ВЕССНА, США, 15. 12. 2007 года

Спектор В.Н. и Воевода Ю.Е. – Подайте вору, Христа ради. Труды МАН ПНБ. М., 1999.

Illine I.A. and Spector V.N. – Think tanks and civil society in Russia. World Bank Conference. Barcelona, Catalonia, Spain

Завадский И.И. Информационная война – что это такое? // Конфидент. Защита информации – 1996.

Libicki M.C. The mesh and the net: Speculation on armed conflict in a time of free silicon. Washington: National defense university, 1994

Зиновьев А.А. «Русский эксперимент»,. 1995., Издательство: L'Age d'Homme – Наш дом

Гельман Захар – Эмират, «Аль-Джазира» и верные полки солдат: Катар стремится к доминированию в арабском мире. Независимая газета: Независимое военное обозрение. [*http://nvo.ng.ru/forces/2012-03-30/1_katar. html*]

Эпштейн М.Н. – Информационный взрыв и травма постмодерна. Русский журнал, 29.10.1998, Эморийский университет, США

Флаксман А.Г. – Адаптивная пространственная обработка в многоканальных информационных системах. Диссертация на соискание учёной степени доктора ф. м. н. М.: РГБ, 2005

Nyquist H. – Certain topics in telegraph transmission theory. Trans. AIEE, vol. 47, 1928

Küpfmüller K. – Über die Dynamik der selbsttätigen Verstärkungsregler. Elektrische Nachrichtentechnik, vol. 5, no. 11, 1928.

K. Küpfmüller, On the dynamics of automatic gain controllers, Elektrische Nachrichtentechnik, vol. 5, no. 11, (English translation).

Котельников В.А. – О пропускной способности «эфира» и проволоки в электросвязи. Успехи физических наук, 2006, №7.

А.А. Харкевич. Спектры и анализ. 4-е изд. М., ЛКИ, 2007.

Meijering Erik – A Chronology of Interpolation From Ancient Astronomy to Modern Signal and Image Processing. Proc. IEEE, 90, 2002. DOI: 10.1109/5.993400;

Джерри А.Дж. – Теорема отсчётов Шеннона, её различные обобщения и приложения. Обзор. ТИИЭР, т. 65, №11, 1977

Хургин Я.И., Яковлев В.П. – Прогресс в Советском Союзе в области теории финитных функций и её применений в физике и технике. ТИИЭР, 1977, т. 65, №7.

Басараб М.А., Зелкин Е.Г., Кравченко В.Ф., Яковлев В.П. – Цифровая обработка сигналов на основе теоремы Уиттекера-Котельникова-Шеннона. Радиотехника. М., 2004

Овчинников А.А., Спектор В.Н., Боженко К.В. – Кластерный механизм возникновения отрицательного обменного взаимодействия в продуктах неполного сгорания углеводородов. Известия АН (Россия). Сер.: физическая. 1997, т. 61, №5.

Спектор В.Н. – Формирование нового мирового устройства: прогнозируемая роль отдельных государств и цивилизационных сообществ (монография, том 1). МАН ПНБ. М., 1997.

Bibickov S.B., Ghorshenyov V.N., Spector V.N. – Simulation, synthesis and investigation of microwave absorbing composite materials. Synth. Metals, 1997, vol. 86,

Рогозин О.К., Данилевич А.А., Цымбал В.И., Рогозин Д.О., Терехов И.И., Рафаилов А.Г., Терехов Г.И., Шунин О.П. – Международная безопасность и обороноспособность государств. НПО «Конверс АВИА». М., 1998.

Дайнес В.О., Данилевич А.А., Пронько В.А. и др. – История военной стратегии России/Под редакцией В.А. Золотарева; Институт военной истории Министерства обороны РФ. М., 2000.

Данилевич А.А., Рогозин Д.О., Рогозин О. К, Савельев А.Н., Слуцкий Л.Э., Терехов И.И., Цымбал В.И. – Война и мир в терминах и определениях/Под общей редакцией Д.О. Рогозина. Издательский дом «ПоРог». М., 2004.

Данилевич А.А., Рогозин О.К., Тихомиров Ю.П., Цымбал В.И. – Понятия, определения и термины по проблеме «Оборонная достаточность». Изд. «Элорма». М., 1992.

Брезкун С.Т. – Подлость генеральских звёзд. Газета «Дуэль» №12 (34), 17 июня 1997 года

Мэннис Аарон, Хендлер Джеймс – Портрет настоящей кибервойны: Опасайтесь вредоносных программ *http://www.inosmi.ru/world/20090806/251360.html*

Онорский Б. – Информационная война – основная форма борьбы ближайшего будущего? Обозреватель/Observer, 1998, №5

Крикунов А., Королев А. – Вопросы обеспечения информационной безопасности в информационно-телекоммуникационных системах при использовании импортных средств связи и информатизации. Журнал «Ассиметричные угрозы и конфликты низкой интенсивности». ЦАТУ, Спецвыпуск. 2009.

Гусаров А. – Защита информации в сетях связи. Военная наука и техника, №2, 2007

А.В. Манойло «Государственная информационная политика в особых условиях», Монография, М.: Изд. МИФИ, 2003 г.

Корли Эрик (Eric Corley) – Американские спецслужбы активно вербуют хакеров. Журнал 2600: The Hacker Quarterly

Американская разведка сделала прогнозы на 2030 год. Российская газета, 10.12.2012

Хамидуллина З. – Американская разведка видит в России угрозу глобальной безопасности. 09.12.2012 investcafe.ru

Атаманов Г.А. – Информационные технологии: плюсы и минусы внедрения. Изд. ВГСХА «Нива». Известия нижневолжского агроуниверситетского комплекса, 2006, №4.

Кастельс М. – Информационная эпоха: экономика, общество, культура/пер. с англ.; ред. О.И. Шкаратана. ГУ ВШЭ. М., 2000.

Дриккер А.С. – Эволюционный прогноз: пульсация народонаселения; Синергетическая парадигма. Нелинейное мышление в науке и искусстве. М., 2004.

Тоффлер Э. – Третья волна. (пер. с англ.). ООО «Издательство АСТ». М., 2002.

Труды МАН ПНБ. М., 1999, том 1,2,3 вып. 1,3,4,5

Труды МАН ПНБ, М., 2008, т. 2, вып. 1,5,

Труды МАН ПНБ. М., 2010, том 2,3, вып. 3,5.

Труды МАН ПНБ. М., 1997, том 1,

Сибиряков С.Л. – Предупреждение девиантного поведения молодёжи (методологические и прикладные проблемы»). Волгоград, 1998

Хакерская группа GhostShell объявила кибервойну России. Интернет. 3.11.2012, © *Flickr.com/gutter/cc-bysa 3.0*

Сунь Цзы «Искусство войны»

Евсеев В.В. – Интервью «Голосу России», октябрь 2012

Глобальные проблемы – www.avanturist.org 15 марта 2012, csef,

Брюссельский сговор: Косово 2008 – «Судеты 1938». Кто станет «Польшей 1939»? Avanturist, 19.02.2008

Hofstadter Richard Social Darvinism in American Thought, Beacon Press, 1992

Ивашов Л. – Климатическое оружие: блеф или реальность? Информационно-аналитический журнал «Асимметричные угрозы и конфликты низкой интенсивности», №9 2010.

Г. Евстафьев «Подводные камни «американской инициативы. *http://www.izvestia.ru/politic/articl e3125399/index.html*

Птичкин С. – Нападать не будем, а за себя постоим: Президент утвердил Военную доктрину Российской Федерации. «Российская газета» – Федеральный выпуск №5104 (25). 08.02.2010

Спектор В.Н., Спектор В.А. – Глобализация, человек, климат и экология планеты (монография, в печати), М., 2012.

Spector V.N. – Consequences of the synthetic regimes for the solid state reactions of oligoorganosilsesquioxanes with various substrates. Plenary Lecture. In: Proceedings of XI International Symposium on Organosilicon Chemistry. France, Montpelier. 1996

Степанов Р.Ф., Спектор В.Н. Оборонный отдел Госплана СССР. М., 1989

Б.И. Радионов, Н.Н. Новичков «Крылатые ракеты в морском бою» Воен. изд-во, 1987

Салливен Джон П. – Террористическое и нетрадиционное оружие. Моркнига. М., 2009 (перевод с английского)

Горшков С.Г. – Морская мощь государства. Военное издательство МО СССР. М., 1976.

Вартанесян В.А. – Радиоэлектронная разведка. М. Воениздат, 1975;

Демин В.П. и др. – Радиоэлектронная разведка и радиомаскировка. М.: Изд-во МАИ, 1997;

Лагутин В.С., Петраков А.В. – Утечка и защита информации в телефонных каналах. М.: Энергоатомиздат, 1996;

Мельников Ю.П. – Воздушная радиотехническая разведка. М.: Радиотехника, 2005;

Меньшаков Ю.К. – Защита объектов и информации от технических средств разведки. М.: РГГУ, 2002.

Радзиевский А.Г., Сирота А.А. – Теоретические основы радиоэлектронной разведки. М.: Радиотехника, 2004;

Хорев А.А. – Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 1998;

Энциклопедия «Оружие и технологии России. XXI век», т. т. 10,11,13

Тараскин М.М., Чешуин С.А. – Взгляды высшего военно-политического руководства ведущих иностранных государств на противодействие угрозам кибернетических войн. Бюллетень «Проблемы безопасности» №3 НИЦ «Наука-XXI»

Горбачев Ю. Е., Тюрин В. М. – К вопросу о «войне в четвертой сфере». Независимое военное обозрение. 20.04 2001

Костюхин А. А., Горбунов Г. С., Сажин А. А. – Информационные операции в планах командования ВС США. Информационный сборник ГШ ВС РФ по зарубежным странам и армиям Центра зарубежной военной информации и коммуникации. 2006, № 3.

Иванов В. – Контрразведывательные операции в киберпространстве. Независимое военное обозрение, 8.02. 2008

Сидоров В. – Кибервойны: от дождя к урагану. Красная Звезда. 26 марта 2008

Соловьев А. А., Метелев С. Е., Зырянова С. А. –Защита информации и информационная безопасность. Омск: Изд-во Омского института РГТЭУ, 2011.

Польских А. – О применении глобальной компьютерной сети Интернет в интересах компьютерного противоборства. Зарубежное военное обозрение. 2005, № 7,

Словарь терминов и определений в области информационной безопасности. НИЦ «Информационной безопасности» ВА ГШ ВС РФ. М., 2008.

Иващенко А. – Борьба Пентагона с террористами в Интернете. Зарубежное военное обозрение. 2006, № 5.

Война в киберэпоху: концепция геоцентрического ТВД http://habrahabr.ru/post/108701/

Spector V.N. – The Russian Perspective on Nuclear and Radiological Terrorism. Доклад на семинаре Департамента по информации и разведке Госдепа США и публичный доклад в Кеннановском Институте. Вашингтон. Дистрикт Колумбия, США, 2006

Бьюкенен Патрик Д. – Чья война? Американский консерватор. 24.03.2003

Бьюкенен Патрик Д. – Восстание в Сирии – не дело Америки. Американский консерватор. 08.06.2012

Истомин Всеволод – Разъединённые Штаты. Газета «Наше время». 19 августа 2007

Хёрд Линда – США больше не способны править миром. «Gulf Times», Арабская пресса. 14 августа 2007 года

Барац А. – «Презумпция человечности» (европейская культура в контексте иудаизма). Иерусалим, 1998

Кларк Ричард, Нейк Роберт – Третья мировая война: какой она будет? Высокие технологии на службе милитаризма. Изд. С-П., 2011 г

США нанесли ядерный удар по Сирии. – Newsland noreply@newsland.ru 3.11. 2007

Материалистическая диалектика в 5 томах. Под редакцией проф. Ф. В. Константинова и В. Г. Марахова. Мысль. М.,1981-1985, том 1

Денисов А.А. – Основы метрологического обеспечения управления конфликтами на геоцентрическом ТВД. Информационные войны, 2011, №3.

Информационные войны, 2010, №2, 3, 4.

Денисов А.А. – Системы, превосходящие исследователя по совершенству. IV Международная конференция по проблемам управления. Сборник Трудов. Институт управления им. Трапезникова РАН, 2009, с.

Денисов А.А. – «Призрачные» субъекты в управлении военным и политическим конфликтом. Государственная служба, 2010, №2.

Лефевр В. – Рефлексия. «Когито-центр». М., 2003 г.

Ивлев А.А. – Основы теории Бойда. Направления развития, применения и реализации. М., 2008

Щекотихин В.М.; Королёв А.В.; Королёва В.В., Крикунов А.В., Сёмкин С.Н. – Основы противодействия информационной войне. Академия ФСО России. Орёл, 2009.

Комментарий официального представителя МИД России о прекращении деятельности в Российской Федерации USAID. МИД РФ. Официальный сайт. 19.09.12;

Slaughter Anne-Marie, Wright Thomas – Punishment to Fit the Nuclear Crime. Presented by Cynthia Zeiss. The Washington Post. 2007

Spector V.N. – Dealing with Nuclear Crimes. letters@washpost.com

Nesterikhin Yu.E. – Plenary Report on DUT Interacademy (RF-US) Meeting. M., 1992

Материалы Десятого Национального форума информационной безопасности. Москва, 31 января – 1 февраля 2008 г.;

Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 9 сентября 2000 г., №1895.

Рыжков В.И. – Информационные технологии в государственном и муниципальном управлении. Учебное пособие. Хабаровск: Дальневосточная академия государственной службы, 2004,

Новиков А.А., Устинов Г.Н. – Уязвимость и информационная безопасность телекоммуникационных технологий. Учебное пособие для вузов. Радио и связь. М., 2003.

Онорский Б. – Информационная война – основная форма борьбы ближайшего будущего? Обозреватель/Observer, 1998, №5

Черешкин Д.С., Смолян Г.Л. – Нелегкая судьба российской информатизации. Информационное общество, 2008, вып. 1-2,

Гриняев С., Кудрявцев В., Родионов Б. – Информационная безопасность избирательных кампаний. МАКБП. М., 1999.

Гриняев С.Н. – США развертывают систему информационной безопасности. Независимое военное обозрение; Война в четвертой сфере. Неза-

висимое военное обозрение; Системы обнаружения вторжений на основе мобильных программ-агентов [Connect! Мир связи, №7, 2001

Официальный сайт директора Национальной разведки США, http://www.dni.gov

Бетц Дэвид Дж. -. Революция в военном деле и «армейские операции вне условий войны»: Обоюдоострое оружие [*http://www.strana-oz.ru/?numid=26&article=1133*]

Deleuze Gilles et Guattari Felix – Rhizome Capitalisme et schizophrénie. Mille plateaux. Les Editions de Minuit. Paris, 1980

Беликова Ю.В., Крикунов А.В., Королёв А.В. – Сетевые технологии в информационных операциях НАТО и зарубежных неправительственных организаций в ходе цветных революций и военных конфликтов. ЦАТУ. М., Академия ФСО России, 2012,

Савин Леонид – Кибердиссиденты. Интернет. «Фонд стратегической культуры». 02.04.2012

Noah Shachtman. Exclusive: Darpa Director Bolts Pentagon for Google. March 12, 2012.

Кауфман Стивен – Как обеспечить собственную безопасность и свободу, пользуясь средствами связи. 10 ноября 2011 года. *http://iipdigital.usembassy.gov*

Müller Milton L. – Networks and States: The Global Politics of Internet Governance. MIT Press, 2010

Чолиа С. – Добрые советы от «Freedom House». НПО как инструмент «цветных революций» на постсоветском пространстве. [*http://scienceport.ru*

Макеев М. – Механизмы влияния США на Россию и СНГ

Буш: демократические революции придут на Кавказ и в Среднюю Азию», [*www.rian.ru/politics/20050519/40378390.html*]

Ильин В.М. – Новейшие технологии XXI века в борьбе за души людей. *http://www.kongord.ru/Index/A_tma_06/newtecheatsoul. html*

Дугин А. – Сетецентричные войны. 08.02.2006 [*http://wwwevrazia.org/modules. php?name=News&file=article&sid=2893*]

Димлевич Н. – Информационное противоборство в современном мире. Инфофорум, №45, ноябрь 2009.

«Модулирование поведения» – война против всех. http://vlasti.net/news/79945

Бодвунов А. – НПО: сетевая война против России. Сетевые войны: угроза нового поколения. Евразийское движение. М., 2009,

GLOBAL TRENDS 2015: A Dialogue About the Future With Nongovernment Experts. [*http://www.dni.gov/nic/NIC_globaltrend2015.html*]

Phillips W.R. – Civil-Military Cooperation: Vital to Peace Implementation in Bosnia. NATO Review. 1998, Vol. 46, №1,

Сурков Н. – США проигрывают мировую информационную войну. Независимая газета, 04.03.2011

Олегин А., Сатаров В, – США: ставка на абсолютное превосходство. Журнал «Отечественные записки» №5 (26), 2005

Владимир Большаков «Мир в оранжевых сетях», Столетие. Ru, 18.04. 2008

Субетто А. И. – Капиталократическая эсхатология и мондиализм. «Академия Тринитаризма», М.,Интернет: Эл №77-6567, публ. 10796, 05.11.2003

Нарочницкая Н. А. Оранжевые сети: от Белграда до Бишкека/Под ред. д. и. н. Н. А. Нарочницкой. Алетейя. Санкт-Петербург, 2008

Нарочницкая Н. А. Карла дель Понте 5 лет молчала о злодеяниях албанцев в Косово. Православие и Мир. 8 апреля 2008 г.

Нарочницкая Н. А. – Границы становятся зыбкими: Косово – разменная фигура для США. Столетие. Ru. 25.02.2008

Рябов Кирилл – Новая линия фронта: Интернет. 02.10.2012

Ерофеев Андрей – В русле арт-активизма. Интернет. 13.08. 2012.

А. П. Девятов Разведывательная служба «МИ-6», «Опиумная война» и безопасность Олимпиады –23.08.2008

Выступление заместителя секретаря Совета Безопасности РФ В. Соболева на II Международной конференции «Терроризм и электронные СМИ», Айя-Нап, Кипр, 6-11 ноября 2006

«Звездные войны», которых не было. http://www.buran.ru/htm/str163.htm

Спектор В. Н. – Стратегия десуверенизации как основная угроза национальной безопасности. Пленарный доклад на 1 секции Международного симпозиума Интерполитех-2011. М., 2011.

Европа не верит рейтинговым агентствам 03.07.2012, Forbes Russia.

Европейского рейтингового агентства не будет. [*vestifinance.ru*] Апрель 19, 2012.

Россия и Китай создают рейтинговое агентство – «конкурента большой тройки», *www.ziwa.org*.

Beaumont Peter – Chinese ratings agency threatens US with new debt downgrade. The Guardian (London). 11 November 2011 Dagong, the new Chinese bad guy or a fair player?»,SACR, 21 mars 2012

Арзуманян Рачья – Новые задачи Пентагона в «Стратегическом руководстве по обороне». Глобальные проблемы, 25 января 2012. [*http://www.csef.ru*]

Lee R. – The Far East between Russia, China, and America, Foreign Policy Research Institute. E-Notes, July 2012;

Lukin A. – Russia and America in the Asia-Pacific: A New Entente? Asian Politics and Policy, 2012, Vol. 4, №2.

Спектор В. Н. – Служебная записка в СБ РФ, копия: в ФСБ РФ, ноябрь 2011.

Barnett, Thomas P.M. – The Pentagon's New Map: War and Peace in the Twenty-First Century. Putnam Publishing Group. 2004

Olson, Eric T. – Special Operations: Context and Capabilities in Irregular Warfare. Joint Force Quarterly (JFQ), Issue 65, First Quarter 2010,

Арзуманян, Рачья В. – Сложное мышление и Сеть: парадигма нелинейности и среда безопасности 21 века. Ереван: Научно-образовательный фонд «Нораванк», 2011

R. Tsu and L. Esaki. «Tunneling in a finite superlattice». Applied Physics Letters, 1973, vol. 22, DOI:

Спектор В.Н. – Константы нестойкости комплексов производных хинолина и акридина с солями производных хинолиния и акридиния. Сб. Материалы Всесоюзной конференции по термодинамике органических соединений. Изд. ГГУ. Горький, 1973.

Соборовер Э.И., Мухина Г.Н., Пахомов Л.Г., Спектор В.Н. – Константы нестойкости комплексов производных хинолина и акридина с солями производных хинолиния и акридиния.

«Электроника органических материалов». Изд. «Наука». М., 1985,

Малыгин А.А. – Химия поверхности и синтез многокомпонентных оксидных наноструктур методом молекулярного наслаивания. В кн.: Труды XVII Менделеевского съезда по общей и прикладной химии. Казань, 2003.

Гнеденко Б.В. – Курс теории вероятностей, 5 издание, М., 1969;

Прохоров Ю.В., Розанов Ю.А. – Теория вероятностей, 2 издание. М., 1973

Ляпунов А.М. – Новая форма теоремы о пределе вероятности. Собрание сочинений, том 1, М., 1954, с.

Ляпунов А.М. – Избранные труды. Л., 1948

Хюпенен Анатолий, Покладов Сергей – Кто организует борьбу на новом ТВД? Необходим военный учебно-научный центр ВКО. Общероссийская газета «Военно-промышленный курьер ВПК»

Хюпенен А.И. – Крах трёх академий. Военно-промышленный курьер. 2012

Спектор В.Н. – Геополитическая концепция Договора о противодействии распространению ядерных вооружений, оружия массового поражения и средств их доставки. Лекция и семинар в Управлении информации и разведки Госдепа США. Вашингтон. США, 2006

Путин В.В. – Мюнхенское выступление. *archive.kremlin.ru*

Программа конверсии оборонного потенциала в области материалов и технологий. Госплан СССР. М., 1989, в трёх томах

Пахомов Л.Г. – Автореферат докторской диссертации. ИХФ АН СССР. М., 1990,

Олег Демидов. Социальные сетевые сервисы в контексте международной и национальной безопасности [Электронный ресурс] // ПИР-Центр.– 2011.– Режим доступа: http://www.pircenter.org/kosdata/page_doc/p2714_1.pdf

Евгений Морозов: «Moldova's Twitter Revolution» (Net Effect, 7 апреля 2009) neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution).

Julius Court. People Power II in the Philippines: The First E-Revolution? [Electronic resource]/Background Paper.– Overseas Development Institute, January 2001.– Mode of access: www.odi.org.uk/resources/details.asp?id=3147&title=people-power-iiphilippines-first-e-revolution.

Пользователи Facebook готовят новую революцию – в Сирии [Электронный ресурс] // БалтИнфо, 27 февраля 2011.– Режим доступа: http://www.baltinfo.ru/2011/02/27/Polzovateli-Facebook-gotovyat-novuyu-revolyutciyu-190430

Freedom on the Net 2011 [Electronic resource]/Freedom House, 2011.– Mode of access: http://www.freedomhouse.org/report/freedom-net/freedom-net-2011

International Telecommunication Union 2009 (http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx) и Social Map (http://geographics.cz/socialMap/)

Andrew Sullivan. The Revolution Will Be Twittered [Electronic resource]/The Atlantic, The Daily Dish, 13 June 2009.– Mode of access: http://andrewsullivan.theatlantic.com/the_daily_dish/2009/06/the-revolution-will-be-twittered-1.html

Thomas Sander. Why the revolution won't be tweeted [Electronic resource]/Social Capital Blog, September 29, 2010.– Mode of access: http://socialcapital.wordpress.com/2010/09/29/why-the-revolution-wont-be-tweeted/

Malcolm Gladwell. Social media platforms and revolutions [Electronic video resource]/CNN, March 27, 2011.– Mode of access: http://vijana.fm/2011/04/04/social-media-and-revolutions/

Malcolm Gladwell, Clay Shirky. From Innovation to Revolution [Electronic resource]/Foreign Affairs.– Council on Foreign Relations, March/April 2011.– Mode of access: http://www.foreignaffairs.com/articles/67325/malcolm-gladwell-and-clay-shirky/from-innovation-to-revolution

David Weinberger. Gladwell proves too much [Electronic resource]/Joho the Blog, February 4, 2011. Mode of access: http://www.hyperorg.com/blogger/2011/02/04/gladwell-proves-too-much/

http://twitter.com/anthonyshadid

http://twitter.com/#!/jilliancyork/status/25972726774636544

http://twitter.com/#!/techsoc/status/25973597747023872

http://twitter.com/#!/techsoc/status/25984459006279680

Evgeny Morozov. Why the internet is failing Iran's activists [Electronic resource]/Prospect Magazine, January 5, 2010.– Mode of access: http://www.prospectmagazine.co.uk/2010/01/why-the-internet-is-failing-irans-activists/

Evgeny Morozov. How dictators watch us on the web [Electronic resource]/Prospect Magazine, November 18, 2009.– Mode of access: http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/

Patrick Philippe Meier Where I Disagree with Morozov vs Shirky on Digital Activism [Electronic resource]/iRevolution. From innovation to revolution, January 7, 2010.– Mode of access: http://irevolution.net/2010/01/07/morozov-vs-shirky/

Catherine O'Donnell. New study quantifies use of social media in Arab Spring [Electronic resource]/University of Washington, September 12, 2011.– Mode of access: http://www.washington.edu/news/articles/new-study-quantifies-use-of-social-media-in-arab-spring

Clay Shirky. The Political Power of Social Media [Electronic resource]/Foreign Affairs.– Council on Foreign Relations, January/February 2011.– Mode of access: http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media

Yousri Marzouki, Inès Skandrani-Marzouki, Moez Béjaoui, Haythem Hammoudi, and Tarek Bellâj. The Contribution of Facebook to the 2011 Tunisian Revolution: A Cyberpsychological Insight [Electronic resource]/Cyberpsychology, Behavior, and Social Networking, May 2012, 15 (5).– p. 237-244.– Mode of access: http://online.liebertpub.com/doi/abs/10.1089/cyber.2011.0177.

Андрей Коротаев, Леонид Исаев. Революция бугров и разломов [Электронный ресурс] // Эксперт, 2012, №30-31 (813),.– Режим доступа: http://expert.ru/download/1/magazine/381960/

Сергей Долмов. Вирус в колыбели [Электронный ресурс] // Эксперт, 2012, №30-31 (813), стр.18.– Режим доступа: http://expert.ru/download/1/magazine/381960/

Бедность в мире [Электронный ресурс] // RATE1, 11 сентября 2009.– Режим доступа: http://www.rate1.com.ua/issledovanija-rate1/1290/

Сергей Филатов. Ближний Восток: «Идеальный шторм» [Электронный ресурс] // Международная жизнь, 28 февраля 2011.– Режим доступа: http://interaffairs.ru/read.php?item=664

Philip N. Howard. Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring? [Electronic resource]/Project on Information Technology and Political Islam, September 11, 2011.– Mode of access: http://pitpi.org/?p=1051

Freedom on the Net 2011 – Iran [Electronic resource]/Freedom House, 2011.– Mode of access: http://www.unhcr.org/refworld/pdfid/4dad51b6d.pdf

«Секреты «Цветных революций», Елена Пономарева, журнал «Свободная мысль», 2012, № 1/2 (1631)

Михаил Остроменский. Основы противодействия гражданского общества «цветным» революциям [Электронный ресурс] // Война и мир, 23 октября 201.– Режим доступа: www.warandpeace.ru/ru/exclusive/view/62983/

С. Марков. Цветная революция – это новый тип политических технологий по смене политической

власти [Электронный ресурс] // km.ru, 15 ноября 2005.– Режим доступа: www.km.ru/glavnoe/2005/11/15/arkhiv/

Сергей Грачев. Информационные технологии в египетских событиях 2011 года. [Электронный ресурс] // Вестник Института стратегических исследований ПГЛУ, 2012, № 3.– Режим доступа: http://www.pglu.ru/science/researches/niipanin/vestnik/v3/Grachev_Sheshneva_Zavjalov.pdf

Jon Swaine. Egypt crisis: the young revolutionaries who sparked the protests [Electronic resource]/The Telegraph, February 11, 2009.– Mode of access: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8317055/Egypt-crisis-the-young-revolutionaries-who-sparked-the-protests.html

Мартин Флетчер. Толпы приветствуют мечтателя из Facebook, вдохновившего нацию [Электронный ресурс] // Инопресса, 9 февраля 2011.– Режим доступа: http://www.inopressa.ru/article/09Feb2011/times/facebook.html

Julian Assange. The Banality of 'Don't Be Evil'. [Electronic resource]/The New York Times, June 1, 2013.– Mode of access: http://www.nytimes.com/2013/06/02/opinion/sunday/the-banality-of-googles-dont-be-evil.html?smid=tw-share&_r=3&

Courtney Radsh. Core to Commonplace: The evolution of Egypt's blogosphere [Electronic resource]/

Arab media society, Issue 6, Fall 2008.– Mode of access: http://www.arabmediasociety.com/?article=692

Bloggers Learn New Media Tools [Electronic resource]/Freedom house,– Mode of access: http://www.freedomhouse.org/template.cfm?page=115&program=84&item=87

БИТВА ЗА ВОСТОК. ЧАСТЬ II. Египетское «Движение 6 апреля» – арабский «Отпор»? [Электронный ресурс] // WORLD INVESTIGATION NET.– Режим доступа: http://old.win.ru/win/8045.phtml

За революцией в Египте стоит Вашингтон [Электронный ресурс] // LR News, 31 января 2011.– Режим доступа: http://lrnews.ru/news/full/25311/

Secretary Rice Meets with 'New Generation' of Egyptian Reformers [Electronic resource]/Freedom house, December 2007.– Mode of access:

http://www.freedomhouse.org/article/secretary-rice-meets-new-generation-egyptian-reformers

Карякин В.В. Наступила эпоха следующего поколения войн – информационно-сетевых. Каков будет наш ответ на этот вызов? [Электронный ресурс] // Зарубежное военное обозрение, 22 апреля 2011.– Режим доступа: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html

Елена Пономарева, «Секреты «Цветных революций» (продолжение) [Электронный ресурс] // Свободная мысль, 2012, №3/4 (1632), стр. 43.– Режим доступа: http://svom.info/media/files/2012/07/04/Svobodnaya_misl_3.pdf

Darlene Storm. Army of Fake Social Media Friends to Promote Propaganda [Electronic resource]/PCWorld, February 23, 2011.– Mode of access: http://www.pcworld.com/article/220495/army_of_fake_social_media_friends_to_promote_propaganda.html

George Monbiot. The need to protect the internet from 'astroturfing' grows ever moreurgent[Electronicresource]/TheGuardian,February232011.–Modeofaccess: http://www.guardian.co.uk/environment/georgemonbiot/2011/feb/23/need-to-protect-internet-from-astroturfing

http://www.nytimes.com/2011/02/17/world/middleeast/17sharp.html?pagewanted=all&_r=1&

http://www.bbc.co.uk/russian/international/2012/02/120217_gene_sharp_revolutions_interview.shtml

http://www.ng.ru/world/2011-02-18/1_revolutions.html

Джин Шарп. От диктатуры к демократии. Режим доступа: http://www.aeinstein.org/organizations/org/FDTD_Russian.pdf

M.C. Joyce. Stories of Mobilization.– www.metaactivism.org/2011/06

Джин Шарп. 198 методов ненасильственных действий. [Электронный ресурс] // Режим доступа: http://www.aeinstein.org/organizations/org/FDTD_Russian.pdf

Enemies of the Internet [Electronic resource]/Reporters Without Borders, 2011.– Mode of access: march12.rsf.org/i/Internet_Enemies.pdf

Freedom of the Press 2009 – Egypt [Electronic resource]/Freedom House, 2009.– Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2009/egypt

Freedom of the Press 2010 – Egypt [Electronic resource]/Freedom House, 2010.– Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2010/egypt

В Египте арестованы два журналиста «Аль-Джазиры» [Электронный ресурс] // rin.ru, 8 апреля 2010.– Режим доступа: http://news.rin.ru/news_text/160058/

Online Censorship in the Middle East and North Africa [Electronic resource]/Human Rights Watch, November 2005 Volume 17, No. 10 (E).– Mode of access: http://www.hrw.org/sites/default/files/reports/mena1105webwcover.pdf

Rafael Lorente. Freedom House: Press freedom dropped to lowest point in a decade in 2010 [Electronic resource]/February 2, 2011.– Mode of access: http://ijnet.org/stories/freedom-house-press-freedom-dropped-lowest-point-decade-2010

Freedom on the Net 2011- Egypt [Electronic resource] Freedom House, 2011.– Mode of access: http://www.freedomhouse.org/sites/default/files/inline_images/Egypt_FOTN2011.pdf

Enemies of the Internet – Countries under surveillance [Electronic resource]/Reporters Without Borders, 2010.– Mode of access: http://en.rsf.org/IMG/pdf/Internet_enemies.pdf

Press Freedom Index 2009 [Electronic resource]/Reporters Without Borders, 2009.– Mode of access: http://en.rsf.org/press-freedom-index-2009,1001.html

Freedom of the Press 2008 – Iran [Electronic resource]/Freedom House, 2008.– Mode of access: http://expression.freedomhouse.org/reports/freedom_of_the_press/2008/iran

FIDH and LDDHI condemn the death sentence for Kurdish journalists in Iran [Electronic resource]/kurd.net, July 26, 2007.– Mode of access: http://www.ekurd.net/mismas/articles/misc2007/7/irankurdistan274.htm

Internet Filtering in Tunisia [Electronic resource]/Open Net Initiative, 2009.– Mode of access: http://opennet.net/sites/opennet.net/files/ONI_Tunisia_2009.pdf

Helmi Noman, Jillian C. York. West Censoring East: The Use of Western Technologies by Middle East

Censors, 2010-2011 [Electronic resource]/OpenNet Initative, March 2011.– Mode of access: opennet.net/west-censoring-east-the-use-westerntechnologies-middle-east-censors-2010-2011

В Иране начались демонстрации протеста против переизбрания Ахмадинеджада [Электронный ресурс] // lenta.ru, 13 июня 2009.– Режим доступа: http://lenta.ru/news/2009/06/13/iran/

Мобильная связь и веб-сайты отключены в Тегеране на фоне протестов [Электронный ресурс] // РИА Новости, 14 июня 2009.– Режим доступа: http://ria.ru/world/20090614/174300365.html

'Neda' becomes rallying cry for Iranian protests [Electronic resource]/CNN, June 22, 2009.– Mode of access: http://edition.cnn.com/2009/WORLD/meast/06/21/iran.woman.twitter/

The Top 10 Everything of 2009 [Electronic resource]/Time, December 08,

2009.– Mode of access: http://www.time.com/time/specials/packages/article/0,28804,1945379_1944701_1944705,00.html

Anonymous video of Neda Aghan-Soltan's death wins Polk award [Electronic resource]/The Guardian, February 16, 2010.– Mode of access: http://www.guardian.co.uk/media/pda/2010/feb/16/george-polk-awards

Angela Moscaritolo. Iran election protesters use Twitter to recruit hackers [Electronic resource]/SC Magazine, June 15, 2009.– Mode of access: http://www.scmagazine.com/iran-election-protesters-use-twitter-to-recruit-hackers/article/138545/

Katie Combs. Iran's «Twitter Revolution» – myth or reality? [Electronic resource]/World Focus, June 19, 2009.– Mode of access: http://worldfocus.org/blog/2009/06/18/irans-twitter-revolution-myth-or-reality/5869/

Alex Comninos. 2011 – Internet rights and democratization [Electronic resource]/Global Information Society Watch, 2011.– Mode of access: http://www.giswatch.org/ca/node/511

US embassy cables: The 'OTT' lifestyle of Tunisian president's son-in-law, including pet tiger [Electronic resource]/The Guardian, 7 December 2010.–Mode of access: http://www.guardian.co.uk/world/us-embassy-cables-documents/218324

Yasmine Ryan. Tunisia's bitter cyberwar [Electronic resource]/Al Jazeera, 06 January, 2011.– Mode of access: http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html

David D. Kirkpatrick. Mubarak Orders Crackdown, With Revolt Sweeping Egypt [Electronic resource]/The New York Times, January 28, 2011.– Mode of access: http://www.nytimes.com/2011/01/29/world/middleeast/29unrest.html?_r=1&hp

Маликов С. С. Internet. История развития и принципы работы, протоколы передачи данных, система адресации. Сервисы Internet: электронная почта, форум, ICQ, файловая передача, среда WorldWideWeb, среда поиска информации. CoolReferat.com)

Кубякин Е. О Информационный экстремизм как феномен социокоммуникативной реальности XX1 в.– научный журнал «Гуманитарные, социально – экономические и общественные науки». В.№ 1-2011 г.)

СОДЕРЖАНИЕ

УДК 004.6
ББК 30
Т 82

Научное издание

Т.Д. ТУЛЕШОВ, В.Н. СПЕКТОР

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК СПОСОБ ЗАЩИТЫ ГЕОПОЛИТИЧЕСКИХ ИНТЕРЕСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Издание осуществляется Европейским учебным институтом
при МГИМО (У) МИД РФ

НАУЧНЫЕ РЕЦЕНЗЕНТЫ:

О.Н. Барабанов – заведующий кафедрой политики и
функционирования ЕС и Совета Европы
МГИМО – Университета МИД России,
доктор политических наук, профессор;
В.Н. Лихачев – Чрезвычайный и Полномочный посол РФ,
доктор юридических наук, профессор;
А.А. Новиков-Ланской – заведующий кафедрой
политической и деловой журналистики РАНХИГС
при Президенте РФ, кандидат филологических наук

Тираж 1000 экз.

Подписано в печать 17.03.15. Формат 70x100/16. Объем 29,0 п. л.
Заказ № 16143
Отпечатано по заказу компании «АРТИДИ»
в типографии ООО «B2B Принт», г. Москва

ISBN 9785427000991