В. С. Овчинский

Криминология цифрового мира

Учебник для магистратуры

НОРМА
ИНФРА-М
Москва, 2018

УДК 343.9::004.738.5(075.8)
ББК 67.51я73
О35

Автор

Владимир Семенович Овчинский — доктор юридических наук, заслуженный юрист РФ, советник министра внутренних дел РФ.

Рецензенты

Осипенко А. Л. — доктор юридических наук, профессор, заместитель начальника Воронежского юридического института МВД России.

Сундиев И. Ю. — доктор философских наук, профессор, главный научный сотрудник ВНИИ МВД России.

Овчинский В. С.

О35 Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. — М. : Норма : ИНФРА-М, 2018. — 352 с.

ISBN 978-5-91768-896-1 (Норма)
ISBN 978-5-16-013659-2 (ИНФРА-М, print)
ISBN 978-5-16-106320-0 (ИНФРА-М, online)

Учебник посвящен актуальным вопросам криминологического анализа преступности цифрового мира и мерам ее предупреждения.

Для магистрантов, специализирующихся в области криминологии и информационной безопасности.

УДК 343.9::004.738.5(075.8)
ББК 67.51я73

ISBN 978-5-91768-896-1 (Норма)
ISBN 978-5-16-013659-2 (ИНФРА-М, print)
ISBN 978-5-16-106320-0 (ИНФРА-М, online)

Оглавление

Раздел II
Преступность цифрового мира

Раздел III
Преступники и девианты цифрового мира

Раздел IV
Предупреждение преступлений в цифровом мире

Введение

Цифровой мир XXI в. — системное понятие, интегрирующее такие категории, как цифровая среда (пространство), цифровые технологии, цифровое общество, цифровая экономика, цифровое государство и граждане цифрового мира.

В 2017 г. цифровая революция вошла в решающую фазу — к Интернету подключился каждый второй житель Земли. По оценке Глобального института McKinsey (MGI), уже в ближайшие 20 лет до 50% рабочих операций в мире могут быть автоматизированы, и по масштабам этот процесс будет сопоставим с промышленной революцией XVIII—XIX вв.

Россия уже живет в цифровой эре: по количеству пользователей Интернета она занимает первое место в Европе и шестое — в мире. За последние три года смартфонов у нас стало вдвое больше — теперь они есть у 60% населения. Это больше, чем в Бразилии, Индии и странах Восточной Европы[1].

Цифровые преобразования — один из главных факторов мирового экономического роста. По оценкам Глобального института McKinsey, в Китае до 22% увеличения ВВП к 2025 г. может произойти за счет итернет-технологий. В США ожидаемый прирост стоимости, создаваемый цифровыми технологиями, впечатляет не меньше — здесь он к 2025 г. может составить 1,6—2,2 трлн долл. США.

По оценкам Глобального института McKinsey, потенциальный экономический эффект от цифровизации экономики России увеличит ВВП страны к 2025 г. на 4,1—8,9 трлн руб. (в ценах 2015 г.), что составит от 19 до 34% общего ожидаемого роста ВВП[2].

Такие смелые экономические прогнозы связаны не только с эффектом от автоматизации существующих процессов, но и с внедрением принципиально новых, прорывных бизнес-моделей и технологий. Среди них — цифровые платформы, цифровые экосистемы, углубленная аналитика больших массивов данных, технологии «Индустрии-4.0», такие как 3D-печать, роботизация, «Интернет вещей» (Internat of Things, IoT).

Как отмечено в концептуальных документах стран — лидеров цифрового мира, важнейшим *критерием перехода* страны в цифровой

[1] См.: Цифровая Россия: новая реальность: отчет / Digital/McKinsey. Июль, 2017 // URL: http://apptractor.ru.
[2] Там же.

мир является всеобщая связанность, интеграция личных девайсов (многофункциональных устройств), общественных сетей, корпоративных систем и правительственных инфраструктур в единое целое — цифровой взаимосвязанный мир. Это открывает невиданные возможности, но одновременно делает нас обитателями дома со стеклянными стенами. В данном случае возможности, риски и угрозы растут пропорционально и экспоненциально.

Данный факт требует кардинального *изменения подхода к национальной цифровой безопасности и кибербезопасности* как несущей конструкции цифровой безопасности.

Криминология цифрового мира представляет собой, с одной стороны, часть общей науки криминологии, на которую распространяется традиционное учение о причинах преступности, личности преступника, мерах предупреждения преступлений. С другой стороны, учитывая специфический характер самого цифрового мира, действующей в нем преступности и факторов, ее детерминирующих, криминология цифрового мира может рассматриваться как самостоятельная наука, предполагающая также и самостоятельную учебную дисциплину.

Актуальность такой учебной дисциплины весьма велика.

Как отмечено в *Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы*, утв. Указом Президента РФ от 9 мая 2017 г. № 203 (далее — Стратегия развития информационного общества), в России с 2014 г. осуществляется подключение населенных пунктов с населением от 250 до 500 человек к сети Интернет, в результате чего 5 млн граждан России, проживающих почти в 14 тыс. таких малонаселенных пунктов, получат доступ к сети Интернет. Уже сейчас в среднем на одного россиянина приходится два абонентских номера мобильной связи. Электронные средства массовой информации, информационные системы, социальные сети, доступ к которым осуществляется с использованием сети Интернет, стали частью повседневной жизни россиян. Пользователями российского сегмента сети Интернет в 2016 г. стали более 80 млн человек.

Информационные и коммуникационные технологии оказывают существенное влияние на развитие традиционных отраслей экономики. Объем реализации товаров и услуг россиянам с использованием сети Интернет в 2015 г. достиг эквивалента 2,3% ВВП и имеет тенденцию к росту.

Информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

В России наряду с задачей обеспечения всеобщего доступа к информационным и коммуникационным технологиям актуальной является проблема *интенсификации использования самих технологий*. Технологии, созданные на основе передовых знаний (нано- и биотехнологии, оптические технологии, искусственный интеллект, альтернативные источники энергии), становятся доступными.

Развитие технологий сбора и анализа данных, обмена ими, управления производственными процессами осуществляется на основе внедрения *когнитивных технологий, их конвергенции с нано- и биотехнологиями*. Значительное увеличение объема данных, источниками и средствами распространения которых являются промышленные и социальные объекты, различные электронные устройства, приводит к формированию новых технологий. Повсеместное применение таких технологий способствует развитию нового этапа экономики — *цифровой экономики* и образованию ее экосистемы.

Главным способом обеспечения эффективности цифровой экономики становится внедрение технологии обработки данных, что позволит уменьшить затраты при производстве товаров и оказании услуг.

В то же время в Стратегии развития информационного общества отмечено, что с использованием сети Интернет все чаще совершаются компьютерные атаки на государственные и частные информационные ресурсы, объекты критической информационной инфраструктуры.

Международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети Интернет, не установлены. Большинство государств (в том числе Россия) вынуждены «на ходу» адаптировать государственное регулирование сферы информации и информационных технологий к новым обстоятельствам.

Со Стратегией развития информационного общества неразрывно связан другой основополагающий документ — *Доктрина информационной безопасности Российской Федерации*, утв. Указом Президента РФ от 5 декабря 2016 г. № 646 (далее — Доктрина информационной безопасности). В ней даны оценки, напрямую связанные с криминологической характеристикой ситуации. В частности, отмечено, что различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической

деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Особо подчеркнуто, что возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

В Доктрине информационной безопасности делается вывод о том, что состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении России, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности России.

В связи с этим в учебнике рассмотрены понятие и элементы цифрового мира; технологии цифрового мира в эпоху третьей и четвертой промышленных революций; криминогенные факторы, действующие в эпоху третьей и четвертой промышленных революций; особенности преступности, терроризма и экстремизма цифрового мира; личности преступников и преступных организаций, действующих в цифровом мире; меры предупреждения преступлений в цифровом мире.

Раздел I
ЦИФРОВОЙ МИР КАК ОБЪЕКТ КРИМИНОЛОГИЧЕСКОГО АНАЛИЗА

Глава 1. Элементы и содержание цифрового мира

§ 1. Цифровая среда (пространство)

Для целей данного учебника понятие цифровой среды (пространства) во многом идентично мировому пониманию *информационного пространства*, определяемого Стратегией развития информационного общества как совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

Что касается понятия *информационной инфраструктуры* России, то в учебнике используется определение, даваемое в Доктрине информационной безопасности. Это совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории России, а также на территориях, находящихся под юрисдикцией России или используемых на основании международных договоров России.

Информационная среда существует столько же, сколько существует человечество. Менялись лишь средства коммуникации, способы хранения и предоставления информации, уровень ее доступности.

Цифровое пространство представляет собой метафору, характеризующую пространство распространения сигналов в любых управляющих системах[1].

Очевидно, что цифровая среда (пространство) получила принципиально новое качество с появлением Интернета, базирующегося на информационных технологиях и электронно-вычислительной технике. В основе любых вычислений лежат операции с цифрами. Поэтому буквально в последние годы и в официальных выступлениях, и в публикациях, и в терминологии различных профессиональных сообществ, включая политиков, военных, стратегистов и т. п., и в повседневном языке все чаще используется термин «цифровая среда».

[1] См.: *Ларина Е., Овчинский В.* Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М., 2014.

Определяющим элементом для цифровой среды являются *цифровые технологии* (англ.: digital technology). Цифровая технология в отличие от аналоговой работает с дискретными, а не с непрерывными сигналами.

Цифровые технологии главным образом используются в вычислительной цифровой электронике, прежде всего компьютерах, в различных областях электротехники, таких как игровые автоматы, робототехника, автоматизация, измерительные приборы, радио- и телекоммуникационные устройства и многие другие цифровые устройства.

Цифровая среда имеет собственные:

— инфраструктуру. Она включает в себя: телекоммуникационные и интернет-линии (оптоволоконные кабели и т. п.); вычислительные комплексы различной размерности — от суперкомпьютеров до смартфонов и планшетных компьютеров; вычислительные управляющие встроенные блоки в различного рода объекты физического мира, начиная от производственных линий и заканчивая кроссовками и майками, соединенными в цифровое пространство;

— структуру. Она состоит из сетевых программных протоколов, обеспечивающих передачу информации по различным сетям, включая Интернет, корпоративные сети, одноранговые сети (типа Tor); программ и программных платформ, осуществляющих хранение, переработку и предоставление информации — от баз данных до привычных всем операционных систем типа Windows, Linux; программ-интерфейсов, обеспечивающих восприятие информации конечными пользователями (интерфейсы сайтов, блогов, порталов, приложений, различного рода программ и т. п.);

— ультраструктуру. Она представляет собой инфосферу, где содержатся воспринимаемые человеком прямые и скрытые смыслы, выраженные в текстах, таблицах, видео- и аудиоконтенте. Ультраструктура включает в себя, во-первых, общедоступные сетевые ресурсы типа сайтов, блогов, порталов, социальных сетей и т. п., во-вторых, защищенные, доступные только для определенных категорий пользователей информационные ресурсы государственной и корпоративной принадлежности, в-третьих, общедоступные ресурсы с платным контентом.

За историю развития общедоступных коммуникационных сетей (с 1991 г.) сложилось два принципиально различных их типа:

— *Интернет*, а также *внутренние государственные и корпоративные сети, недоступные для сторонних пользователей*. Эти сети построены по иерархическому принципу. В сетях существует несколько уровней иерархии, которые аккумулируют и передают информацию. Соответственно, права и возможности регулирования информации на каждом уровне зависят от положения в иерархии: чем выше уровень, тем больше возможностей и прав;

— так называемые *пиринговые, или одноранговые, сети*[1]. Наиболее популярные из них в настоящее время — коммуникационная сеть Tor и платежная сеть Биткойн. В одноранговых сетях информация передается между компьютерами пользователей, которые имеют абсолютно равные права и возможности в передаче информации. В силу этого одноранговые сети работают, как правило, намного медленнее, чем Интернет.

Указанные типы сетей функционируют независимо друг от друга. Соответственно, ресурсы одной сети не обнаруживаются и не находятся поисковыми системами другой сети. При этом в каждой из сетей предусмотрены специальные порталы, которые облегчают использование ресурсов в другой сети.

Интернет имеет следующую *картографию*:

— *web 1.0*. Это наиболее старый, сложившийся сегмент Сети. Он включает в себя правительственные, корпоративные, общественные, персональные порталы, сайты, блоги, онлайн-СМИ. Ресурсы этого сегмента Сети легкодоступны при помощи поисковых систем (типа Google, Yandex и проч.);

— *web 2.0*. Это так называемый социальный веб, или веб социальных сетей и платформ. Здесь расположены такие ресурсы, как «ВКонтакте», Facebook, Twitter и проч. Контент в этом сегменте Интернета создается в основном самими пользователями, поэтому он получил название *социального веба*. Из-за политики собственников платформ и социальных сетей, а также из-за требований приватности они лишь частично видимы для поисковых систем. В этом сегменте ускоренными темпами растет доля видео- и фотоконтента;

— *web 3.0*. Этот сегмент Интернета появился после 2010 г. и растет наиболее быстрыми темпами. Это так называемый *веб мобильных приложений*. Интерфейсы приложений размещаются на экранах планшетных компьютеров, смартфонов. Соответственно, пользователи работают с приложениями без обращения к поисковым системам, просто устанавливая связь между своим устройством и Интернетом;

— *невидимый Интернет*. Это ресурсы, которые не обнаруживаются поисковыми машинами, а также порталы, сайты и т. д., доступ к которым предполагает либо платный характер, либо наличие специального разрешения на использование ресурсов. По имеющимся данным[2], в невидимом Интернете находится около 90% всего ценного научно-

[1] Одноранговая, децентрализованная или пиринговая (от англ.: peer-to-peer, P2P — равный к равному) сеть — это компьютерная сеть, основанная на равноправии участников.

[2] См.: *Paganini P., Amores R.* The Deep Dark Web. 2012.

технического, технологического, финансово-экономического и государственного открытого контента. Объемы невидимого Интернета постоянно растут. Он развивается более быстрыми темпами, чем web 1.0 и web 2.0. Главными причинами опережающих темпов являются, с одной стороны, стремление к архивации всех доступных данных корпоративными пользователями, а с другой — желание обладателей ресурсов вывести их из общедоступного пользования в платный сегмент, т. е. монетизировать;

— *«Интернет вещей»*. Представляет собой соединенные через Интернет с управляющими центрами встроенные информационные блоки самых различных объектов физического мира, в том числе производственной, социальной, коммунальной инфраструктуры. Например, к нему относятся подсоединенные к Всемирной сети технологические линии, системы управления водо- и теплоснабжением и т. п. В последние годы быстрыми темпами растет подключение к Интернету всех типов домашнего оборудования, бытовой техники, вплоть до холодильников, стиральных машин и т. п.;

— *бодинет*. Со стремительным развитием микроэлектроники появилась возможность встраивать элементы, передающие информацию, в предметы гардероба (кроссовки, майки и т. п.), а также широко использовать микроэлектронику в новом поколении медицинской техники, реализующей различного рода имплантаты — от чипов, контролирующих сахар в крови, до искусственного сердца и т. п. Кроме того, новой тенденцией стало создание *распределенного компьютера*, который предполагает, что отдельные его элементы распределяются по человеческому телу: фактически человек носит на себе компьютер и взаимодействует с ним круглые сутки[1].

Бóльшую часть одноранговых сетей относят к так называемому *темному вебу* (dark web). Своим названием этот сегмент Сети обязан широкому использованию своих ресурсов различного рода преступными, незаконными группами и группировками. Основными сегментами этого веба являются *сеть Tor*, созданная в 2002 г. военно-морской разведкой США, и *платежная сеть криптовалют*. В настоящее время сети часто используются для противоправной деятельности, киберпреступности, торговли наркотиками, оружием, детской порнографией и т. п., а также для осуществления целенаправленных акций по подрыву государственного суверенитета.

Особый сегмент Сети, располагающийся частично в сети Интернет, частично — в специально созданных одноранговых сетях, составляют так называемые *сети денег*. Общемировой тенденцией является сокращение наличного платежного оборота и переход к электронным деньгам во всех их видах. Сеть денег включает в себя специализированные телекоммуникационные расчетные сети, связывающие крупнейшие банки типа SWIFT, а также платежные системы, использующие Интернет, типа PayPal, «Яндекс.Деньги» и т. п. Отдельным быстро развивающимся сегментом денежных сетей являются *специализированные платежные системы, базирующиеся на одноранговых сетях и зашифрованных сообщениях*. Наиболее известные из этих систем — платежные системы криптовалют.

[1] Подробнее см.: *Ларина Е. С.* Встречайте — bodynet! // URL: http://www.therunet.com/articles/1877-vstrechayte-bodynet.

Таким образом, цифровая среда имеет сложную картографию, где отдельные сегменты развиваются по собственным, независимым от общих закономерностей трендам. При этом ряд основополагающих тенденций являются общими для всех сегментов цифровой среды.

Первой основополагающей тенденцией цифровой среды является *информационный взрыв*. В последнее время объем информации удваивается каждые два года[1]. По данным компании Cisco, объем сгенерированных данных к 2020 г. увеличится до 40 зеттабайт[2]. Примерно треть передаваемых данных составляют автоматически сгенерированные данные, т. е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к Интернету. На 40% ежегодно растет объем корпоративной информации, передаваемой и хранящейся в сети Интернет.

§ 2. Цифровой мир в эпоху третьей и четвертой промышленных революций

Цифровой мир сегодняшнего дня уникален и не имеет исторических аналогов, поскольку основывается сразу на *двух новых промышленных революциях*. В последние несколько лет в ведущих странах мира — от США до Китая, от Южной Кореи до Германии — разворачиваются и набирают темпы третья и четвертая промышленные революции. Третья стала предметом обсуждения ведущих мировых политиков, предпринимателей и экспертов после опубликования международного бестселлера Дж. Рифкина «Третья промышленная революция»[3].

Наряду с книгой Дж. Рифкина новой производственной революции посвящены еще два бестселлера — книги П. Марша «Новая инду-

[1] См.: IDC iView. Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. URL: http://www.emc.com/leadership/digital-universe/2012iview/big-data-2020.htm.

[2] См.: Cisco Visual Networking Index: Global Data Traffic Forecast Update, 2013-2020. URL: http://www.cisco.com/c/solutions/service-provider/visual-networking-index-vni/white-paper-listing.html.

[3] *Рифкин Дж.* Третья промышленная революция. М., 2016.

стриальная революция: потребители, глобализация и конец массового производства» и К. Андерсона «Производители: Новая промышленная революция».

В 2016 г. на Всемирном экономическом форуме в Давоссе его председатель К. Шваб провозгласил начало четвертой промышленной революции. Вскоре после давосского форума в свет вышла книга К. Шваба, которая была переведена практически на все основные языки мира[1].

Под четвертую промышленную революцию в Германии реализуется программа «Индустрия-4.0».

В 2017 г. заговорили уже о пятой революции. В марте 2017 г. на выставке CeBit в немецком городе Ганновер (ключевом для мира инноваций мероприятии, объединившем в 2017 г. 200 тыс. человек и 3 тыс. технологических компаний) японский премьер-министр Синдзо Абэ презентовал свой проект «Общество-5.0» (Society 5.0). Этот проект идет еще дальше, чем проект четвертой промышленной революции «Индустрия-4.0». Идея японских властей — поставить новые технологии на службу общества, внедрить их во все сферы жизни. Цель — оптимизировать быт, деловую деятельность, эффективнее решать проблемы старения населения, ухода за людьми с ограниченными возможностями, обучения.

Промышленная революция означает глубокие, быстрые в исторической перспективе, скачкообразные (фазовые) изменения в самих основах техники и технологий, используемых во всех основных отраслях хозяйства. Эти изменения ведут к необратимым и качественным сдвигам в организации труда и производства, системах снабжения, маркетинга и потребления. Промышленная революция изменяет базовые структуры экономической жизни, полностью перестраивает социум и привычные способы его регулирования, преобразует политические институты.

Новые промышленные революции по своим масштабам, последствиям и сдвигам не только стоят наравне, но, возможно, и превосходят первую и вторую производственные революции[2].

Уже на начальных стадиях новых промышленных революций можно выделить несколько определяющих черт:

1) одновременное широкое производственное применение различных независимых кластеров технологий, прежде всего робототехники, 3D-печати, новых материалов со спроектированными свойствами, биотехнологий, новых информационных технологий и конечно же диверсификация энергетического потенциала производства и общества;

[1] См.: *Шваб К.* Четвертая промышленная революция. М., 2017.

[2] Как известно, первая производственная революция конца XVIII — начала XIX в. была связана с текстильной отраслью, энергией пара, углем, железными дорогами и т. п. Вторая производственная революция конца XIX — первой половины XX в. стала детищем электричества, двигателей внутреннего сгорания, триумфом машиностроения и конвейера как метода организации производства.

2) постоянно возрастающее взаимодействие между отдельными технологическими кластерами, их своеобразное «слипание», взаимное кумулятивное и резонансное воздействие друг на друга;

3) появление на границах технологических кластеров принципиально новых, не существовавших ранее технологий и семейств технологий, в которых кластеры взаимодействуют между собой.

Основа основ превращения отдельных технологических кластеров или паттернов в единую технологическую платформу — это *информационные технологии*. Они буквально пронизывают все стороны технологической и производственной жизни, связывая между собой отдельные технологические блоки. Наиболее яркими примерами этого являются такие технологические паттерны, как биотехнологии, робототехника, управляемая на основе больших данных, и т. п.

В сфере организации производства и труда отличительной чертой новых производственных революций является миниатюризация производства в сочетании с сетевой логистикой и персонификацией потребления продукции.

Децентрализация производства, переход к прямым связям в сфере распределения и персонификации потребления будет происходить в условиях сохранения господства цифровых гигантов, контролирующих ключевую технологию новой производственной революции — системы сбора, хранения, интеллектуальной обработки и распределенной доставки цифровых данных и компьютерных программ всех типов и размеров.

Первым ключевым направлением новых промышленных революций является *стремительная автоматизация и роботизация производства*, армии и всех сторон общественной жизни. Как отмечают эксперты, многие элементы автоматизации и роботизации могли быть внедрены в промышленное производство еще в 90-е гг. прошлого и первое десятилетие нынешнего века. Однако в те времена экономически выгоднее оказалось использовать вместо роботов практически дармовой труд рабочих из Китая и других азиатских стран. Однако по прошествии времени ситуация изменилась. С одной стороны, труд в Азии заметно подорожал. С другой стороны, деиндустриализация Америки, многих стран Европы и частично Японии нанесла сильнейший удар по экономике этих стран. Наконец, в последние годы появились принципиально новые программные и микроэлектронные решения, позволяющие в разы повысить эффективность и функционал роботов при снижении себестоимости их производства. Сегодня,

например, типовой американский робот на конвейере окупается в течение полутора — максимум двух лет.

В мире разворачиваются новые промышленные революции. Принципиально новые производства, линии и т. п. массово и согласованно приходят на смену традиционным технологиям, организационным структурам и финансово-экономическому механизму, характерному для индустрии второй производственной революции. Среди направлений производственной революции три, без сомнения, являются ключевыми. Это робототехника, IT-технологии и биотехнологии.

Вторым направлением новых промышленных революций является *3D-печать*. В ее основе лежит технология Additive Manufacturing, т. е. аддитивное (можно сказать, поэтапное) изготовление. Метод подразумевает, что принтер послойно формирует изделие, пока оно не примет окончательный вид. 3D-принтеры не наносят на бумагу краску, а «выращивают» объект из пластмассы, металла или других материалов.

В 2014—2016 гг. произошел прорыв в области промышленного использования 3D-печати крупнейшими корпорациями. Линии 3D-печати в настоящее время строят Boing, Samsung, Siemens, Canon, General Electric и др.

Третьим направлением новых промышленных революций является *производство новых материалов*, включая материалы с заранее спроектированными свойствами, композитные материалы и т. п. Необходимость появления широчайшей гаммы новых материалов диктуется, с одной стороны, требованиями широкого внедрения экономичной, эффективной 3D-печати, а с другой — развитием микроэлектроники, биотехнологий и т. п.

В свое время новое материаловедение связывали исключительно с *наноматериалами*, т. е. с новыми материалами, производимыми на основе миниатюризации.

Ключевым направлением новых промышленных революций являются, без сомнения, *биотехнологии* в широком смысле этого слова. По сути, сюда входит *индустрия индивидуализированных лекарств*, на которые делают ставку и фармацевтические гиганты, и новые, молодые, быстроразвивающиеся компании в этой сфере. Сюда же относятся различные виды *регенеративной медицины*. Широко используются *возможности 3D-печати для производства донорских органов*. Сегодня это уже не фантастика, а прошедшая клинические испытания обыденность, которую взяли на вооружение медицинские учреждения Франции, Германии, Соединенных Штатов, Израиля, Китая и других стран.

Особым направлением является *биоинформатика*. Группе исследователей во главе с Дж. К. Вентером удалось впервые в истории создать *искусственную жизнь*, используя ДНК одного из вирусов. Теперь эта

команда может производить новые виды бактерий и живых организмов прямо из компьютера. Дж. Вентер так и заявил, что им удалось сделать «первый самовоспроизводящийся биологический вид на планете, родителем которого является компьютер».

Стержневой составляющей, пронизывающей все технологические кластеры новых промышленных революций и превращающей их в единый технологический пакет, являются, без сомнения, *информационные технологии*. В структуре информационных технологий выделяются три ключевые составляющие.

Первая — это *большие данные* (big data). Большие данные — это сбор, хранение, оцифровка, обработка и предоставление в удобном для пользователя виде в любое время и в любой точке всей совокупности сведений о тех или иных событиях, процессах, явлениях и т. п. Ключевым в больших данных является то, что они позволяют работать именно со всей информацией в режиме он-лайн. Главным здесь является слово «всей». У пользователя больших данных имеется вся картина, не зависящая, как раньше, от каких-либо выборок, ограничений по источникам, времени предоставления данных и т. п. Большие данные могут включать в себя любые форматы — от таблиц до потокового видео, от оцифровки старых отчетов до текстовой записи, сделанной теми или иными источниками. Никогда раньше в истории человечества у лиц, занимающихся анализом, прогнозированием, конструкторско-инженерной деятельностью, геологией, принятием решений и т. д., не было возможности оперировать всей информацией. Причем не просто оперировать, а получать эту информацию в удобном и доступном для восприятия виде. Сегодня безусловными лидерами в сфере больших данных являются США, Великобритания, Япония и Китай. В этих странах имеются большое количество платформ, обеспечивающих работу с большими данными, специальные курсы подготовки, множество центров, где компании могут получить консультации или услуги, связанные с большими данными.

Сами по себе большие данные являются важнейшим государственным и корпоративным активом, который при должном использовании обеспечивает их владельцам устрашающее интеллектуальное превосходство и деловое доминирование.

Вторая ключевая составляющая — это *когнитивные вычисления и экспертные системы*. За последние годы Соединенным Штатам и Великобритании удалось осуществить подлинный прорыв в области создания экспертных систем, базирующихся на так называемых когнитивных вычислениях. В основу когнитивных вычислений заложены программы, моделирующие и имитирующие некоторые известные психофизиологические процессы. За счет этого созданы программы,

которые облают возможностями совершенствования, учитывающего при решении тех или иных задач ошибки.

Третья ключевая составляющая — это *«облачные» и распределенные вычисления*. Согласно российской Стратегии развития информационного общества *«облачные» вычисления* — информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети Интернет к общему набору конфигурируемых вычислительных ресурсов («облаку»), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера.

В период 2014—2016 гг. все ведущие страны мира приняли государственные документы, касающиеся в основном вопросов национальной безопасности. В них впервые зафиксирован важнейший вывод. *Любая высокая технология имеет тройное применение: гражданское, военное и криминальное*. Соответственно, новые промышленные революции в целом, их направления и конкретные технопакеты *не только открывают новые возможности, позволяют создать эффективные средства противодействия силам деструкции, но и наделяют преступников и террористов новыми, не существовавшими ранее методами и инструментами*. Одним из важнейших следствий этого процесса является подтверждение так называемой теоремы Станислава Лема. В книге «Сумма технологий» он предсказал, что *по мере технологического прогресса неуклонно возрастает разрушительная мощь малых групп и даже отдельных индивидов*. В работе, изданной еще в начале 1960-х гг., он спрогнозировал, что в начале XXI в. маленькие группы террористов и бандитов и даже отдельные преступники смогут шантажировать и ставить под угрозу нормальное функционирование и жизнь населения мегаполисов и даже небольших государств. Новая производственная революция превратила прогнозы С. Лема в реальность[1].

§ 3. Цифровое (информационное) общество

Стратегия информационного общества понимает само это общество в широком смысле — как *общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан*.

Международные принципы создания информационного общества и подходы к его созданию определены Окинавской хартией глобального информационного общества (2000), Декларацией принципов «Построение информационного общества — глобальная задача в новом тысячелетии» (2003), Планом действий Тунисского обязательства (2005).

[1] См.: *Лем С.* Сумма технологий. М., 2012.

Введение термина «информационное общество» приписывают профессору Токийского технологического университета Юдзиро Хаяши, который в 1969 г. по заказу правительства Японии опубликовал несколько докладов: «Японское информационное общество: темы и подходы» и «Контуры политики содействия информатизации японского общества»[1]. В 1971 г. Токийский технологический университет представил публике доклад «План информационного общества». В этих работах говорилось о том, что компьютеризация обеспечит людям доступ к надежным источникам информации, освободит их от рутинной работы и создаст высокий уровень автоматизации производства. Производство не материального («индустриального»), а «информационного» продукта станет двигателем образования и развития нового, «информационного» общества.

В США принято считать, что понятие «информационное общество» ввел в науку в 50-х гг. прошлого века эмигрировавший в США австрийский экономист Ф. Махлуп. Он же говорил о наступлении эры «информационной экономики».

Если углубиться еще дальше в историю — в 40-е гг. XX в., можно найти записку англо-австралийского экономиста К. Кларка о перспективе появления «общества информации и услуг»[2].

Американский социолог Д. Белл полагает, что информационное общество как следующая стадия общественного развития может характеризоваться тремя основными критериями:

1) должен произойти переход от доминирования индустриального производства к производству услуг (массовый рабочий не нужен);

2) научное знание приобретает определяющее значение в процессе реализации технологических нововведений;

3) интеллектуальные технологии должны стать ключевым элементом системного анализа и теории принятия решений[3].

В середине 1990-х гг. американский социолог испанского происхождения М. Кастельс выпустил трехтомную монографию «The Information Age». Исследование являет собой энциклопедический анализ роли и места информации в современном мире.

По мнению Кастельса, начиная с 70-х гг. прошлого века появляющиеся новые формы капитализма постепенно начинают оформляться в то, что автор называет *информационным капитализмом, главным ре-*

[1] URL: https://sputnikipogrom.com/society/64415/infoage-1.

[2] Там же.

[3] См.: *Белл Д.* Социальные рамки информационного общества // Новая технократическая волна на Западе. М., 1986; *Он же.* Грядущее постиндустриальное общество. М., 2001.

сурсом которого становятся информационные сети, необходимые как для обеспечения производства внутри конкретного предприятия, так и для ведения бизнеса по всему миру[1].

§ 4. Цифровая экономика и ее технологии

Стержневой основой цифрового мира является *цифровая экономика*, которую Стратегия развития информационного общества определяет как хозяйственную деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

Целями программы «Цифровая экономика Российской Федерации», утв. распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р, являются:

— создание экосистемы цифровой экономики РФ, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности, обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан;

— создание необходимых и достаточных условий институционального и инфраструктурного характера; устранение имеющихся препятствий и ограничений для создания и (или) развития высокотехнологических бизнесов и недопущение появления новых препятствий и ограничений как в традиционных отраслях экономики, так и в новых отраслях и высокотехнологичных рынках;

— повышение конкурентоспособности на глобальном рынке как отдельных отраслей экономики России, так и экономики в целом.

Цифровая экономика представлена *тремя* следующими *уровнями*, которые в своем тесном взаимодействии влияют на жизнь граждан и общества в целом:

— рынки и отрасли экономики (сферы деятельности), где осуществляется взаимодействие конкретных субъектов (поставщиков и потребителей товаров, работ и услуг);

— платформы и технологии, где формируются компетенции для развития рынков и отраслей экономики (сфер деятельности);

— среда, которая создает условия для развития платформ и технологий и эффективного взаимодействия субъектов рынков и отраслей

[1] См.: *Кастельс М.* Информационная эпоха: экономика, общество и культура. М., 2000.

экономики (сфер деятельности) и охватывает нормативное регулирование, информационную инфраструктуру, кадры и информационную безопасность.

Развитие цифровой экономики России основывается на основных трендах третьей и четвертой промышленных революций.

Полная оцифровка экономики. Сквозное проникновение технологий во все отрасли экономики как в качестве цифровых (нематериальных) активов в форме новых бизнес-моделей, так и в форме промышленного «Интернета вещей» (IoT) обусловливает формирование больших массивов экономически значимых отраслевых и межотраслевых данных. Равно сквозное проникновение технологий в социальную сферу — в форме технологий связи и коммуникаций и «Интернета вещей», когда практически каждый предмет быта и окружающего человека мира оказывается подключен к глобальному цифровому пространству, формирует предпосылки для использования соответствующих данных для оценки и прогнозирования экономического развития.

Обеспечение всеобщего доступного подключения к высокопроизводительным широкополосным сетям. Всеобщий доступ к Интернету позволит развивать преимущества «Интернета вещей» и промышленного «Интернета вещей». По самым скромным подсчетам, к 2045 г. к Интернету по всему миру будет подключено более 100 млрд устройств. Это будут мобильные и переносные устройства, приборы, медицинские устройства, промышленные датчики, камеры безопасности, автомобили, одежда и др. Все эти устройства будут производить огромное количество информации и делиться ею, что произведет революцию в том, как мы работаем и живем. Люди будут использовать информацию, полученную через IoT, для принятия более разумных решений и получения более глубокого понимания их собственных жизней и окружающего их мира. В то же время устройства, подключенные к Интернету, также автоматизируют многие задачи мониторинга, управления и ремонта, которые в настоящее время требуют человеческого труда. Пересечение IoT, аналитики и искусственного интеллекта создаст глобальную сеть умных машин, которые будут проводить огромное количество критически важных бизнес-операций без участия человека. Хотя IoT улучшит многие аспекты экономической эффективности, общественной безопасности и производительности труда, это также потребует дополнительных мер по обеспечению кибербезопасности и защиты конфиденциальности.

Цифровые платформы. В настоящее время существует множество цифровых платформ, которые обеспечивают рынки товаров, услуг и информации, поставляемых как в физическом, так и в цифровом виде.

Государственные цифровые платформы представляют собой цифровую экосистему, технологическую среду с API (Application Program-

ming Interface), предоставляющую услуги и сервисы для управления жизненными ситуациями граждан, а также площадку, где формируются договоры между государством и различными категориями стейкхолдеров, заинтересованных в получении государственных услуг. На государственных платформах могут предоставляться в том числе бесплатные сервисы, основанные на обработке открытых больших данных — как для бизнеса, так и для населения.

Компании-платформы — один из базовых элементов новой экономики. Следует наращивать инвестиции в национальные цифровые платформы. Развитие цифровых технологий должно быть включено во все программы и планы социально-экономического развития. Задействованным в развитии цифровых платформ частным компаниям должен быть обеспечен максимально облегченный доступ к кредитам, субсидиям, налоговым и иным финансовым льготам.

Инфраструктура для хранения информации. С учетом объема устройств, подключенных к цифровому пространству и общей цифровизации экономики, количество данных растет экспоненциально. В связи с этим возрастает роль высокотехнологичных решений для безопасного, надежного, долгосрочного хранения больших данных.

Технологии обработки больших данных. Для упрощения масштабного перехода бизнеса на цифровые платформы требуется снижение стоимости вычислительной мощности. Решения в данной сфере будут обусловливать конкурентные преимущества и уменьшать порог входа микробизнеса на рынок информационных услуг.

Формирование доверенного цифрового пространства. Формирование доверенной среды для хранения и обработки больших данных, а также для аутентификации и идентификации субъектов цифровой экономики в цифровом пространстве обусловит повышение уровня вовлеченности бизнеса и населения в цифровую экономику и обеспечит предоставление качественных цифровых услуг.

Новые технологии и их влияние на традиционные сектора экономики. Цифровые инновации в узком смысле относятся к внедрению нового или значительно улучшенного продукта информационно-коммуникационных технологий — ИКТ (товара или услуги), т. е. инновационной продукции в области ИКТ; в более широком смысле — к использованию ИКТ для внедрения нового или значительно улучшенного продукта, процесса, метода маркетинга или организационного метода, т. е. инноваций с использованием ИКТ.

Технологии, которые определяют переход к цифровой экономике. *Технологии в области работы с данными* включают:

— *искусственный интеллект* — наука и технология создания интеллектуальных машин, особенно интеллектуальных компьютерных программ; свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека. Искусственный интеллект связан со сходной задачей использования компьютеров для понимания человеческого интеллекта, но не обязательно ограничивается биологически правдоподобными методами;

— *«туманные вычисления»* (fog computing) — архитектура системного уровня для расширения «облачных» функций хранения, вычисления и сетевого взаимодействия. Концепция предполагает обработку данных на конечных устройствах сети (компьютерах, мобильных устройствах, датчиках, смарт-узлах и т. п.), а не в «облаке»;

— *квантовые технологии* — технологии, в которых используются специфические особенности квантовой механики, прежде всего квантовая запутанность. Цель квантовой технологии состоит в том, чтобы создать системы и устройства, основанные на квантовых принципах, к которым обычно относят дискретность (квантованность) уровней энергии (квантово-размерный эффект, квантовый эффект Холла); принцип неопределенности Гейзенберга; квантовую суперпозицию чистых состояний систем; квантовое туннелирование через потенциальные барьеры; квантовую сцепленность состояний;

— *суперкомпьютерные технологии* — набор инструментов, используемых для решения специализированных задач с использованием специализированных вычислительных машин (суперкомпьютеров), которые превосходят по техническим параметрам и скорости вычислений большинство существующих в мире компьютеров. Суперкомпьютеры представляют собой большое число высокопроизводительных серверных компьютеров, соединенных друг с другом локальной высокоскоростной магистралью для достижения максимальной производительности в рамках подхода распараллеливания вычислительной задачи;

— *технологии идентификации* — автоматическая идентификация и сбор данных — AIDC (Automatic Identification and Data Capture) — общий термин для методов автоматической идентификации объектов, сбора данных о них и обработки данных автоматическими и автоматизированными системами. Технологии идентификации объектов включают магнитную карту, чип-карту, оптические (штрих-код, Data Matrix, OCR), радиочастотные (RFID, RTLS), биометрические (дактилоскопия, in vitro, определение ДНК), аудиологические (распознавание голоса), оптические (идентификация по радужной оболочке глаза, распознавание лица) технологии;

— *математическое моделирование* — опосредованное практическое или теоретическое исследование объекта, при котором непосредственно изучается не сам интересующий нас объект, а некоторая вспомогательная искусственная или естественная система (модель), находящаяся в некотором объективном соответствии с познаваемым объ-

ектом, способная замещать его в определенных отношениях и дающая при ее исследовании в конечном счете информацию о самом моделируемом объекте;

— *сквозные технологии* — совокупность методов обработки, в составе которых на базе одной системы существует набор специализированных программ, не зависящих от конкретных методик и позволяющих осуществлять интерактивный обмен данными. Сквозная обработка — STP (Straight-Through Processing) — процесс непрерывной, полностью автоматизированной обработки информации. На всех этапах обработки данных исключено ручное вмешательство, что достигается применением стандартов обмена информацией между автоматизированными системами и их полного взаимодействия. Первичные данные могут формироваться как автоматическими системами, так и ручным вводом, но их последующая передача и обработка происходят полностью автоматически. В более узком смысле STP-технология предполагает, что брокерская компания выступает в роли автоматического посредника между клиентами и внешним рынком. Ордера клиентов автоматически переправляются для заключения сделок на внешнем рынке или на крупного контрагента;

— *технологию блокчейна* — многофункциональные и многоуровневые информационные технологии, предназначенные для надежного учета различных видов активов[1]. Блокчейн — распределенная база данных, которая содержит непрерывно возрастающий набор упорядоченных записей (блоков), каждый блок содержит метку времени и связь с предыдущим блоком. Блокчейны — открытые, распределенные регистры, в которые могут вноситься записи о транзакциях между двумя участниками надежным и достоверным образом;

— *нейронные сети* — математические модели, а также их программные или аппаратные реализации, построенные по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма.

Технологии в области производства:

— *киберфизические системы — CPS (Cyber-Physical System)* — системы, состоящие из различных природных объектов, искусственных подсистем и управляющих контроллеров, позволяющих представить такое образование как единое целое. Новизна и принципиальное отличие CPS от существующих встроенных систем или автоматизированных систем управления технологическим процессом, на которые они похожи внешне, состоит в том, что CPS интегрируют в себе кибернетическое начало, компьютерные аппаратные и программные технологии, качественно новые исполнительные механизмы, встроенные в окружающую их среду и способные воспринимать ее изменения, реагировать на них, самообучаться и адаптироваться;

[1] См.: *Свон М.* Блокчейн: Схема новой экономики. М., 2017.

— *3D-технологии (печать), или «аддитивное производство»,* — процесс создания цельных трехмерных объектов практически любой геометрической формы на основе цифровой модели. 3D-печать основана на концепции построения объекта последовательно наносимыми слоями, отображающими контуры модели. Фактически 3D-печать является полной противоположностью таких традиционных методов механического производства и обработки, как фрезеровка или резка, где формирование облика изделия происходит за счет удаления лишнего материала (так называемое субтрактивное производство);

— *роботизация* — использование интеллектуальных робототехнических комплексов, функциональные особенности которых состоят в достаточно гибком реагировании на изменения в рабочей зоне;

— *аддитивные технологии* — технологии по созданию объектов за счет нанесения последовательных слоев материала. Модели, изготовленные аддитивным методом, могут применяться на любом производственном этапе — как для изготовления опытных образцов (быстрое прототипирование), так и в качестве самих готовых изделий (быстрое производство). В производстве, особенно машинной обработке, термин «субтрактивные» подразумевает более традиционные методы и является ретронимом, придуманным в последние годы для разграничения традиционных способов и новых аддитивных методов. Хотя традиционное производство использует по сути «аддитивные» методы на протяжении веков (такие, как склепка, сварка и привинчивание), в них отсутствует трехмерная информационная технологическая составляющая. Машинная же обработка (производство деталей точной формы), как правило, основывается на субтрактивных методах — опиловке, фрезеровании, сверлении и шлифовании;

— *технологии открытого производства* — технологии, основанные на новой модели социоэкономического производства, в рамках которой физические объекты создаются исходя из принципов открытости, взаимодействия и распределения, при этом модель основывается на принципах открытого проектирования и открытого источника (open source).

Технологии в области взаимодействия с окружающей средой:

— *беспилотные технологии* — комплекс, оборудованный системой автоматического управления, который может передвигаться без участия человека;

— *безбумажные технологии* — технологии, при которых основным носителем информации является не бумажный, а электронный документ, формируемый на машинном носителе (в памяти компьютера) и доводимый до пользователя через экран дисплея;

— *мобильные технологии* — комплекс методов и решений (приложений, устройств), позволяющих достигать независимости пользователя от стационарных вычислительных устройств при решении поставленных задач;

— *биометрические технологии* — набор инструментов идентификации отдельно взятого человека, основанный на измерении его уникальных характеристик;

— *технологии «мозг — компьютер»* — нейрокомпьютерный интерфейс (НКИ) (называемый также прямым нейронным интерфейсом, мозговым интерфейсом, интерфейсом «мозг — компьютер») — система, созданная для обмена информацией между мозгом и электронным устройством (например, компьютером). В однонаправленных интерфейсах внешние устройства могут либо принимать сигналы от мозга, либо посылать ему сигналы (например, имитируя сетчатку глаза при восстановлении зрения электронным имплантатом). Двунаправленные интерфейсы позволяют мозгу и внешним устройствам обмениваться информацией в обоих направлениях. В основе нейрокомпьютерного интерфейса часто используется метод биологической обратной связи.

Цифровая трансформация сельского хозяйства. Для предотвращения глобальных вызовов в сфере продовольственной и биологической безопасности человечеству необходимо сельское хозяйство нового типа, соответствующее модели циркулярной (безотходной) экономики и принципам устойчивого развития. Вопросам перехода к новой экономической модели и к «интеллектуальному» сельскому хозяйству как ее неотъемлемому компоненту уделяют все большее внимание ведущие международные организации и национальные правительства.

Электронная торговля. Электронная торговля составляет значимый институт цифровой экономики, проникает во все большее количество правоотношений, складывающихся в сфере торговли, и охватывает весь спектр отношений — прямое взаимодействие потребителей с потребителями (C2C), взаимодействие продавцов с потребителями (B2C), взаимодействие между предпринимателями (B2B), взаимодействие бизнеса и государства в электронной форме (B2G) и др.

Цифровая трансформация в сфере связи и телекоммуникаций. По мере развития цифровой (электронной) экономики нагрузки на цифровую инфраструктуру, в основе которой лежат средства связи и телекоммуникаций, многократно возрастают. Пользователями востребуется уже не столько связь, сколько доступ к различным платформам, сервисам и услугам в электронном виде. Само понятие «пользователь» кардинально меняется, поскольку в условиях цифровой трансформации в эту категорию попадают не только люди, но и представители «Интернета вещей» (подключенные устройства), количество которых уже превышает количество людей в разы, а скоро превысит уже и на порядки. Таким образом, речь идет о нагрузках на средства связи и телекоммуникаций и их пропускной способности, превосходящих существующие на несколько порядков.

Цифровая трансформация транспорта и логистики. «Цифровая логистика» возникает как ответ на глобальные вызовы цифровой экономики для традиционного сектора транспорта и логистики, такие как стремительно изменяющаяся глобализированная и сверхконкурентная торговая среда, сложность цепочек поставок, быстрое изменение ожиданий клиентов, ограниченные ресурсы инфраструктуры.

Проблемы логистики в электронной торговле связаны прежде всего с более быстрыми темпами формирования и реализации цепочек поставок товаров по сравнению с традиционной торговлей. Данная особенность электронной торговли определяет необходимость совершенствования механизмов прогнозирования спроса, что должно способствовать более рациональному планированию запаса товаров на складах в различных географических регионах, сокращая время оборота товаров и стоимость доставки. В рамках развития электронной торговли необходимо разрабатывать и внедрять технологии анализа данных по спросу для планирования распределительной логистики.

В то же время в секторе «B2B» (Business to Business — бизнес для бизнеса) перспективным может оказаться внедрение технологий, в том числе использующих достижения «Интернета вещей», позволяющих потенциальному заказчику самостоятельно отслеживать актуальную информацию о предложении, а именно о готовящемся к реализации товаре, через отслеживание производственного цикла (факт изготовления, отгрузки, транзитное время, ориентировочная дата прибытия на склад и т. п.), что позволит осуществлять более эффективное планирование закупок и, соответственно, их логистического обеспечения.

Сфера финансовых услуг. Под областью финансовых технологий понимают применение инновационных технологий в целях оказания финансовых услуг. Однако в связи со множеством применяемых в финансовой отрасли технологий границы термина «отрасль финансовых технологий» размыты.

Основными сегментами области финансовых технологий на данный момент являются: платежи и переводы, краудфандинг[1], управление активами, финансовый маркетплейс[2], блокчейн.

[1] От crowd — толпа, funding — финансирование. Коллективное сотрудничество людей, добровольно объединяющих свои ресурсы.

[2] Marketplace — рыночная площадь. В интернет-коммерции это место, где могут договариваться, заключать контракты участники рынка.

При этом мы видим усиление тенденции по созданию полностью цифровых банков, которые в своей деятельности ориентируются преимущественно на тех, кто предпочитает использование онлайн банковских услуг.

Цифровая трансформация энергетики. Россия является одним из крупнейших в мире производителей ископаемого топлива, в то же время запасы нефти и газа небезграничны и необходимы новые решения для создания высокоинтегрированных интеллектуальных системообразующих и распределительных электрических сетей нового поколения в Единой энергетической системе России (интеллектуальные сети — Smart Grid).

Цифровая трансформация ЖКХ. По прогнозам, к 2045 г. в городах будет жить 65—70% населения земного шара — примерно 6,4 млрд человек. Массовая миграция в города окажет значительное давление на городские транспортные системы, продовольствие и водоснабжение, энергетическую инфраструктуру, санитарию и общественную безопасность.

Информационные и коммуникационные технологии будут способствовать росту «умных городов», использующих данные и автоматизацию для увеличения эффективности и устойчивости городских центров. Распределенные сенсорные системы будут контролировать потребление воды и электроэнергии и автоматически балансировать распределение по смарт-сетям. Сетевые системы трафика и автономные варианты транспортировки смогут революционизировать массовый транспорт и логистику. Новые материалы и методы проектирования будут использоваться для построения интеллектуальных зданий, которые максимизируют эффективность нагрева, охлаждения и освещения. Внешние солнечные панели, микроветряные турбины, тепловая энергия и другие возобновляемые источники энергии обеспечат чистую распределенную выработку электроэнергии.

Новые системы управления. В условиях цифровой экономики данные становятся формой капитала. Формирование, накапливание и использование такого рода капитала требуют тесного сотрудничества государства и бизнеса, государства и гражданского общества, бизнеса и гражданского общества. Однако экономические преимущества получают те государства и хозяйствующие субъекты, которые имеют не только доступ к данным, но также эффективные технологии их обработки. Качественный рост экономики возможен при наличии технологий, позволяющих максимально возможно точно оценивать текущее состояние рынков и отраслей, а также осуществлять эффективное прогнозирование их развития и быстро реагировать на изменения в конъюнктуре национальных и мировых рынков.

Основными принципами управления как на уровне промышленных предприятий, так и на уровне государства становятся:

— получение данных в реальном времени;

— управление экономическими процессами, основанное на автоматизированном анализе больших данных;

— высокая скорость принятия решений, изменение правил в реальном времени — мгновенное реагирование на изменения и интерактивность среды;

— ориентация на конкретного пользователя, жизненные ситуации клиентов как бизнес-процесс (пользователь становится ближе благодаря мобильным устройствам и «Интернету вещей»);

— решения в одно касание;

— цифровая экосистема как центр синергии государства, бизнеса и граждан.

Ключевым фактором успеха в цифровой экономике, высококонкурентной и трансграничной, становятся не технологии, а новые модели управления технологиями и данными, позволяющие осуществлять оперативное реагирование и моделирование будущих вызовов и проблем для государств, бизнеса и гражданского общества.

§ 5. Граждане цифрового мира и их права

Digital native примерно можно перевести как «коренной житель цифрового общества, человек, родившийся в цифровом обществе, цифровое поколение»[1].

Человек в цифровом обществе, его проблемы — это предмет междисциплинарных профессиональных интересов специалистов в области философии, информатики, психологии, лингвистики, медицины, этнографии, педагогики, экономики и связывающих эти дисциплины областей (таких, например, как психолингвистика или клиническая психология) и, конечно, криминологии.

В современном цифровом обществе особенно острым является *соблюдение прав граждан* при пользовании цифровыми технологиями.

«Государства должны содействовать доступу к Интернету как к общественной службе, с тем чтобы каждый человек независимо от своего места проживания мог пользоваться его благами». Такое требование содержится в проекте Кодекса этики для информационного общества (ЮНЕСКО, 2010)[2].

[1] Термин был предложен М. Пренски, американским писателем и популяризатором технологий обучения и просвещения, в статье «Digital Natives, Digital Immigrants» (2001).

[2] См. также: Верховенство права в Интернете и в остальном цифровом мире: тематический доклад Совета Европы. 2014.

В этом же рекомендательном документе сказано:

— там, где общий доступ пока обеспечить невозможно, государства должны предоставить всем людям возможность получать легкий доступ к Интернету, например с помощью телецентров, библиотек, общинных центров, больниц и школ. Люди должны получить доступ к разветвленной национальной системе интернет-услуг, подключенной к международной сети;

— создание телекоммуникационной инфраструктуры, разработка правил, определение платы, введение налогов и установление тарифов должны обеспечивать доступ для всех имущественных групп населения, при этом особое внимание следует уделять потребностям государственных служб, образовательных учреждений, обездоленных групп населения и инвалидов;

— необходимо разрабатывать интерфейсы, контенты и прикладные программы, которые обеспечивали бы доступ для всех, включая людей с физическими, сенсорными или когнитивными недостатками, а также людей, говорящих на языках меньшинств;

— государства должны соответствующим образом содействовать применению открытых и технических стандартов взаимодействия программного и компьютерного обеспечения в цифровом мире, включая стандарты, разработанные для цифрового вещания, которые обеспечили бы людям широкий доступ к контенту;

— необходимо обеспечивать свободный доступ к информации для всех лингвистических групп, внедрять технологии, которые делали бы информацию доступной для людей с физическими недостатками, представителей обоих полов, лиц с разными уровнями развития, пожилых людей и групп, представляющих разные культуры и имеющих разный уровень дохода;

— люди должны иметь свободный доступ ко всей информации, представленной им другими. Люди должны иметь также удобные инструменты, позволяющие им легко, быстро и эффективно производить информацию, обмениваться ею и получать к ней доступ. Информационные сети должны быть открыты для контента из всех источников, что позволило бы всем заинтересованным лицам стать создателями продукции, а не оставаться лишь ее потребителями;

— государствам следует предотвращать попытки ограничить доступ и права на использование информации. Им следует обеспечить признание и осуществление права на всеобщий онлайновый доступ к общественной и правительственной документации, включая информацию, необходимую для граждан в современном демократическом обществе;

— государствам следует содействовать обеспечению доступа к ИКТ и образованию, чтобы позволить всем людям, особенно детям,

приобрести и сохранить навыки, необходимые для работы с самыми разными ИКТ, и критически оценить качество информации, особенно той, которая могла бы причинить им вред;

— государства обязаны защищать свободу выражения мнений. Им следует содействовать свободе выражения мнений и свободе распространения информации не только как ценности самой по себе, но и как ценности, обеспечивающей осуществление других прав, таких как право на образование, право на уважение человеческого достоинства, право на свободу вероисповедания и т. д.;

— право на свободу выражения мнений не должно ограничиваться правительствами, за исключением лишь тех случаев, которые строго определены и регламентированы общепризнанными положениями международного права или стандартами. Эти ограничения должны соответствовать международным правовым документам и стандартам по правам человека и принципам законности, а также устанавливаться соразмерно поставленной цели;

— государствам не следует подвергать интернет-контент каким-либо особым ограничениям, которые превышают ограничения, уже применяемые в отношении других средств распространения контента;

— органы власти не должны лишать общественность доступа к информации и другим коммуникационным продуктам в Интернете путем общей блокировки или фильтрации информации независимо от границ. Это не мешает установке фильтров для защиты малолетних, особенно в таких доступных для них местах, как школы или библиотеки, или для защиты Интернета от таких эндогенных угроз, как вирусы, вредоносные программы, спам и другие вредные технологии;

— государствам следует принять соответствующие законодательные акты, направленные на защиту личных данных и частной жизни в соответствии с нормами международного права, защиту пользователей от незаконного хранения их личных данных от хранения неточных личных данных или от злоупотребления или несанкционированного разглашения таких данных, или на защиту от вторжения в их частную жизнь путем, например, произвольной рассылки сообщений с явными коммерческими целями;

— государствам следует уважать волю пользователей Интернета не разглашать свои личные данные и обеспечивать, чтобы ИКТ не использовались для слежки или контроля органами власти или частными структурами сверх того, что разрешено международными актами по правам человека. Это не мешает государствам принимать меры и сотрудничать с целью нахождения лиц, ответственных за преступные деяния, в соответствии с национальным законодательством и международными соглашениями, касающимися правосудия и полиции;

— государствам следует содействовать принятию регламентов, определяющих меры по самостоятельному и совместному регулированию участниками частного сектора деятельности по защите права на уважение частной жизни и охране тайны переписки;

— государственные или частные организации, требующие от отдельных людей предоставления личных данных, должны запрашивать лишь минимально необходимое количество таких сведений и на минимально короткий срок. Собранные данные должны быть защищены от несанкционированного разглашения, а ошибки, связанные с угрозой личной безопасности, должны исправляться немедленно. В тех случаях, когда данные, собранные с определенной целью, больше не востребованы, они должны уничтожаться. Людей необходимо предупреждать о возможности использования представленных сведений не по назначению. Организации обязаны извещать людей в случае злоупотреблений, потери или кражи этой информации;

— государствам следует признать свободу граждан критиковать государственные или общественные учреждения. Критике со стороны средств информации могут подвергаться государственные, правительственные или любые другие учреждения исполнительной, законодательной или судебной власти;

— государствам и другим заинтересованным сторонам следует сотрудничать в области повышения безопасности Интернета и информации, что дало бы им возможность пресекать действия, подрывающие их стабильность и наносящие ущерб наличию, достоверности, целостности и конфиденциальности сохраняемых или передаваемых данных и услуг, предлагаемых сетями и системами или открывающих доступ к ним;

— необходимо содействовать разработке общих правил сотрудничества между провайдерами услуг информационного общества и правоохранительными органами, обеспечивая среди прочего, чтобы такое сотрудничество осуществлялось на строгой правовой основе, обеспечивающей соблюдение всех правил, регулирующих частную жизнь;

— государствам следует укреплять потенциал всех пользователей, включая детей и молодежь, с целью содействия обеспечению безопасного использования Интернета и ИКТ, недопущения появления и распространения незаконных и пагубных контентов путем регулирования в соответствии с международными стандартами;

— людям необходим свободный доступ к эффективным и действенным механизмам решения проблем, связанных с нарушениями прав человека. Когда права человека и основные свободы ставятся под угрозу материалами Интернета или же незаконным контролем, ограничениями свободы выражения мнений и других прав, участники должны иметь доступ к механизмам, позволяющим им принимать ответные меры по таким нарушениям.

Исходя из перечисленных требований, вряд ли для России приемлем опыт КНР по реализации Программы создания системы социального кредита (2014—2020). Из Программы следует, что к 2020 г. не только каждая компания, но и каждый житель материкового Китая будет отслеживаться и оцениваться этой системой в режиме реального времени. Рейтинг доверия физических лиц будет привязан к внутреннему паспорту. Рейтинги будут публиковаться в централизованной базе данных в Интернете в свободном доступе.

Обладатели высокого рейтинга будут пользоваться различными социальными и экономическими льготами. А тем, у кого рейтинг будет плохой, придется страдать — на них обрушится вся мощь административных санкций и ограничений. Главная задача, и это прямым текстом указывается в Программе Госсовета КНР, чтобы «оправдавшие доверие пользовались всеми благами, а утратившие доверие не могли сделать ни шагу».

Система в 2017 г. уже работала в пилотном режиме в 37 городах Китая. Передовиком в этом деле стал город Жунчэн в провинции Шаньдун. Всем жителям города (670 тыс. человек) дается стартовый рейтинг 1000 баллов. Далее в зависимости от их поведения рейтинг либо растет, либо падает. Разрозненная информация о жизни и деятельности гражданина поступает из муниципальных, коммерческих, правоохранительных, судебных органов в единый информационный центр, где обрабатывается с помощью технологии больших данных, и рейтинг гражданина, соответственно, либо повышается, либо снижается. В Жунчэне единый информационный центр анализирует 160 тыс. различных параметров из 142 учреждений. Активно приветствуется и система доносов. Гражданину, сообщившему о всяких «нехороших» делах своего соседа, полагается как минимум пять баллов.

Какого-либо единого документа, где было бы четко прописано, что делать можно, а что нельзя и что за это будет, система не предполагает. Известно лишь, что если твой рейтинг больше 1050 баллов, то ты образцовый гражданин и маркируешься тремя буквами А. Имея 1000 баллов, можно рассчитывать на АА, 900 — на В. Если рейтинг упал ниже 849, ты уже подозрительный носитель рейтинга, С — тебя выгонят со службы в государственных и муниципальных структурах[1].

В «черный список» к 2017 г. попало около 5 млн человек.

[1] См.: *Ковачич Л.* Большой брат 2.0. Как Китай строит цифровую диктатуру. Московский центр — Фонд Карнеги за международный мир. URL: http://carnegie.ru/commentary/71546 (дата обращения: 18.07.2017).

Глава 2. Криминогенные факторы, действующие в эпоху третьей и четвертой промышленных революций

Перечисляя подобные факторы, автор во многом основывается на выводах доклада Национального разведывательного совета США «Глобальные тренды: парадоксы прогресса», подготовленного офисом Директора национальной разведки в январе 2017 г. для представления в Конгрессе США, а также докладов Интерпола и Европола 2015—2017 гг. и ряда международных исследований (ООН, ЮНЕСКО, МВФ, Всемирного банка и др.).

§ 1. Социальное и цифровое неравенство

В теории криминологии с момента ее возникновения в XIX в. неравенство относили к числу главных причин преступности.

С начала XXI в. во всем мире слово «неравенство» не сходит со страниц газет и экранов телевизоров, по этой теме ежегодно публикуются тысячи книг и статей — как академических, так и публицистических. Большинство авторов полагают, экономическое неравенство — это главное зло, с которым сталкиваются современные общества. Ведущие международные организации — Всемирный банк, МВФ, Международная организация труда — заказывают и публикуют десятки специальных исследований, с разных сторон рассматривающих феномен экономического неравенства. В оборот вводятся все новые статистические данные о распределении доходов и богатства. С невероятной быстротой множится число посвященных этой проблеме научных работ. Книги о неравенстве становятся мировыми бестселлерами[1]. Многие видят в радикальном сокращении неравенства единственно возможное средство, способное оживить экономический рост. Ожесточенные дебаты по этой проблеме ведутся сегодня и в России.

Характерна статья К. Джомо и В. Попова под названием «Долгосрочные тенденции в распределении доходов», рисующая апокалиптическую картину: глобальное неравенство растет, неравенство внутри отдельных стран достигло пиковых по историческим меркам значений; вознаграждение топ-менеджеров компаний в сотни раз превышает заработки среднего работника; в развитых странах реальная заработная плата стагнирует в течение уже нескольких десятилетий; безработица находится на высоком уровне; социальная мобильность остается низкой; доля капитала в национальном доходе непомерно высока, а доля труда неоправданно низка; растущее экономическое неравенство обескровливает экономический рост; по всему фронту идет контр-

[1] См., например: *Пикетти Т.* Капитал в XXI веке. М., 2015.

наступление капитала, а организованный социальный протест отсутствует; эскалация неравенства в странах Запада стала следствием исчезновения противовеса в виде системы мирового социализма; современный капитализм все больше теряет «человеческое лицо»; уже в ближайшее время дальнейшее нарастание неравенства чревато острейшими социальными конфликтами, а в перспективе — даже революциями и разрушением целых наций; выход из создавшейся ловушки возможен только при условии проведения государством специальной политики, направленной на радикальное сокращение экономического неравенства[1].

Для нашей книги интерес представляет особый вид неравенства современного мира — *цифровой барьер, цифровое неравенство, информационное неравенство* (digital divide) — ограничение возможностей социальной группы из-за отсутствия у нее доступа к современным средствам коммуникации.

Цифровой барьер является термином социально-политического характера. На возможности ущемленной группы влияют отсутствие или ограниченный доступ к телевидению, Интернету, телефонной связи (мобильной и стационарной), радио. Все это ограничивает возможности этой группы в поиске работы, налаживании социальных связей, культурном обмене и может негативно влиять на экономическую эффективность, развитие и сохранение культуры, уровень образования. Согласно общепринятым воззрениям на цифровое (информационное) общество его специфика такова, что свободный обмен информацией способствует преодолению нищеты и неравенства, однако у тех, кто отключен от такого обмена, перспективы катастрофически ухудшаются.

«Глобальный тренд заключается в том, что информационная экономика подключает к своей сети тех, кто представляет для нее ценность (тем самым придавая им дополнительную ценность), но отключает тех, кто не имеет для нее ценности (тем самым еще более уменьшая их шансы обрести какую-то ценность)»[2].

Термин применяется как в отношении разницы между странами (например, в Исландии доступ к Интернету имеют более 86% населения, а в Либерии — 0,03%), так и в отношении разницы в возможностях разных социальных слоев внутри одного общества.

На данный момент примерно 53% населения Земли не пользуется Интернетом. Так, в наименее развитых странах (более 40 стран, офи-

[1] См.: *Джомо К. С., Попов В. В.* Долгосрочные тенденции в распределении доходов // Журнал Новой экономической ассоциации. 2016. № 3. С. 146—160.

[2] *Химанен П., Кастелс М.* Информационное общество и государство благосостояния. Финская модель = The Information Society and Welfare State: The Finnish Model. M., 2002.

циальный термин ООН) лишь 15,2% граждан могут похвастаться тем, что они являются интернет-пользователями. В некоторых случаях причиной такого невысокого процента вовлеченных граждан оказывается банальное отсутствие или недостаточная распространенность технологий передачи сигнала; в других — ограничения идеологического характера, которые негативно влияют на доступность интернет-коммуникации для определенных стран.

В данном случае не так важно, какими конкретно причинами продиктовано наличие цифрового неравенства между теми, кто может пользоваться благами и соблазнами Сети, и остальным миром. Существенно другое: *цифровое будущее провоцирует возникновение «новых бедных»*.

В эту группу можно зачислять не только тех, кто по объективным причинам лишен возможности доступа к Интернету и цифровым устройствам. Сюда же попадают и пользователи, некачественно применяющие предложенные технические возможности. Кажется, что разница между этими группами велика, но это не совсем так. Первые не могут познакомиться с плодами научно-технической революции, вторые — осознанно или нет — не хотят. Результат в обоих случаях плачевен: будущее наступает без них.

Пока это расслоение может быть не столь заметным. В конце концов, многие из перечисленных технологических решений еще не стали продуктами, которые можно легко приобрести в ближайшем магазине. А какие-то рынки (например, нейротехнологий), несмотря на сопровождающий их большой медийный шум, еще только формируются. Но не надо быть футурологом, чтобы заметить: цифровые технологии завоевывают все большее внимание исследователей, становятся частью значительного количества самых разных экономических, политических, социокультурных инициатив и постепенно начинают обеспечивать жизнедеятельность не только частных лиц, но и сообществ, индустрий.

Нельзя не согласиться с культурологом О. Мороз в том, что «быть исключенным из этого контекста означает быть выключенным из современности, быть обреченным на жизнь, качество которой будет постепенно снижаться»[1].

§ 2. Безработица в результате новых технологических революций

Безработица, как и неравенство, также всегда была основополагающим фактором преступности. Новая технологическая революция усугубила безработицу и падение доходов, устранив нужду в малопро-

[1] *Мороз О.* Цифровое неравенство // Газета.ру. 2017. 11 июня. См. также: *Волченко О. В.* Динамика цифрового неравенства в России // Мониторинг общественного мнения: Экономические и социальные перемены. 2016. № 5. С. 163—182.

фессиональных рабочих. Робототехника и сложное компьютеризированное оборудование успешно заменили квалифицированную рабочую силу. Программное обеспечение теперь заменяет журналистов, создавая новости в электронном виде путем сканирования Интернета. Даже трейдеров на финансовых рынках заменяют автоматизированные алгоритмы.

Коммуникации, сделавшие возможной недорогую передачу голоса, а также почти мгновенные трансферы огромных объемов данных, наряду со все более высокочеткими изображениями, способствовали перемещению производительных мощностей. Все более возрастающими темпами это развивается в таких сферах услуг, как инженерное дело, архитектура, бухгалтерский учет, юридические услуги и даже медицинские услуги.

В сочетании с технологией удаленного управления, изначально разрабатывавшегося для военных, теперь стало возможным контролировать высокоавтоматизированное производство и даже добычу в удаленных регионах.

Многим категориям работающих независимо от профессии и навыков сейчас угрожает *технологическая безработица*.

Существовала убежденность в том, что новые отрасли вберут в себя оставшихся без работы людей. К сожалению, реальность оказалась иной. Число людей, занятых в технологическом секторе, остается скромным, около 5—6% всей рабочей силы. По некоторым оценкам, всего около 0,5% рабочей силы в США устроены в отраслях, не существовавших до 2000 г. В Кремниевой долине только 1,8% работников трудоустроены в новых отраслях.

Одна из причин кроется в том, что новые отрасли не требуют много рабочей силы, а когда требуют, то задачи выводятся на аутсорсинг самым дешевым поставщикам рабочей силы в мире. Лидирующие компании вроде Google дают всего 60 тыс. рабочих мест во всем мире.

Многим из тех, кто вынужденно лишился работы, крайне трудно найти новую. Маловероятно, что работники легкой промышленности или рабочие на сборочных мощностях интегрируются в рабочую силу в сфере знания, в технологов, биоинженеров, финансистов и т. п.

Стоимость обучения резко возросла. Многие выпускники не могут получить работу в выбранных ими отраслях, и их начальные доходы на 10—20% ниже, чем в период, когда они начинали учиться.

Сложность и динамизм цифровой экономики означают, что возможность трудоустройства для переучивающихся людей не гарантирована. Для тех, кто нашел работу, угроза неполной занятости или безработицы является постоянной, что затрудняет выстраивание дол-

госрочных планов и достижение долгосрочной финансовой и личной безопасности.

Хотя и существуют хорошо оплачиваемые места для небольшой части рабочей силы с необходимыми навыками, большинство новых рабочих мест находится в секторе низкооплачиваемых услуг, таких как розничная торговля или безопасность. Молодежная безработица остается на высоком уровне.

Бóльшая часть населения в настоящее время являются членами так называемого *уязвимого пролетариата* (термин, используемый в Японии для работников без гарантии занятости), которые составляют до 30% всех трудозанятых страны на фоне того, что компании сокращают издержки на рабочую силу.

Изменения на рынке рабочей силы влияют на характер общества. В новом цифровом мире совсем небольшая элита — 5% населения обладают существенными накоплениями и контролируют бóльшую часть ресурсов. Они нанимают еще один слой людей — 20%, чтобы управлять их делами, а также контролировать уязвимый пролетариат, который составляет 75% населения.

В международном исследовании, озаглавленном «Технологии в работе 2: будущее — это то, чего еще не было» (2016), дан всесторонний анализ рисков для традиционных моделей стран с развивающейся экономикой, которые влекут за собой резкий рост автоматизации производства.

Опираясь на информационные сводки Всемирного банка, авторы исследования соглашаются с наличием определенной угрозы в связи с автоматизацией труда в развивающихся странах. В то время как мануфактура, как правило, дает возможность развивающимся странам уменьшить экономический разрыв с более богатыми странами, автоматизированное производство, напротив, негативно сказывается на их возможностях, что требует поиска новых моделей роста.

Рост автоматизации может стать критичным для развивающихся стран, где постепенно снижается уровень потребительского спроса и ограничивается социальная защищенность. Например, осваивая автоматизированное производство и разработки в области трехмерной печати, развивающиеся страны стремятся упростить себе задачу и в связи с этим создают *угрозу преждевременной деиндустриализации*.

Российский социолог и футуролог С. Цирель в статье «Экономика ближайшего будущего»[1] исходит из того, что общество в ближайшем будущем разделится по родам занятости на три неравные группы. Самый верхний слой — топ-менеджеры крупных компаний, политики, финансисты, успешные программисты и инженеры, научная элита

[1] См.: Terra Economicus. 2017. Т. 15. № 1.

и т. д., с членами семей это не более 10% общества — в ближайшие десятилетия останется сообществом с заметным преобладанием мужчин и распределением гендерных ролей, близким к сегодняшнему. Вторая группа, наиболее многочисленная, — это основная масса работоспособного населения. Ее можно разделить на две подгруппы. Одна будет занята в отраслях с высокой степенью компьютеризации и современных технологий, и здесь основным внутренним конфликтом окажется возрастной: старшим поколениям сложнее приспособиться к быстрым технологическим переменам уже сегодня. Другая же подгруппа — это растущая сфера «контактных» услуг. И, наконец, нижний слой населения — это люди, которым просто некуда деваться при таком разделении труда, их будет около 40% в развитых странах Запада.

В «лишние люди» попадут многие представители «образцового» социально-психологического типа трудящегося индустриальной эпохи XIX — первой половины XX в. Это мужчина трудоспособного возраста с навыками физического труда, нередко с «золотыми руками», молчаливый интроверт, преданный своей семье и профессии. Он окажется в этой нижней группе, поскольку будет не нужен в эпоху всеобщей роботизации производства. В таких людях, возможно, сохранится потребность как в обслуживающем техническом персонале для робототехники, когда она будет ломаться, но, конечно, они не нужны будут в большом количестве.

Такое устройство общества, по мнению С. Цирeля, не слишком стабильно и вряд ли продержится очень долго, во-первых, в силу дальнейшего расширения роботизации и компьютеризации, возможного появления искусственного интеллекта, а во-вторых, из-за изменения самой генетической природы человека в результате развития геномики, что тоже не исключено.

При *усилении социального расслоения* должна *вырасти преступность*. Развитый мир во многом от массовой «уличной» преступности отвык за последние пару десятков лет. Это следствие и роста уровня жизни, и компьютеризации: компьютерные игры значительную часть агрессии загнали в виртуальный мир. Конечно, бывают и «выбросы» этой агрессии в мир реальный, но все же это не массовое явление. В связи с возможной массовой безработицей и неизбежным крушением социальных государств в том виде, в каком они возникли во второй половине XX в., новый всплеск преступности станет реальной опасностью.

Многие из процессов, о которых шла речь, Россию, по мнению С. Цирeля, затронут в меньшей степени. Прежде всего в России иная структура экономики, значительно более слабая, чем в ЕС и США,

организация труда, мало высокотехнологичных производств и, наоборот, по-прежнему высокая занятость. Скажем, в угольных шахтах, где у нас оборудование такое же, как в США, до самого последнего времени производительность труда была ниже в пять-семь раз, т. е. тонну угля добывает в пять-семь раз больше людей. Сейчас этот разрыв немного сократился, но по-прежнему весьма велик.

Общество, которое так выглядит, — конечно, не самое передовое. Но, как ни странно, оно за счет этого несколько более стабильно, потому что эти механизмы замедляют рост безработицы и распад традиционной структуры общества.

Потребность в ресурсах, которыми обладает Россия как самая крупная страна мира, никуда не денется. Возможно, структура российского экспорта в каких-то деталях будет меняться, но в целом поставщиком сырьевых ресурсов, возможно пищевой продукции и т. д. Россия, по мнению С. Циреля, безусловно, останется. Несмотря на падение качества образования, Россия полностью не лишится высокотехнологичных производств, хотя их доля будет небольшой; это то, что связано с военно-промышленным комплексом, с космической отраслью и некоторыми программными продуктами.

§ 3. Нарастание миграционных процессов негативного свойства

Миграция сохранит высокие темпы в течение следующих двух десятилетий. Люди ищут экономические возможности, бегут от конфликтов и ухудшающихся условий окружающей среды. Число международных мигрантов достигло самых высоких показателей в 2015 г. — 310 млн человек. Получается, что один из 112 человек в мире — это мигрант. Рост числа иммигрантов и беженцев продолжится из-за глобальной экономической дифференциации, постоянных конфликтов и усиливающейся этнической и религиозной напряженности. Число мигрирующих людей сохранится на высоком уровне или даже увеличится из-за ухудшения экологических условий в предстоящие 20 лет.

В XXI в. масштабы законных и незаконных миграционных потоков являются крупнейшими за весь исторический период. В настоящее время существуют три ярко выраженных центра, привлекающих законных и незаконных мигрантов. Это Россия, Соединенные Штаты и страны ЕС. В каждом из отмеченных регионов свои закономерности, причины и формы нелегальной миграции.

При наличии некоторых общих черт ситуация с нелегальными мигрантами в России, США и странах ЕС существенно различается в настоящее время, и будет различаться в ближайшие пять-семь лет.

Сразу после распада СССР численность нелегальных мигрантов в России из новых государств постсоветского пространства ежегодно

возрастала. Главная причина снижения численности нелегальных мигрантов в 2013—2016 гг.— это экономическая рецессия в России, начавшаяся в 2012 г. Поскольку двумя основными сферами занятости нелегальных мигрантов являются строительство и жилищно-коммунальное хозяйство, резкое уменьшение объемов жилищного строительства обрушило спрос на нелегальную рабочую силу у российских строительных организаций. При экономическом оживлении стоит ожидать нового *увеличения численности нелегальных мигрантов*.

По оценкам независимых исследовательских центров, фактическая численность нелегальных мигрантов в России составляет от 6 до 10 млн человек. Значительная часть незаконных мигрантов просачиваются на территорию Российской Федерации через российско-казахскую и в меньшей степени через российско-белорусскую границу, где де-факто отсутствует пограничный контроль. По половозрастному составу почти 75% незаконных мигрантов согласно обследованиям это мужчины. Примерно 40% из них — это молодежь в возрасте от 17 до 29 лет. Не менее 45% новых незаконных мигрантов почти или вообще не знают русского языка и не адаптированы к российскому обществу.

По официальной статистике Главного информационно-аналитического центра (ГИАЦ) МВД России, доля преступлений мигрантов в целом по России не превышает 5%. Но криминальная ситуация среди мигрантов в различных регионах и городах страны имеет существенные различия. Например, по данным ГУВД по г. Москве, в 2013—2016 гг. мигрантами в столице совершалось до 20% тяжких преступлений. Но это только видимая часть айсберга мигрантской преступности. В ходе обследований, проведенных Комитетом гражданских инициатив А. Кудрина, полицейские реагируют в среднем на одно из 7—10 заявлений, касающихся незаконных мигрантов, поскольку рассматривают такие дела как бесперспективные и имеющие тенденцию становиться, на полицейском сленге, «висяками».

Характерной для России негативной тенденцией миграции иностранных граждан является их *вовлечение в криминальную террористическую среду*. К категории этих лиц прежде всего относятся иностранные граждане:

— участники международных террористических и экстремистских организаций;

— члены организованных групп и преступных сообществ.

Еще одним фактором угрозы является *массовая вербовка* нелегалов эмиссарами ИГИЛ[1] и других радикальных группировок. Осуществля-

[1] Запрещенная в России террористическая группировка.

ется это прямо на стройках, в общежитиях и кафе, где скапливаются мигранты.

Масштабы радикализации мусульманского сообщества стран Центральной Азии можно оценить исходя из количества боевиков «Исламского государства», имеющих при себе паспорта граждан Таджикистана, Узбекистана, Туркменистана, Казахстана и Киргизии. The International Crisis Group (ICG, Международная кризисная группа) приводит следующие цифры: от 2 до 4 тыс. граждан Центральной Азии отправились на контролируемые ИГИЛ территории. По подсчетам авторитетных экспертов, в рядах ИГИЛ находится также около 5 тыс. граждан России (в основном выходцев с Северного Кавказа).

Численность нелегальных мигрантов на территории США оценивается по состоянию на 2016 г. в 11 млн человек. Если брать долю нелегальных мигрантов в общей численности населения, то она примерно равна российскому уровню и заметно выше, чем в странах ЕС. Из общего числа нелегальных мигрантов почти 55% составляют нелегальные мигранты из Мексики. Их число превышает 6 млн человек.

Несмотря на то что удельный вес нелегальных мигрантов к общей численности населения в странах ЕС несколько ниже, чем в США и России, именно ситуация с нелегальными мигрантами в Европе является наиболее обсуждаемой.

В 2016 г. Европол и Интерпол опубликовали объемные подробные доклады, анализирующие процессы нелегальной миграции в тесной увязке с организованной преступностью. Эти доклады в совокупности рисуют объективную картину ситуации с миграцией в Европе.

В последние годы беспрецедентного уровня достиг поток в Европейский Союз нелегальных мигрантов. Это в основном люди, изгнанные из родных земель нестабильностью, отсутствием безопасности и ужасающей бедностью породившими серьезный гуманитарный кризис и создавшими многочисленные возможности для транснациональных преступных сетей.

Организованные преступные группы (ОПГ) ждут миллионы мигрантов из Африки, Ближнего Востока и Азии, чтобы извлечь криминальную прибыль, эксплуатируя потребность людей в помощи и мечты о лучшей жизни. Они обеспечивают незаконное пересечение морских и сухопутных границ, изготовление и предоставление поддельных проездных документов и удостоверений личности, создают сложности для правоохранительных органов в противодействии незаконной миграции.

В 2015—2016 гг. масштабы миграционных потоков в ЕС достигли невиданных высот. По оценкам Европола, более 90% мигрантов, пре-

бывающих в ЕС, используют услуги, оказываемые *преступными сетями*. В основном они связаны с транспортировкой и обеспечением размещения в стране пребывания. В большинстве случаев эти услуги представляются преступными группами. В этом криминальном бизнесе участвует большое количество криминальных сетей, а также отдельных преступников. Они получают огромную и все возрастающую прибыль, связанную с нелегальным ввозом мигрантов.

Благоприятно расположенные вдоль маршрутов горячие точки, совпадающие с транспортными хабами, привлекают мигрантов и используются контрабандными сетями.

Горячие точки располагаются в районах с развитой транспортной инфраструктурой, включая международные вокзалы, аэропорты, порты, точки технического обслуживания для междугородних автобусов и т. п. Наряду с транспортными хабами горячие точки возникают в районах со слабым контролем правоохранительных органов, а также в разрушенных или несостоявшихся государствах. Кроме того, горячие точки расположены в зонах пограничного контроля, особенно в тех местах, где криминальным сетям удалось коррумпировать пограничников, полицейские патрули и подразделения военно-морского флота. Горячие точки расположены также в местах расселения диаспор, сходных по этническому и национальному составу с незаконными мигрантами.

Преступные сети, организующие и обслуживающие незаконную миграцию, вытянуты вдоль миграционных маршрутов. Лидерами ОПГ являются в основном граждане стран, не входящих в ЕС, имеющих то же происхождение или вероисповедание, что и мигранты. При этом в состав сетей входят преступники, являющиеся гражданами не только стран, не входящих в ЕС, но и государств — членов ЕС.

Другой вывод состоит в том, что многие лидеры и активные участники преступных сетей, родившись за пределами ЕС, в последующем стали гражданами или получили вид на жительство в странах ЕС, где они и осуществляют преступный бизнес. За пределами ЕС лидеры и активные участники преступных сетей, как правило, работают с мигрантами того же этнического происхождения, что и они сами.

Грубая оценка годового денежного оборота преступников за счет незаконного ввоза мигрантов может быть получена на основе оценки численности мигрантов в ЕС в 2015 г. Около 1 млн человек незаконно оказались в ЕС. Большинству из них было оказано содействие в перевозке, транспортировке, проникновении и закреплении в странах пребывания. В среднем мигранты заплатили за услуги от 3,2 до 6,5 тыс. долл. США или 3—6 тыс. евро за человека. Указанные цифры

позволяют оценить средний оборот преступных сетей в сумму от 5 до 6 млрд долл. США в год.

Согласно данным Европола и Интерпола преступные сети получают деньги в основном из стран конечного назначения. Это означает, что мигранты, как правило, платят не в начале маршрута, а тогда, когда достигают страны назначения. Фактически преступные сети авансируют незаконных мигрантов, поскольку транспортные услуги, а также продвижение по маршруту предполагает предварительные затраты. Преступные сети выступают как своеобразные кредитные учреждения по отношению к мигрантам. Оборотной стороной этого является жесткий контроль миграционного потока на всех его стадиях со стороны преступников с наличием в каждой мигрантской группе контролеров и своего рода охранников, обеспечивающих доставку мигрантов до места назначения в целости.

Данные Европола и Интерпола свидетельствуют: преступный бизнес на незаконной миграции все теснее сращивается с криминалом, специализирующимся на незаконном обороте наркотиков, подделке документов, имущественных преступлениях и торговле людьми и органами. В 2015 г. было выявлено более 220 случаев, когда преступные сети, занятые нелегальной миграцией, были идентифицированы Европолом как сети и отдельные преступники, участвующие более чем в одной области преступности. Из них 22% были связаны с незаконным оборотом наркотиков, 20% — с незаконной торговлей людьми, 20% — с преступлениями против собственности и 18% — с подделкой документов.

С географической точки зрения маршруты нелегальной миграции идентичны криминальным логистическим цепочкам, используемым для контрабанды товаров, а также наркотиков, оружия и т. п. В результате группы контрабандистов и наркосиндикаты включаются в бизнес, связанный с нелегальной миграцией. Кроме того, сам нелегальный интенсивный антропоток (перемещение людей) позволяет увеличить наркотрафик, объемы незаконной торговли оружием, контрабанду различных товаров и т. п.

Нелегальные мигранты уязвимы для криминальных сетей как до, так и после их прибытия в ЕС. В результате сложившихся условий, а также в силу необходимости оплатить транзит они подвергаются со стороны преступных сетей сексуальной эксплуатации, вынуждены работать на предприятиях криминальной экономики либо на легальных предприятиях без регистрации, с минимальной оплатой, перевозить наркотики, а также участвовать в качестве исполнителей самого низового уровня в деятельности преступных сетей, в том числе связанных с нелегальной миграцией.

§ 4. Усложнение технологий третьей и четвертой промышленных революций

Развитие технологий будет продолжать расширять права и возможности отдельных лиц, небольших групп, корпораций и государств, а также ускорять темпы изменений. Но этот же процесс породит новые сложные проблемы и конфликты.

Нельзя не согласиться с положениями британской Стратегии национальной кибербезопасности 2016—2021 гг. в том, что сложилась парадоксальная ситуация: чем выше технологический уровень государства и общества, чем глубже информационно-коммуникационные технологии проникли во все компоненты жизни общества, тем более уязвимыми становятся общество и государство для организованной преступности и террористов.

Разработка и использование усовершенствованных информационных коммуникационных технологий, искусственный интеллект, новые материалы, робототехника и автоматизация, усовершенствование биотехнологий и нетрадиционных источников энергии разрушат рынки труда и изменят тип экономического развития.

Новые технологии потребуют тщательного исследования, чтобы оценивать, как они воздействуют на здоровье человека, общество, государства и планету. В ближайшей перспективе будет необходимо устанавливать нормы безопасности и общие протоколы для новых ИКТ, биотехнологий и новых материалов. Немногие организации, будь то государственные, коммерческие, научные или религиозные, имеют диапазон знаний, необходимых для выполнения системного анализа, не говоря уже о предсказании технологического развития.

Без регулирующих стандартов развитие и использование искусственного интеллекта, даже менее способного, чем человеческий интеллект, будет очень опасно для людей. Оно угрожает частной жизни граждан и подрывает интересы государства. Отказ разрабатывать стандарты для искусственного интеллекта в робототехнике, вероятно, снизит экономическую эффективность из-за несовместимости отдельных составляющих робототехнических комплексов с искусственным интеллектом и контролем человека.

Биофармацевтические достижения приведут к разногласиям по поводу прав интеллектуальной собственности. Если отказы от патентов и обязательные лицензии станут более распространенными, это может угрожать появлению новых лекарств и уменьшить прибыль многонациональных фармацевтических компаний. Правительства должны будут взвесить экономические и социальные выгоды от вне-

дрения новых биотехнологий, таких как генетически сконструированные зерновые культуры.

На международном уровне возможность устанавливать нормы и протоколы, определяющие этические пределы исследований и защиту права интеллектуальной собственности, обусловит техническое лидерство.

§ 5. Восстание идентичностей в эпоху коренных технологических преобразований

Особая роль в ближайшие десятилетия будет принадлежать *восстанию идентичностей*. Экономическая, информационная и отчасти политическая унификация последних 25 лет сопровождалась усилением существующих и появлением новых этнических, культурных, религиозных и иных сообществ. Эти сообщества существуют внутри государственного устройства. В одних странах границы идентичности совпадают с государственными границами, в других — нет.

Идентичность можно определить как устойчивую платформу ценностей, верований и убеждений, определяющих как повседневное поведение людей, так и их долговременные жизненные программы. Основы идентичности могут быть различными:

— ценностная — свойственна для западной культуры;

— религиозная — характерна для регионов, населяемых мусульманами и отчасти православными христианами;

— культурно-языковая — наиболее явно присутствует в Китае, Японии, отчасти Индии и т. п. В этих странах, несмотря на различные религии и гражданские конфликты, удается избежать войн из-за того, что глубинным основанием идентичности являются не различные верования, а единые язык и культура.

Восстание идентичностей частично связано с процессами системной динамики. Чем сложнее система, тем более независимы ее компоненты. Поскольку мы сегодня живем в сложном мире, компонент идентичности стал более независимым. Его динамика входит в противоречие, например, с экономической динамикой. Последняя требует глобальной, унифицированной среды движения товаров, людей, инвестиций и информации. Любая же идентичность в известной степени самодостаточна и старается ограничить влияние внешнего мира на саму себя. Отсюда — очевидное неустранимое противоречие между императивами глобального технологического, финансово-экономического и информационного развития и требованиями выживания культурных, религиозных и иных идентичностей.

Поскольку идентичность предполагает отдельность, опираясь на нее, легко найти внешних врагов. Внешний враг крайне полезен слабым режимам, поскольку, с одной стороны, оправдывает тяготы и лишения населения стран, а с другой — выступает мобилизующим фактором, позволяющим бороться с противниками власти в собственных элитах и за рубежом.

Если ранее опора на идентичность была характерна для режимов авторитарного типа, а также в слабых и несостоявшихся государствах, то в последние годы использование *политики идентичности* становится нормой для крупных западных стран.

Если в определенных условиях и в определенные исторические периоды для слабых, технически и экономически отсталых государств мобилизационная политика идентичности имеет несомненные преимущества и оправдана будущим, то использование политики идентичности развитыми, зрелыми странами гибельно.

Использование в развитых странах подхода на основе идентичности ведет к общественной фрагментации, усилению внутренних противоречий. Все это раскручивает кризисные явления. Это плохо и для элит, и для населения. Еще хуже то, что упор на политику идентичности разваливает систему международного сотрудничества, гражданского мира и в конечном счете усиливает *глобальный беспорядок*. А глобальный беспорядок — это питательная среда для развития терроризма и преступности.

Экономическая депрессия во всех странах мира является оборотной стороной популизма. *Популистская политика* может быть успешной только в случае ведения страной крупномасштабных военных действий. В этом случае она выполняет роль обеспечения внутренней мобилизации. В таких странах, как Великобритания, Испания, Италия, а в ближайшие годы, вероятно, Германия и Швейцария, восстание идентичностей пройдет под знаменами антимиграционных настроений и регионального сепаратизма.

Религиозная идентичность в отличие от национальной и тем более культурной имеет собственную логику. Можно сделать несколько прогнозов относительно значения религиозной идентичности.

Если в странах Запада в рамках восстания идентичностей лидирующую роль будет играть популизм, то в кризисных регионах, а также странах незападной цивилизации будет все больше доминировать религиозная идентичность. Эти страны характеризуются стремительным ухудшением экономического положения, подавлением свобод и гражданских прав. Именно вера дает шанс людям выжить в столь сложной ситуации. Поэтому в ближайшие пять лет стоит ожидать глобального религиозного возрождения. В настоящее время в мире примерно 80% верующих. Аналогичный показатель до 2000 г. составлял около 60%. При этом следует отметить, что опросы, проводимые ООН, не касались стран Африки, Китая и Ирана.

Совершенно по-разному проявляется влияние религиозной идентичности на Западе и, например, на Ближнем и Среднем Востоке. На Ближнем и Среднем Востоке именно религиозная, а конкретно — исламская идентичность (связанная с принадлежностью к конкретному течению ислама, например суннитам, шиитам, суфиям и т. п.) является основой любых общностей. На Западе религия оказывает влияние на экономические, политические и социальные процессы, но не является преобладающим фактором.

§ 6. Трудности деятельности государственной власти в период третьей и четвертой промышленных революций

Правительствам в условиях неоднозначных перспектив экономического развития будет все сложнее удовлетворить общественные запросы, обеспечить безопасность, дать отпор преступности и снизить неравенство. Эти усилия будут сдерживаться фискальными ограничениями, растущей политической поляризацией, увеличивающимся разрывом между динамикой технологий, законами и нормами, лежащими в основе государственной власти.

В ближайшие десятилетия следует ожидать появления субъектов, которые могут если не бросить вызов государствам как главным субъектам, то по крайней мере серьезно ограничить их возможности и ресурсы. Речь идет не только о крупнейших корпорациях и наднациональных организациях типа ЕС. Все большее значение будут приобретать глобальные религиозно-политические движения, а также субъекты, соединяющие теневой банкинг, транснациональную преступность и неформальную занятость.

Кроме того, государства столкнутся с усилением общественного недоверия и недовольства, связанным с охватившей ведущие страны коррупцией, а также эрозией законодательства. Население развитых стран будет все более недовольно де-факто сложившимся различием в отправлении законодательства и правосудия применительно к элите и остальному населению. Это также увеличит вероятность протестов, нестабильности и эрозии государственных механизмов управления.

Основные конфликты между государством и населением будут скорее всего проходить по следующим схемам. Громкие протесты, например в таких странах, как Бразилия и Турция, где в течение последнего десятилетия значительно вырос средний класс, показывают, что более состоятельные граждане в большей степени, чем бедняки, критически настроены к правительствам и требуют решительной борьбы с коррупцией. Бедные слои населения, особенно в социальных государствах, таких как западноевропейские страны ЕС, Канада, в последние годы — США, в решающей степени зависят от государственных дотаций и пособий и поэтому готовы терпеть коррупцию и кумовской капитализм, т. е. «для своих» (crony capitalism), в обмен на продолжение выплат. Средний класс также требует от государства гарантий собственности и ведения деятельности. Они хотят быть уверены, что государство не отнимет у них то, что они приобрели в последние десятилетия. В то же время замедление экономического роста, давление на заработную плату роботизации и закредитованность ведущих экономик мира сужают возможность маневра для государств в отношении удовлетворения запросов среднего класса. Кроме того, в условиях, когда государственный долг большинства ведущих стран значительно превысил размеры внутреннего валового продукта, правительства более не смогут улучшать, а во многих случаях и поддерживать сложившийся уровень доходов бедных слоев населения. В результате правительства окажутся перед двойным вызовом: со стороны как среднего класса, так и бедняков. Это может подорвать стратегию политического управления, реализуемую в большинстве стран G20 в течение последних 25 лет.

Фактором стремительного изменения политического ландшафта уже стал все расширяющийся доступ к информации о лидерах и ведущих политиках для населения. Негативная информация о них не только подрывает доверие к источникам власти, но и делегитимизирует само государство. Сочетание уменьшения финансовых возможностей государства с негативным информационным потоком о властвующих элитах неизбежно приведет к подъему популистского движения по всему миру. Кроме того, технологический прогресс за последние 25 лет в значительной степени свел на нет влияние политических партий и профсоюзов. Власть из согласительной стала *технологичной*. Это проявилось в росте числа *технократических правительств* по всему миру.

Разрушение представительной власти вместе с делегитимизацией элит и деструкцией системы сдержек и противовесов, базирующейся на компромиссе между властвующей элитой и иными общественными группами, партиями, приведет в ближайшие годы к глубокому *кризису демократии*.

Угрозу для демократии создают и настроения молодежи. Исследования показывают, что в Северной Америке и Западной Европе молодежь все меньше интересуется политическими вопросами, отдавая предпочтения досугу и профессиональной карьере. Растет число *гибридных государств*. В них смешаны элементы демократии с чертами авторитарного правления. Как правило, такие гибридные государства склонны к консервации внутренней жизни во всех ее проявлениях. В условиях кризиса они разваливаются, оставляя за собой огромные зоны нестабильности. По сообщению неправительственной органи-

зации Freedom House, индекс свободы в 2016 г. в глобальном масштабе сократился на наибольшее значение за последние 10 лет.

Международные институты будут стараться адаптироваться к более сложной среде, стараясь компенсировать неизбежное в интервале 10—15 лет *ослабление национальных государств*. Эффективность международных институтов может быть повышена в том случае, если удастся сбалансировать интересы и выровнять вклады крупных держав по таким вопросам, как поддержание мира в кризисных регионах и оказание гуманитарной помощи в районах стихийных бедствий и политико-экономических катастроф.

Следует ожидать замедления реформы международных и региональных институтов, а также возрастания препятствий при создании новых организационных структур международного характера. В решающей степени это будет связано с неизбежным в ближайшие 10—15 лет кризисом национальных государств из-за снижения темпов экономического роста, возрастания долговой нагрузки и старения населения. В этих условиях неизбежны рост популизма, а также стремление к возведению таможенных барьеров.

Кризис международных институтов еще более ослабит национальные государства. Терроризм, киберпреступность, трансграничный криминал не ограничены рамками национальных государств и будут действовать как глобальные структуры. В условиях практически неизбежного кризиса международных институтов и возрастания политического и экономического национализма это чревато не только кризисом международного масштаба, но и внутренними проблемами для всех развитых государств.

Уже сейчас наблюдается *драматическое отставание юридической и политической системы государств от технологического развития*. Существующие институты не способны эффективно регулировать нетрадиционные вопросы, такие как синтетическая биология, искусственный интеллект, совершенствование человека, как в части законодательной и правоприменительной практики, так и в практической деятельности. Темпы технологических изменений значительно опережают возможности государств, агентств и международных организаций по установлению и применению юридических норм, технических стандартов, управленческой политики. Это порождает все более увеличивающийся серьезный дисбаланс между возможностями и полномочиями государств в новых сферах; благоприятствует наращиванию потенциала террористов, преступников и субъектов «кумовского» (дружеского) капитализма. Это особенно верно для киберпространства, где частные коммерческие акторы и преступные структуры играют де-факто бóльшую роль в формировании тенденций развития, чем государство.

§ 7. Многомерная многосторонность международных и внутригосударственных конфликтов

Риск возникновения конфликтов увеличится из-за расхождения интересов среди ведущих держав, увеличения террористической угрозы, длительной нестабильности в слабых государствах и распространения смертельных, разрушительных технологий. Разрушающиеся общества и несостоявшиеся государства станут более распространенным явлением. Они будут обладать высокоточным оружием дальнего радиуса действия, кибер- и роботосистемами для проникновения в целевые инфраструктуры издалека и более доступными технологиями для создания оружия массового уничтожения.

В течение следующих 20 лет настоящие и будущие тенденции будут вести в беспрецедентном темпе к увеличению числа и сложности проблем. Наиболее разрушительными из них будут *кибератаки, терроризм* и *экстремальные погодные условия*.

Демографические изменения повлияют на работоспособность, социальное обеспечение и социальную стабильность. Богатый мир стареет, в то время как бóльшая часть бедного мира — нет. Все больше и больше людей живут в городах. Некоторые из них становятся все более уязвимыми в результате природных катаклизмов. Борьба за хорошую работу приобретает глобальный масштаб, в то время как технологии разрушают рынок труда. Технологии будут способствовать расширению возможностей отдельных лиц и небольших групп объединять людей. В то же время ценности, национализм и религия будут все больше разделять их.

На национальном уровне разрыв между популярными ожиданиями от правительственных действий и реальными действиями будет увеличиваться. Сама демократия уже не может быть принята как само собой разумеющееся явление. За ее сохранение придется бороться. На международном уровне концентрация власти в отдельных элитных группах ухудшит коллективное взаимодействие против глобальных проблем.

Растет риск возникновения конфликтов. Война будет все меньше и меньше походить на войны прошлого. Сотрется разница между миром и войной, тылом и фронтом, между регулярными подразделениями армий и иррегулярными формированиями[1]. Все чаще конфликты будут происходить не на поле боя, а в киберпространстве, финансово-экономической и ментальной сферах.

Хронические угрозы загрязнения воздуха, нехватка воды и изменение климата станут более заметны. Это приведет к серьезным столкновениям.

[1] См.: *Ларина Е., Овчинский В.* Мировойна. Все против всех. Новейшие концепции боевых действий англосаксов. М., 2015.

Среди крупных держав, элит и населения чем дальше, тем больше нет согласия в вопросе о путях решения глобальных и региональных проблем. Динамика развития приходит в острое противоречие с расстройством системы глобального управления.

В следующие 20 лет будут нарастать риски возникновения конфликтов, в том числе межгосударственного характера. Конфликты будет порождать не только соперничество между крупными державами, но и их увлечение гибридными и прокси-войнами (англ.: proxy — представитель), т. е. опосредованными войнами, ведущимися чужими руками. В межгосударственных конфликтах все шире будут участвовать частные военные компании, иррегулярные воинские образования, рекрутируемые из бывших военных и криминала и т. п. Данный фактор в сочетании с нарастанием глобальной террористической угрозы и усилением нестабильности в несостоявшихся и гибридных государствах особо взрывоопасен в условиях распространения смертоносных и разрушительных технологий.

Ожидается перелом тенденции, имевшей место в последние 30 лет и связанной со снижением числа и интенсивности конфликтов. Вероятно, в предстоящие 20 лет число, разнообразие и интенсивность конфликтов увеличатся. Соответственно, заметно возрастут не только смертность на поле боя, но и потери среди гражданского населения.

В условиях, когда небольшие террористические, повстанческие и преступные группы могут иметь на вооружении технологии массового поражения, может возникнуть уникальная ситуация, отбрасывающая нас в Средневековье, когда с бандами преступников и отрядами наемников воевали государства. Эта тенденция уже проявляет себя. Количество, интенсивность, человеческие и экономические издержки конфликтов неуклонно растут, начиная с 2011 г.

История гражданских конфликтов в Египте, Ливии, Сирии, на востоке Украины показывает, что для подобных конфликтов характерно стремительное нарастание числа независимых друг от друга участников, вплоть до полной неразличимости повстанцев, террористов и криминальных группировок. Главная опасность конфликтов подобного типа состоит в том, что в них так или иначе участвуют в виде сил поддержки крупные державы. Соответственно, неуправляемые локальные конфликты вписаны в глобальный геополитический контекст и повышают риски возникновения серьезных кровопролитных конфликтов. Принципиальной чертой следующих 30 лет будет стирание граней между военными и невоенными инструментами, войной и миром, юридическими нормами, применимыми в мирной и военной жизни. Более того, в ходе таких конфликтов стираются четкие грани между повстанцами, преступниками и террористами. Это становится огромной проблемой для всех крупных держав.

Будущие конфликты предполагают расширение сферы противоборств. Противоборства будут происходить не только в военной и дипломатической, но и в информационной, психологической, экономической и технологической сферах. В будущих конфликтах более слабая сторона будет максимально уклоняться от традиционных военных действий и сосредоточивать свои усилия на террористических атаках против мирного населения и разрушении критической инфраструктуры противника. Инициаторы конфликта будут уходить во все более глубокое подполье.

Война в физическом пространстве будет все более приближаться по своему характеру к войне в киберпространстве. Идеалом для инициаторов подобных конфликтов будет ситуация, когда невозможно разобрать, кто, зачем и против кого воюет. Первый пример конфликта такого рода можно наблюдать в настоящее время в Сирии.

Для инициаторов конфликтов нового типа главным инструментом станет целенаправленное стравливание между собой этнических, религиозных, культурных, экономических и политических групп и их максимальное раздробление. Данная технология позволяет нарушить инфраструктуру общественного сотрудничества, которая является основой функционирования любого государства, возможно не менее важной, чем сама государственная власть. Такая стратегия направлена на максимальное обезличивание инициаторов при минимизации их расходов и перекладывании их на население и различного рода группы внутри страны — поля конфликта.

Подрывные группы. В последние годы проявилась тенденция, которая будет оказывать влияние в течение ближайших 20 лет. Негосударственные группы, в том числе террористы, боевики, преступные группировки, будут иметь все более широкий доступ к все более разнообразному спектру летальных и нелетальных средств огневого, инфраструктурного и поведенческого поражения. Уже сегодня такие группы, как «Хизболла» и ИГИЛ, получили доступ к самому современному вооружению и широкому спектру технологий. Это не только противотанковые ракеты, ракеты класса «земля — земля», дроны, но и современные виды программно-аппаратных средств информационного и поведенческого воздействия. Ранее такие вооружения были монополией государственных армий. Есть основания полагать, что неконтролируемая диффузия вооружений будет продолжаться.

Дополнительным фактором станет повсеместная доступность кибервооружений, которые уже сегодня могут нанести ущерб, превосходящий разрушения, вызванные огневым оружием. Появление у деструктивных группировок все более разрушительных вооружений неизбежно будет побуждать государства и коалиции к превентивным,

опережающим действиям против них. Это, в свою очередь, начнет раскручивать спираль конфликта, циклы насилия и придавать им все более идеологический характер, вплоть до религиозных войн.

Удаленные войны. Господствующей тенденцией конфликтов нового типа станет стремление государств и негосударственных акторов вести так называемые *неопознанные войны*, предполагающие акцент на дистанционных действиях. Дистанционные атаки будут осуществляться как комбинация кибератак, использования высокоточного оружия, роботизированных систем и беспилотного оружия с применением средств поведенческого и психологического воздействия.

Дистанционные атаки ведут к снижению порога для начала конфликта. В то же время войны как обмен дистанционными атаками ломают равновесие между мечом и щитом. В удаленных войнах гораздо большее, чем в обычных, преимущество получает тот, кто атакует первым. Конфигурация конфликтов такого типа в решающей степени будет зависеть от того, способна ли одна из сторон конфликта не позволить другой навязать обычные военные действия, может ли она перенести военные действия на территорию напавшей страны. В связи с этим, несмотря на кажущийся менее кровопролитный характер войн издалека, они имеют гораздо больший, чем традиционные войны, потенциал неуправляемой эскалации. Кроме того, в таких войнах даже на первом этапе неизбежно будут задействованы не только дисциплинированные воинские подразделения или даже террористические сети, но и никому не подчиняющиеся повстанческие отряды, сформированные из бывших преступников, или преступные группы, называющие себя повстанческими отрядами.

Будущие кризисы неизбежно будут иметь гораздо больший эскалационный потенциал и меньшую управляемость, чем традиционные войны, поскольку стороны — инициаторы конфликта будут иметь равные стимулы, чтобы нанести удар первыми, до того, как они подвергнутся нападению.

В удаленной войне целями первого порядка станут телекоммуникации и, соответственно, спутниковые группировки, их поддерживающие.

Проблема нового оружия массового поражения. Потенциально самой большой угрозой миропорядку является использование в качестве оружия достижений *биотехнологий и синтетической биологии*. Эти технологии практически недоступны для международного контроля в его сегодняшнем виде, а по разрушительной мощи не уступают ядерному вооружению. Имеются данные, что овладеть подобного рода оружием стремятся не только известные террористические организации и преступные группировки.

В ближайшие два десятилетия вполне возможен крах слабых государств, обладающих определенной научной базой, в том числе на территории Европы и Центральной Азии. Это откроет путь террористам и преступникам для овладения лабораториями и специалистами, способными произвести оружие массового поражения. Кроме того, возможна несанкционированная передача оружия массового поражения террористам и преступникам из государственных арсеналов в слабых и несостоявшихся государствах.

Конфликты в «серых» зонах. Размывание грани между войной и миром, между армиями национальных государств, частными военными компаниями и различного рода иррегулярными формированиями, между полноценными военными действиями, спецоперациями и террористическими актами, между непосредственными войнами и прокси-конфликтами меняет динамику современного мира. Чем дальше, тем больше эта разница будет стираться. Многие силы в современном мире заинтересованы в последовательном расширении «серой» зоны конфликтов. Их наиболее точным определением будет являться состояние «ни войны, ни мира». (Как известно, впервые этот термин применил Л. Троцкий при заключении Брестского мира.)

Характерной чертой конфликтов в «серых» зонах является изменение соотношения между летальными и нелетальными компонентами конфликта. На протяжении всей истории сердцевиной, кульминацией конфликта выступало применение летального оружия. Именно это подчеркивало высказывание «Война — это продолжение политики иными средствами».

В ближайшие 20 лет наряду с традиционными военными конфликтами все бóльшую роль будут играть конфликты, где применение летальных вооружений является вспомогательным компонентом. Основное противоборство будет в финансово-экономической, технологической, информационной, поведенческой, экологической сферах и конечно же в киберпространстве.

Проблема воды — ключевой фактор геополитики XXI в. При трех основных сценариях климатической динамики в ближайшем будущем: соответственно, похолодании, потеплении и усилении волатильности, или неустойчивости, климата — в мире будет нарастать проблема обеспечения населения и экономики пресной водой.

Данная проблема выходит за рамки экологии и в значительной степени порождена урбанистикой и социальными процессами. Человечество на протяжении всей истории использует примерно одни и те же водные ресурсы. Проблема состоит в том, что эти же ресурсы используются для решения промышленных, транспортных и иных задач. Кроме того, в последнее 15-летие по экспоненте развивается процесс переструктурирования зон расселения.

Мегаполисы и агломерации все более сдвигаются из глубины континентов и территорий в прибрежные районы морей и океанов. Если еще в 1950 г. в промышленно развитых государствах в прибрежных районах проживало не более 15—17% населения, то теперь эта доля перевалила за 50%. При этом в прибрежных районах может сложиться гораздо более неблагоприятная ситуация с пресной водой, чем во внутриконтинентальных с их реками и озерами.

Пресная вода, получаемая человечеством из рек и озер, как правило протекающих по территории нескольких государств, в течение столетий была предметом конфликтов, включая войны. Именно для преодоления конфликтов, связанных с водой, стали заключаться первые крупные международные правовые соглашения. В этом смысле вода — в известной степени основа нынешнего мирового юридического порядка.

Еще более опасная ситуация сложилась с системами водоснабжения крупных городов и агломераций. В странах G20 не менее трети систем городского водоснабжения находятся в руках компаний, связанных либо замеченных в связях с криминалом. Реальная доля может быть еще выше.

Принимая во внимание тесную связь криминала с терроризмом, можно утверждать, что системы городского водоснабжения являются одной из критических систем жизнеобеспечения цивилизации. Кроме того, в западноевропейских странах в 2016 г. до половины работников, обслуживающих системы городской канализации мегаполисов, были мигрантами, преимущественно мусульманского вероисповедания. Подавляющая часть из них являются гражданами других стран, нередко мигрантами во втором и третьем поколении. Однако в условиях нехватки средств в городских бюджетах и наличия связей компаний-эксплуатантов и владельцев систем городского водоснабжения с криминалом в структуре занятых постоянно растет доля нелегальных мигрантов. Они в значительно большей степени, чем легальные мигранты, подвержены влиянию джихадизма и прямо или косвенно связаны с ультрарадикальными движениями и группировками. Это также ведет к растущим рискам.

§ 8. Возрастание мощи небольших негосударственных групп и повышение потенциала террористов

Данная тенденция обусловлена рядом факторов.

1. Ключевым фактором повышения могущества малых групп и индивидов является *развитие ИКТ*. С одной стороны, развитие этих технологий привело к широкому внедрению Интернета, а соответственно, и к возможности не только разрушить, но и взять под управление любые системы, связанные с Интернетом через киберпространство. С другой стороны, ИКТ резко удешевляют производственные процессы и делают доступными многие изделия, оборудование и т. п. для небольших групп. Наконец, информационные технологии в значительной мере развиваются вне системы защиты интеллектуальной собственности на основе решений с открытым программным кодом. Соответственно, небольшие группы и даже отдельные граждане могут получить новейшие разработки критических технологий, например искусственного интеллекта, по сути, бесплатно.

2. Смена технологических, институциональных и юридических основ глобальной финансово-экономической системы открывает возможность для различных акторов — от преступных синдикатов до религиозных групп — *бесконтрольно отмывать, накапливать и транспортировать деньги и иные активы*. Согласно имеющимся данным в офшорах, находящихся в основном под британской и голландской юрисдикциями, находится сейчас примерно 6 трлн долл. США из общей суммы 19 трлн долл. США в офшорах. Теневой банкинг набирал силу в течение последних 40 лет.

Стремительное развитие криптовалют, нерегулируемых платежных сервисов, множества платформ новых финансов типа краудинвестинга, краудлэндинга и т. п. ставит крест на банковской системе, базирующейся на господстве центральных банков, национальной юрисдикции и хранимых транзакциях. Особенность новой финансовой экономики такова, что даже при наличии политической воли чем дальше, тем больше понять источники и локацию финансовых средств или иных активов не представляется возможным.

3. *Многофункциональный характер* любой *современной технологии* способствует тому, что практически одни и те же механические узлы, компьютерные программы и технологические решения могут быть использованы как в военной и гражданской, так и в преступной и террористической деятельности. Большинство новых высоких технологий появляется на широком рынке даже быстрее, чем у государства. В сочетании с эффективными системами рекрутинга и телекоммуникаций это резко повышает могущество негосударственных деструктивных сил, включая повстанцев, террористов, преступников и т. п.

В последние два-три года мир стал свидетелем беспрецедентного использования информационной среды для обеспечения управляемой деградации когнитивных процессов в обществе, его фрагментации и дезинформации.

В информационной сфере сегодня возобладали деструктивные процессы. Если в ближайшее время не будут осуществлены решительные действия, то именно они определят информационный ландшафт двух ближайших десятилетий. Если в течение первых 25 лет развития Интернета киберпространство объединяло людей доброй воли и создавало беспрецедентную среду знаний, торговли и общения, то в следующие 25 лет информационная сфера может стать местом разрушения ценностей и основ общества, подрыва любых общих интересов и полем глобальной информационной войны.

Борьба без правил в информационном пространстве на межгосударственном и внутригосударственном уровне приведет к тому, что сложившиеся политические классы перестанут существовать, гражданские общества будут дезорганизованы и деморализованы. Соответственно, выгоду получат небольшие радикальные центры по всему политическому и идеологическому спектрам.

Повышение могущества отдельных лиц и групп имеет преимущественно деструктивный, а не конструктивный характер. Малые группы, непримиримо настроенные к гражданскому обществу, могут добиться очень многого в разрушении, но не в выработке конструктивных решений или достижении консенсуса противоречивых интересов, имеющихся в каждом обществе.

Большинство известных исследовательских центров, эксперты разведсообществ США, Европола и Интерпола прогнозируют, что в ближайшие десятилетия все ведущие государства ожидает тяжелейший глобальный кризис. Выход из него может длиться продолжительное время, вплоть до 7—15 лет.

Неблагоприятные тенденции в области экономического роста будут накладываться на растущее могущество негосударственных акторов, включая террористические организации и преступные сети.

Государства и крупные организации, включая корпорации, даже не приступили в настоящее время к разработке программ классификации опережающего распознавания и отражения угроз со стороны компактных групп, включая террористов, преступников, а также групп политического действия и религиозных фанатиков.

Аналитики разведсообщества США выделяют следующие наиболее опасные и принципиально новые угрозы:

— *интегрированные образования* глобального или регионального характера, в состав которых входят террористические и криминальные группировки, легальные общественные организации и религиозные микроконфессии, и даже политические объединения, и легальные экономические и финансовые структуры. По располагаемым ресурсам такие группировки могут превосходить некоторые средние,

а то и крупные государства. При этом в отличие от государств они будут действовать вне и поверх границ, не соблюдая правовых норм;

— глобальные *религиозно-террористические движения*. В настоящее время подобные движения используют в качестве своей общей ценностной базы различные направления ислама. Это известные ИГИЛ, «Аль-Каида», «Талибан» и т. п. Есть основания полагать, что ИГИЛ — это лишь первоначальная локализованная форма всемирного халифата. Он останется субъектом международной политики на десятилетия. Если сегодня борьба с ИГИЛ предполагает в первую очередь удаленные военные действия на ближне- и средневосточном театрах военных действий и контртеррористическую борьбу в других регионах мира, то в ближайшее время ИГИЛ, вероятно, перенесет противоборство с крупными державами во все сферы. Возможно возрождение на новой основе *анархо-террористических организаций*, чьей экономической базой являются наркотрафик и эксплуатация природной среды, а идеологической — католицизм в форме теологии освобождения в Латинской Америке;

— локальные, в том числе небольшие, *группы действия*. Такие группы будут состоять из высокообразованных, технически компетентных и профессионально продвинутых людей с экстремистскими убеждениями. Прообразами таких малых групп являются хакерские группировки, а также некоторые группировки цифровых хактивистов. Историческими предшественниками групп действия были состоящие в основном из интеллектуалов «Красные бригады» в Италии и «Роте арми» Баадера — Майнхофа в ФРГ в XX в.

В последние годы идет незаметный и малопонятный процесс переплетения, а точнее, использования террористическими структурами догматов тех или иных вероучений, прежде всего ислама, его организационных и социальных инфраструктур. На протяжении истории именно вера была наиболее мощным фактором мобилизации элит и масс.

Правительства и гражданские общества Северной Америки и Европы недооценивают угрозу ИГИЛ. Это террористическая организация, в известном смысле порожденная и пронизанная одним из течений ислама. Для простоты прижилось наименование «джихадизм». Но оно является неправильным. Джихад — это священная война. В джихаде могут участвовать любые мусульмане, будь то шииты, сунниты, суфии и т. п.

Вследствие недостаточного внимания к анализу теологической проблематики терроризма, по мнению экспертов разведсообщества США, Запад не понимает, что ИГИЛ — это не одно из ответвлений салафизма или ваххабизма, к которым он не имеет никакого отноше-

ния, а уникальное течение ислама, специально адаптированное для быстрого понимания и принятия людьми, даже первоначально далекими от ислама. ИГИЛ рассматривается как террористическая организация. Нередко даже в документах внутреннего пользования, а тем более в меморандумах, рассчитанных на политическое руководство и широкую публику, западное разведывательное сообщество привыкло перечислять через запятую ИГИЛ, «Аль-Каида», «Джебхад ан-Нусра», «Талибан» и т. п.

На основании анализа всего основного корпуса теологических трудов богословов, близких к ИГИЛ, имеющихся в распоряжении видеокурсов и проповедей, а также практики этой организации можно сделать вывод, что ИГИЛ не является типичной джихадистской террористической организацией типа «Аль-Каиды», а представляет собой своего рода военно-религиозный орден. В отличие от орденов древности и Средневековья он в своей деятельности использует высокие технологии, опирается на разнообразные организационные структуры и действует по всему миру.

Однако по сути ИГИЛ является именно *орденом*, т. е. боевой организацией, силой и молитвой распространяющей определенное религиозное учение всюду, где это возможно. Такая постановка вопроса позволяет по-новому посмотреть на стратегию и тактику ИГИЛ. Она позволяет излечиться от иллюзий относительно того, что взятие Мосула или Ракки будет означать победу и конец ИГИЛ. Любой орден предполагает мученичество. Чем больше игиловцев и мирного населения погибнет в Мосуле и Ракке, тем больше шансов, что ИГИЛ активизирует свои спящие ячейки в Европе, Америке и в России.

Аналитики разведки США прогнозируют: в течение ближайших пяти лет, несмотря на военные успехи, не удастся не только победить, но и сколько-нибудь сильно ослабить терроризм. Террористические насильственные структуры, базирующиеся на тех или иных направлениях ислама, будут оставаться фактором международной политики. Наиболее опасной, но вполне вероятной тенденцией в течение ближайших пяти лет станет перемещение активности ИГИЛ как наиболее мощной исламистской террористической организации с истощенных войной ресурсных площадок суннитских районов Ирака и Сирии в Ливию и Пакистан. В обеих этих странах сегодня существуют мощные подразделения ИГИЛ, которые контролируют определенные территории и обладают воинскими подразделениями. Выход в Ливию фактически открывает для ИГИЛ южное подбрюшье Европы. Оперирование в Пакистане позволяет ИГИЛ вплотную подойти к овладению ядерным оружием.

Не только религия, но и *психологические* и *социальные факторы* будут способствовать усилению террористических организаций и увеличению активности наряду с террористическими сетями и орденами небольших групп и даже единичных террористов. К этим факторам относятся:

— растущий уровень отчуждения и атомизации внутри всех развитых стран. Повсеместно социум все более фрагментируется и разобщается по все большему числу признаков. Угнетаемое меньшинство может увидеть в терроризме единственный способ защиты своих интересов. В современных динамичных и фрагментированных обществах для угнетаемых групп и индивидов единственной защитой становятся семейные и родовые связи, а также сообщества выходцев из одного населенного пункта или сельской местности, а также религиозные центры. Они являются важным фактором, вовлекающим индивидов в террористические организации;

— кризис западной идентичности. Потребительская ориентация обществ Северной Америки и Европы вызывает протест у определенных групп населения, в основном молодежи. Те группы, которые склонны к пассивному протесту, как правило, примыкают к различного рода новым религиозным культам, а сторонники активных форм протеста в зависимости от обстоятельств либо вливаются в ряды экстремистских несистемных политических организаций, либо пополняют ряды террористов;

— кризис государства. Северная Америка и Европа в XXI в. под воздействием экономических сложностей переживают кризис социального государства. Если в XX в. государства в Европе и Америке вкладывали значительные средства и усилия в интеграцию вновь прибывающих мигрантов в западное общество, то в XXI в. победила доктрина мультикультурализма. Это произошло не вследствие несуществующего либерального заговора, а сугубо по финансовым причинам. Мультикультурализм предполагает проживание в рамках одного государства различных этноконфессиональных групп, сохранивших свою идентичность. Это означает, что не надо тратить деньги на интеграцию. Соответственно, легальные и нелегальные мигранты оказываются в странах нового проживания предоставленными сами себе и, испытывая фрустрацию, ищут защиту и поддержку в мечетях, частично находящихся под контролем радикальных и террористических организаций;

— обострение этнических и религиозных конфликтов. По всему миру в условиях ослабления национальных государств возрастает конфликтность между культурно-религиозными идентичностями.

Технология — всегда палка о двух концах. С одной стороны, она облегчает террористам взаимодействие, рекрутинг, материально-техническое обеспечение и осуществление кровопролитных актов. С другой стороны, технологии предоставляют властям, располагающим бóльшими ресурсами, чем террористы, возможность своевременно выявлять и распознавать угрозы, а также эффективно купировать их, впрочем, если им это позволяет общественность.

В ближайшие годы *террористические акты будут перемещаться в киберпространство*. Это не обязательно означает, что террористические акты будут осуществляться в киберпространстве. Это означает, что террористы все активнее будут использовать уязвимость критической инфраструктуры государственных, корпоративных и частных сетей, соединенных с «Интернетом всего», для осуществления кровопролитных террористических актов. В отличие от традиционных огневых атак подобные террористические акты чрезвычайно сложно распознать. Это конечно же резко дестабилизирует глобальную ситуацию.

Технологии в целом ведут к постепенной передаче многих функций от иерархических, жестко организованных структур к *децентрализованным сетям*. Не вызывает сомнения, что децентрализованные сети слабее защищены от атак террористов, чем иерархические.

Британские исследовательские центры и структуры по борьбе с терроризмом — разработчики Стратегии национальной кибербезопасности 2016—2021 гг. — полагают, что в ближайшие пять лет в странах Западной Европы и Северной Америки будет иметь место буквально взрыв кибертерроризма, связанного с исламскими экстремистскими террористическими сетями. Это произойдет под влиянием как минимум трех обстоятельств:

— во-первых, из года в год растет число молодых людей, исповедующих фундаменталистские и экстремистские версии ислама и находящихся под влиянием террористических сетей, в первую очередь ИГИЛ, которые обладают навыками использования относительно сложных программных продуктов;

— во-вторых, военные действия в странах Ближнего Востока, а также фундаменталистский религиозный экстремизм в странах Среднего Востока продолжают подпитывать эмиграционные потоки из региона. Среди легальных эмигрантов значительно число лиц, имеющих высокий уровень образования и компетенции в ИКТ;

— в-третьих, в силу отмеченных выше процессов формирования глобального хакерского общества, различные сегменты которого спонсируются технологически развитыми государствами, все бóльшие масштабы приобретает рынок хакерских, шпионских и боевых программ. Как любой рынок, данный рынок не имеет ограничений для

покупателей. Соответственно, последние достижения в области кибервооружения уже в ближайшие годы станут доступными для террористов.

В ближней перспективе не следует ожидать, что в будущем террористические группы и сети будут продолжать действовать исключительно в физическом пространстве. Особенности киберпространства делают эту среду достаточно безопасной для хакеров, особенно малых группировок, с которыми трудно работать методами агентурного проникновения.

В связи с этим британская Стратегия национальной кибербезопасности 2016—2021 гг. исходит из предположения, что в ближайшем будущем отдельные лица, в основном из числа молодежи, а также маленькие — в три-пять человек — хакерские группы будут осуществлять кибератаки не только пропагандистского или шпионского характера, но и нацеленные на разрушение критических инфраструктур. Эти персоны и группы не будут находиться в непосредственной связи с руководством террористических сетей. Они будут действовать по призыву их лидеров, подобно тому как террористы-одиночки действуют в физическом пространстве. Реальное будущее кибертерроризма — это *боевое хакерство малых групп*, осуществляющих свои акты самостоятельно, но от имени и под эгидой террористических сетей, прежде всего ИГИЛ. Одиночный терроризм шагнет в цифровом мире из физического пространства в цифровую среду.

Сопоставляя плюсы и минусы развития информационно-коммуникационных и иных технологий для террористов, приходится сделать вывод: в конкретных сложившихся условиях у террористов появляются новые возможности при снижении рисков.

Раздел II
ПРЕСТУПНОСТЬ ЦИФРОВОГО МИРА

Глава 3. Киберпреступность

§ 1. Международно-правовое определение киберпреступности[1]

В многочисленных научных исследованиях предпринимаются попытки определить термин «киберпреступность». Из практически 200 актов национального законодательства, указанных странами в ответах на вопросник Всестороннего исследования проблемы киберпреступности (ООН, 2013)[2], менее чем в 5% случаев термин «киберпреступность» присутствовал в названии или содержании правовых норм. Вместо этого в законодательстве чаще употребляется термин «компьютерные преступления», «электронные средства связи», «информационные технологии» или «преступления в сфере высоких технологий». На практике многие из этих законодательных актов определяют преступления, которые включены в понятие киберпреступности, например, несанкционированный доступ к компьютерным системам или воздействие на компьютерные системы или данные. В тех случаях, когда в национальном законодательстве слово «киберпреступность» все же присутствовало в названии законодательных актов или разделов, в разделе, в котором давались определения, редко присутствовало определение термина «киберпреступность». Если же правовое определение термина «киберпреступность» и закреплено в законодательстве, как правило, оно просто представляет собой отсылку «преступления, определенные в настоящем Законе».

На 10-м Конгрессе ООН по предупреждению преступности и обращению с правонарушителями (2000 г., Вена) в ходе семинара на соответствующую тематику были выработаны два определения. *Киберпреступность в узком смысле* (компьютерная преступность) — это любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных. *Киберпреступность в более широком смысле*

[1] Более подробно см.: Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. *В. С. Овчинский*. М., 2017.

[2] URL: http://cybersafetyunit.com.

(преступления, связанные с применением компьютеров) — это любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети.

Одно общепринятое определение описывает киберпреступность как любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры или сети. Такое широкое определение вызывает ряд трудностей. Например, следует ли называть киберпреступностью убийство, если правонарушитель использовал клавиатуру для того, чтобы ударить и убить жертву?

В некоторых определениях предприняты попытки учесть цели или намерения и дать более точное определение киберпреступности, определяя ее как действия, осуществляемые посредством компьютеров, которые либо являются незаконными, либо считаются противоправными некоторыми сторонами и которые могут быть совершены с помощью глобальных электронных сетей. Эти более точные описания исключают случаи, когда физическое оборудование используется для совершения обычных преступлений, но они рискуют исключить преступления, которые считаются киберпреступлениями в международных соглашениях, например в Конвенции Совета Европы о компьютерных преступлениях.

Что касается международных или региональных правовых документов, то лишь немногие из них предлагают определение киберпреступности. Например, ни в Конвенции Совета Европы о компьютерных преступлениях, ни в Конвенции о борьбе с преступлениями в области информационных технологий Лиги арабских государств, ни в проекте Конвенции Африканского союза нет определения термина «киберпреступность» для целей этих документов. В Соглашении о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации не используется термин «киберпреступность», а дается определение «преступления в сфере компьютерной информации», которое представляет собой «уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация». Аналогичным образом в Соглашении о сотрудничестве в области обеспечения международной информационной безопасности между правительствами государств — членов Шанхайской организации сотрудничества понятие «информационная преступность» определяется как «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях».

В названном выше исследовании ООН не ставилась задача определения термина «киберпреступность» как такового, а установлен пе-

речень или набор деяний, которые могут составлять киберпреступность. Это позволило сосредоточить внимание на тщательном описании точных действий, которые подлежат криминализации[1].

Анализ международных и региональных правовых документов позволил выявить два основных подхода: а) использование терминологии на базе понятий «компьютерные данные или системы» и б) использование терминологии на базе понятий «информационные данные или системы».

В Конвенции Совета Европы о компьютерных преступлениях используются термины «компьютерная система» и «компьютерные данные». В проекте Конвенции Африканского союза также используются термины «компьютерная система» и «компьютерные данные». Решение ЕС об атаках на информационные системы содержит термины «информационная система» и «компьютерные данные». В Конвенции Лиги арабских государств используются термины «информационная система» и «данные», а в Соглашении Содружества Независимых Государств — термин «компьютерная информация».

Однако анализ элементов определений показывает, что эти термины могут в целом считаться взаимозаменяемыми.

Международные и региональные правовые документы в основном содержат нейтральные с точки зрения технологий формулировки. Они не определяют перечень устройств, которые могут считаться компьютерной или информационной системой. В большинстве случаев такой подход считается оптимальной практикой, если он позволяет снизить риск того, что новые технологии не подпадут под действие правовых норм, в связи с чем потребуется постоянная доработка законодательства.

Опираясь на основополагающее понятие обработки компьютерных данных или информации, эксперты ООН утверждают, что правовые нормы, как правило, применимы к таким устройствам, как центральные процессоры и серверы, настольные персональные компьютеры, портативные компьютеры, смартфоны, планшеты и бортовые компьютеры, установленные на транспортных средствах и машинном оборудовании, а также к мультимедийным устройствам, таким как принтеры, MP3-плееры, цифровые фотоаппараты и игровые автоматы.

[1] Следует отметить, что такой же подход используется в международных правовых документах, таких как Конвенция Организации Объединенных Наций против коррупции, где не дается определение термина «коррупция», а устанавливается обязанность государств-участников признать в качестве уголовно наказуемых определенный набор деяний, которые можно более точно определить. Поэтому понятие «киберпреступность» лучше рассматривать как *совокупность* деяний или действий.

Исходя из понятия «обработка компьютерных данных или информации», вполне можно утверждать, что это определение охватывает любые устройства, такие как беспроводной или проводной маршрутизатор, который подключен к Интернету. Строго говоря, носители данных, такие как жесткие диски, карты памяти USB или флэш-карты, могут являться, а могут и не являться частью «компьютерной системы» или «информационной системы». Но если они не являются ее частью, правовые нормы все же могут определять их в качестве соответствующих объектов.

По мере перехода к «Интернету вещей» и развития нанокомпьютерных технологий в мире может потребоваться более полное описание таких понятий, как «компьютерная система» или «информационная система», которые охватывали бы более широкий круг устройств. Однако в принципе основное понятие «автоматическая обработка информации» может оказаться достаточно гибким, чтобы охватить, например, встроенные в бытовые приборы интеллектуальные микросхемы мониторинга и контроля с применением технологий NFC[1] и IP-подключения.

«Компьютерные данные» или «компьютерная информация» обычно определяются как отображение фактов, информации или понятий в форме, пригодной для распознавания, обработки или хранения с помощью компьютера. В некоторых случаях уточняется, что сюда относятся и компьютерные программы. В остальных случаях этот аспект не уточняется. На практике к компьютерным данным или информации могут относиться и данные или информация, хранящиеся на физических носителях данных (таких как жесткие диски, карты памяти USB или флэш-карты), данные или информация, хранящиеся в памяти компьютерной системы или информационной системы, передаваемые данные или информация (через беспроводную, оптическую или радиосвязь) и физическое изображение данных или информации, например в печатной форме или на экране устройства.

§ 2. Классификация киберпреступлений в международно-правовых документах

В то время как единое определение термина «киберпреступность» пока отсутствует, возникает вопрос: можно ли вместо перечня отдельных киберпреступлений (или в дополнение к нему) в общих чертах определить цели, характеристики или способы совершения таких

[1] Near Field Communication — букв.: коммуникация ближнего поля. Технология беспроводной передачи данных малого радиуса действия.

преступлений? Как отмечалось выше, один пример такого подхода можно обнаружить в названном выше Соглашении Содружества Независимых Государств, где «преступление в сфере компьютерной информации» описывается как «уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация». В Соглашении Шанхайской организации сотрудничества «информационная преступность» определяется (в более широком плане) как «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях». В Конвенции Совета Европы о компьютерных преступлениях применяется классификация деяний по следующим общим группам (хотя их названия не определены как термины): «преступления против конфиденциальности, целостности и доступности компьютерных данных или систем», «правонарушения, связанные с использованием компьютерных средств», и «правонарушения, связанные с содержанием компьютерных данных». В проекте Конвенции Африканского союза также использованы названия посвященных криминализации глав, которые проводят различие между «правонарушениями, характерными исключительно для информационно-коммуникационных технологий» и «адаптацией отдельных правонарушений под информационно-компьютерные технологии».

Данные подходы показывают, что для описания киберпреступлений можно использовать ряд общих характеристик. Например, можно сосредоточить внимание на *объекте* преступления, т. е. на лице, предмете или ценности, против которых совершается преступление. Такой подход прослеживается в Соглашении Содружества Независимых Государств (где объектом преступления выступает компьютерная информация), а также в разд. 1 части 1 Конвенции Совета Европы о компьютерных преступлениях, посвященной материальному уголовному праву (где объектами преступления выступают компьютерные данные или компьютерные системы). Второй подход состоит в определении того, являются ли компьютерные системы или информационные системы неотъемлемой частью *способа совершения преступления*. Данный подход также прослеживается в разд. 2, 3 и 4 части 1 Конвенции Совета Европы о компьютерных преступлениях, посвященной материальному уголовному праву, а также в Соглашении Шанхайской организации сотрудничества.

По нашему мнению, наиболее развернутую классификацию киберпреступлений предлагает *Международный союз электросвязи (МСЭ)*[1]. Приведем ее.

[1] См.: Понимание киберпреступности: явление, задачи и законодательный ответ: отчет МСЭ, 2014 // URL: http://www.itu.int.

Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

Все преступления этой категории направлены против как минимум одного из трех юридических принципов: конфиденциальности, целостности и доступности информации. В отличие от преступлений, которые описывались в уголовном законодательстве на протяжении веков, например кражи или убийства, компьютеризация правонарушений появилась не так давно, поскольку компьютерные системы и компьютерная информация разработаны примерно 60 лет назад. Для эффективного наказания за такие деяния требуется, чтобы существующие положения уголовного права не только защищали от незаконных действий вещественные предметы и физические документы, но и были расширены таким образом, чтобы они включали в себя эти новые юридические принципы. Далее приводятся наиболее часто встречающиеся правонарушения, подпадающие под эту категорию.

Незаконный доступ (хакерство, взлом шифра). Правонарушением, описанным как хакерство, называют незаконный доступ к компьютерной системе. Это одно из старейших преступлений, связанных с применением компьютеров. В соответствии с развитием компьютерных сетей (особенно Интернета) это преступление стало массовым явлением.

Примеры хакерских правонарушений включают в себя взлом защищенных паролями веб-сайтов и обход парольной защиты компьютерной системы. Однако к действиям, понимаемым под термином «хакерство», также относятся подготовительные действия, например использование неисправного оборудования или программных реализаций для незаконного получения пароля для входа в компьютерную систему, создание «подставных» веб-сайтов с целью заставить пользователей раскрыть свои пароли и установка аппаратных и программных методов регистрации нажатий клавиш на клавиатуре (например, «клавиатурный шпион»), которые записывают каждое нажатие клавиш и, следовательно, любые пароли, используемые на компьютере и (или) устройстве.

Мотивация у правонарушителей различна. Некоторые правонарушители ограничивают свои действия обходом мер безопасности только для того, чтобы доказать свои способности. Другие действуют по политическим мотивам, известным как хактивизм. Однако в большинстве случаев мотивация у правонарушителей не ограничивается незаконным доступом к компьютерной системе. Правонарушители используют свой доступ для совершения дальнейших преступлений, таких как информационный шпионаж, манипуляции данными, атаки

типа «отказ в обслуживании» (DoS). В большинстве случаев незаконный доступ к компьютерной системе является только необходимым первым шагом.

Растущее число хакерских атак обусловлено тремя основными причинами:

— неадекватной и неполной защитой компьютерных систем. Сотни миллионов компьютеров присоединены к Интернету, и множество компьютерных систем не имеют адекватной защиты для предотвращения незаконного доступа. Анализ, выполненный Университетом Мэриленда, предполагает, что незащищенная компьютерная система, которая присоединена к Интернету, испытывает на себе атаку менее чем через минуту. Установка мер защиты может снизить риск, но успешные атаки на хорошо защищенные компьютерные системы доказали, что меры технической защиты никогда не смогут полностью остановить атаки;

— разработкой программных инструментов, которые автоматизируют атаки. В последнее время для автоматизации атак применяются программные инструменты. С помощью программ и атак с заранее установленными параметрами за один день, используя один компьютер, один нарушитель может атаковать тысячи компьютерных систем. Если у нарушителя имеется доступ к большему числу компьютеров, например с помощью сетевого робота, он может еще больше увеличить масштаб преступления, поскольку бóльшая часть программных инструментов использует заранее определенные методы атак, не все атаки оказываются успешными. Пользователи, которые регулярно обновляют свои операционные системы и программные приложения, снижают для себя риск стать жертвой таких широкомасштабных атак, поскольку компании, разрабатывающие защитные программы, анализируют инструменты атак и готовятся к стандартным хакерским атакам.

Высокоуровневые атаки часто специально разработаны. Успех таких атак часто обусловлен не применением чрезвычайно сложных методов, а количеством атакуемых компьютерных систем. Инструменты, позволяющие выполнять такие стандартные атаки, широко доступны в Интернете, некоторые из них бесплатны;

— растущей ролью частных компьютеров как цели хакерских атак. Доступ к компьютерной системе часто не является основной мотивацией атаки. Поскольку рабочие компьютеры обычно лучше защищены, чем частные компьютеры, атаки на рабочие компьютеры с использованием заранее сконфигурированных программных инструментов осуществить намного сложнее. Нарушители все больше нацеливают свои атаки на частные компьютеры, поскольку многие частные компьютеры защищены недостаточно. Более того, частные компьютеры часто содержат ценную информацию (например, о кредитной карте или о банковском счете). Правонарушители атакуют частные компьютеры, потому что после успешной атаки правонарушитель может включить этот компьютер в свой сетевой робот и использовать его для последующих преступных действий.

Незаконный доступ к компьютерной системе может считаться аналогичным незаконному доступу в здание и во многих странах признается уголовным преступлением. Анализ различных подходов к судебному преследованию компьютерного доступа показывает, что действующие положения в ряде случаев путают незаконный доступ с последующими правонарушениями или пытаются ограничить судебное преследование незаконного доступа только случаями серьезных нарушений. В некоторых положениях предусмотрено судебное преследование первоначального доступа, а в других уголовным преступлением считаются только те случаи, когда система, к которой получен доступ, защищена средствами безопасности или нарушитель имел вредоносные намерения, или информация была получена, изменена или искажена. Другие законодательные системы не считают преступлением простой доступ, а фокусируются на последующих правонарушениях.

Анализ показывает наличие тенденции к более изощренным и целевым атакам помимо широких и масштабных атак, которые преобладали в прошедших десятилетиях. Широкомасштабные атаки носят авантюрный характер и проводить их проще, а целевые атаки требуют больше усилий от правонарушителя, но вместе с тем являются значительно более эффективными и более вредоносными для жертвы.

Незаконное получение данных (информационный шпионаж). Ценная информация часто хранится в компьютерных системах. Если компьютерная система соединена с Интернетом, правонарушители могут попытаться получить доступ к этой информации через Интернет почти из любой точки мира. Интернет все чаще используется для получения коммерческих секретов. Стоимость ценной информации и возможность получить к ней удаленный доступ делает информационный шпионаж чрезвычайно интересным. В 1980-х гг. несколько немецких хакеров успешно проникли в компьютерные системы правительства и Министерства обороны США, получив секретную информацию и продав эту информацию агентам из другой страны.

Правонарушители используют различные способы для получения доступа к компьютерам своих жертв, включая программы для сканирования незащищенных портов или программы для обхода средств защиты, а также психологическую атаку. Особенно интересен для них последний подход, который является нетехническим видом проникновения и опирается главным образом на взаимодействие между людьми, подразумевает обман других людей с целью разрушения обычных процедур обеспечения безопасности, поскольку он основан

не на технических средствах. В контексте незаконного доступа к данным этот подход понимается как манипуляция людьми с целью получения доступа к компьютерным системам. Психологическая атака обычно очень успешна, потому что самым слабым звеном в компьютерной безопасности часто являются пользователи компьютерных систем. Пример тому — фишинг, который в последнее время стал основным преступлением, совершаемым в киберпространстве.

Хорошо образованные пользователи компьютера не являются легкой добычей для правонарушителей, прибегающих к психологической атаке. Как следствие, образование пользователей должно быть важной частью любой стратегии борьбы с киберпреступностью. Помимо этого, для предотвращения незаконного доступа к данным могут быть приняты технические меры. Организация экономического сотрудничества и развития (ОЭСР) подчеркивает важность криптографии для пользователей, поскольку криптография может помочь улучшить защиту данных. Если физическое лицо или организация, хранящие информацию, применят соответствующие меры защиты, криптографическая защита может оказаться более эффективной, чем любая физическая защита. Успех действий правонарушителей в получении ценной информации часто обусловлен отсутствием мер защиты. Поскольку важная информация все чаще хранится в компьютерных системах, необходимо оценить, адекватны ли технические меры защиты данных, принятые пользователями, и требуется ли дополнительная законодательная защита данных в виде уголовного преследования за информационный шпионаж.

Хотя правонарушители обычно нацеливаются на производственные секреты, все чаще их целью становятся данные, хранимые на частных компьютерах. Частные пользователи часто хранят на своих компьютерах данные о банковских счетах или кредитных картах. Правонарушители могут использовать эту информацию для собственных целей (например, данные о банковских счетах для выполнения денежных переводов) или продать ее третьей стороне. Данные о кредитных картах, например, продаются за сумму от 60 долл. США. Интересна нацеленность хакеров на частные компьютеры, поскольку выгода от полученных промышленных секретов обычно выше, чем выгода от получения или продажи информации об одной кредитной карте. Однако, поскольку частные компьютеры обычно защищены хуже, информационный шпионаж, основанный на частных компьютерах, вероятно, станет еще более прибыльным.

Существует два подхода к получению информации. Правонарушители могут получить доступ к компьютерной системе или хранилищу данных и получить информацию или использовать различные манипуляции для того, чтобы заставить пользователей раскрыть информацию или коды доступа, которые помогут правонарушителям получить доступ к информации — фишинг.

Правонарушители часто используют компьютерные инструменты, установленные на компьютерах жертв, или вредоносные программы, называющиеся шпионскими программами, для передачи данных на них. В течение последних 10 лет обнаружены различные типы шпионских программ, например «клавиатурные шпионы». «Клавиатурные шпионы» — это программные инструменты, которые регистрируют каждое нажатие клавиш на клавиатуре зараженного компьютера. Эти же «клавиатурные шпионы» передают всю записанную информацию правонарушителю, как только компьютер выйдет в Интернет. Другие выполняют первоначальную сортировку и анализ записанных данных, например фокусируясь на потенциальной информации о кредитных картах, для передачи любой полученной ценной информации. Аналогичные устройства представлены также как аппаратные устройства, которые подключаются между клавиатурой и компьютерной системой для записи нажатий клавиш клавиатуры. Аппаратные «клавиатурные шпионы» намного сложнее установить и обнаружить, поскольку требуется физический доступ к компьютерной системе. Однако классические антишпионские и антивирусные программы, как правило, не способны их обнаружить.

Помимо доступа к компьютерным системам правонарушители могут также получать данные путем манипулирования пользователями. В последнее время правонарушители разработали эффективные методы обмана для получения секретной информации, например данных о банковском счете или кредитной карте, путем управления пользователем при помощи методов психологической атаки. В последнее время фишинг стал одним из наиболее значительных преступлений в киберпространстве. Термин *фишинг* (англ.: fishing — рыбная ловля) используется для описания таких преступлений, которые характеризуются попытками мошеннического получения ценной информации, например паролей, когда мошенник выдает себя за доверенное лицо или предприятие (например, финансовую организацию) в процессе электронной переписки, которая выглядит как официальная.

Разработки вроде больших данных, когда компании собирают крупные массивы информации с целью проведения сложного анализа, изменили значимость утечек в общей структуре угрозы. Если правонарушители получают доступ к крупным базам с личными данными клиентов, простая утечка может стоить пострадавшей компании значительных денег даже в том случае, если преступник не использует полученные данные для других правонарушений.

Незаконный перехват. Правонарушители могут перехватывать переписку между пользователями, например электронные письма или

другие формы передачи данных (когда пользователи загружают данные на веб-серверы или заходят на внешние средства хранения на базе веб-технологии), для записи передаваемой информации. В связи с этим правонарушители, как правило, могут иметь своей целью любую инфраструктуру связи, например фиксированные или беспроводные каналы, и любые услуги Интернета (электронную почту, чаты или связь VoIP[1]).

Большинство процессов передачи данных через инфраструктуру поставщиков доступа в Интернет или поставщиков услуг Интернета хорошо защищены, их трудно перехватить. Однако правонарушители ищут слабые точки в системе. Беспроводные технологии приобрели большую популярность и в прошлом показали свою уязвимость. Сегодня отели, рестораны и бары предлагают своим клиентам доступ в Интернет через беспроводные точки доступа. Однако сигналы передачи данных между компьютером и точкой доступа могут быть приняты в радиусе до 100 м. Правонарушители, желающие перехватить процесс обмена данными, могут сделать это из любой точки в пределах этого радиуса. Даже в том случае, когда беспроводная передача зашифрована, правонарушители могут иметь возможность дешифровать записанную информацию.

Для получения доступа к ценной информации некоторые правонарушители устанавливают точки доступа вблизи мест, где имеется большой спрос на беспроводной доступ (например, вблизи баров и гостиниц). Местоположение станции часто имеет такое название, чтобы пользователи, ищущие точку доступа в Интернет, с большей вероятностью остановили свой выбор на мошеннической точке доступа. Если пользователи доверяют поставщику услуг доступа в деле обеспечения безопасности своей связи без применения собственных мер безопасности, то правонарушители смогут легко перехватить передачу.

Использование фиксированных линий не мешает правонарушителям перехватывать передачи. Во время передачи данных по проводам излучается электромагнитная энергия. Если правонарушители используют соответствующее оборудование, они могут обнаружить и записать эти передачи и смогут записать передачу данных между компьютерами пользователей и системой, к которой они присоединены, а также внутри компьютерной системы.

Большинство стран защищает услуги связи путем судебного преследования незаконного перехвата телефонных переговоров. Однако, учитывая растущую популярность услуг на базе IP-протокола, законодателям необходимо оценить, до какой степени аналогичная защита может быть обеспечена в услугах на базе IP-протокола.

[1] Voice over Internet Protocol, или IP-телефония, — голосовая связь через Интернет.

Искажение информации. Компьютерная информация жизненно важна для частных пользователей, предприятий и администраций, все они зависят от целостности и доступности данных. Отсутствие доступа к данным может привести к существенным финансовым потерям. Правонарушители могут нарушить целостность данных и исказить их путем удаления, блокировки или изменения компьютерных данных. Одним из распространенных примеров удаления данных является компьютерный вирус. С самого начала развития компьютерных технологий компьютерные вирусы угрожали пользователям, не установившим соответствующую защиту. С тех пор количество компьютерных вирусов значительно увеличилось. Помимо роста количества вирусных атак изменились также алгоритмы и функции вирусов (загружаемые данные).

Ранее компьютерные вирусы распространялись через устройства хранения данных, такие как гибкие диски, тогда как теперь бóльшая часть вирусов распространяется через Интернет в виде приложений либо к электронным письмам, либо к файлам, загружаемым пользователями. Эти новые эффективные методы распространения намного усилили вирусное заражение и существенно повысили число зараженных компьютерных систем.

Большинство компьютерных вирусов первого поколения либо удаляли информацию, либо отображали сообщение. В последнее время загружаемые данные стали разнообразными. Современные вирусы способны устанавливать потайные входы, позволяющие правонарушителям дистанционно управлять компьютером жертвы или шифровать файлы так, чтобы жертвы не могли получить доступ к собственным файлам, пока они не заплатят за ключ.

Искажения системы. Вопросы, вызывающие озабоченность в связи с атаками на компьютерные данные, относятся и к атакам на компьютерные системы. Большинство организаций используют интернет-услуги в процессе производства, что позволяет иметь готовность 24 часа в сутки и доступность по всему миру. Если правонарушители сумеют нарушить беспрерывность работы компьютерных систем, это может привести к большим финансовым потерям у их жертв.

Атаки могут выполняться путем физического нападения на компьютерную систему. Если нарушители сумеют получить доступ к компьютерной системе, они смогут разрушить аппаратуру. В большинстве уголовных законодательств дела о дистанционном воздействии не являются существенной проблемой, так как они аналогичны классическим делам о повреждении или разрушении собственности. Однако для высокодоходных предприятий электронной коммерции финансовый урон, наносимый атаками на компьютерную систему, часто намного выше, чем просто стоимость компьютерного оборудования.

Наиболее сложными для законодательства являются обманы на базе веб-технологий. Среди примеров таких дистанционных атак на компьютерные системы — компьютерные «черви» (самовоспроизводящиеся вредоносные программы) и атаки типа «отказ в обслуживании» (DoS — Denial of Service).

Компьютерные «черви» являются подгруппой вредоносных программ (типа компьютерных вирусов). Это самовоспроизводящиеся компьютерные программы, которые наносят вред сети, инициируя множество процессов передачи данных. Они могут влиять на компьютерные системы путем затруднения беспрерывной работы компьютерной системы, используя ресурсы системы для самовоспроизведения в Интернете, или путем создания трафика в сети, который может закрыть доступность определенных услуг, например веб-сайтов.

В то время как компьютерные «черви», как правило, заражают всю сеть, не имея целью определенные компьютерные системы, атаки DoS нацелены на конкретные компьютерные системы. Атака DoS делает ресурсы компьютера недоступными для легальных пользователей. Направляя на некую компьютерную систему большее число запросов, чем эта компьютерная система способна обслужить, правонарушители могут не дать пользователям возможности получить доступ к компьютерной системе, проверить электронную почту, прочесть новости, заказать авиабилет или загрузить файлы.

Определение наказания за атаки DoS и атаки с использованием компьютерных «червей» — сложная задача для большей части уголовных правовых систем, поскольку эти атаки могут не приводить к физическому повреждению компьютерных систем. Помимо обычной необходимости судебного преследования атак на базе веб-технологий обсуждается вопрос о том, требуется ли отдельный законодательный подход к наказанию за атаки на важнейшую инфраструктуру.

Несмотря на развитие профилактических технических средств и стратегий смягчения рисков, атаки типа «отказ в обслуживании» остаются серьезной проблемой для компаний и государственных учреждений. Согласно некоторым исследованиям угроза таких атак и связанные с ними затраты растут.

Преступления, связанные с контентом

К этой категории относится контент, который считается незаконным, включая детскую порнографию, ксенофобские материалы или оскорбления в адрес религиозных символов. Разработка правовых инструментов для борьбы с этой категорией преступлений испытывает более сильное влияние со стороны национальных подходов, которые могут учитывать фундаментальные культурные и правовые принципы. В том, что касается запрещенного контента, системы оценки и законодательные системы в различных обществах существенно различаются. Распространение ксенофобских материалов является незаконным во многих европейских странах, но может защищаться принципами свободы слова в Соединенных Штатах. Использование пренебрежительных замечаний в адрес пророка Мухаммеда является преступлением во многих арабских странах, но не является таковым в некоторых европейских странах. Юридические попытки ввести уголовную ответственность за противозаконный контент не должны нарушать право на свободу выражения мнений.

Там, где существует соглашение, запрещающее доступ к веб-сайтам с запрещенным содержанием, размещенным за пределами страны, государства могут иметь строгие законы, блокировать веб-сайты и фильтровать контент.

Существуют различные подходы к созданию *систем фильтрации*. Согласно одному из решений требуется, чтобы поставщики устанавливали программы, анализирующие посещаемые веб-сайты, и блокировали веб-сайты, занося их в «черный список». Другим решением является установка фильтрующих программ на компьютеры пользователей (удобное решение для родителей, желающих контролировать содержание, которое могут видеть их дети, а также для библиотек и интернет-терминалов общего пользования).

Попытки контролировать контент в Интернете не ограничиваются определенными типами контента, которые считаются незаконными. В некоторых странах технологию фильтрации используют для ограничения доступа на веб-сайты, где рассматриваются политические вопросы.

Назовем далее основные на сегодняшний день преступления, связанные с контентом.

Эротические или порнографические материалы (за исключением детской порнографии). Материалы сексуального содержания были одними из первых видов контента, который стал коммерчески распространяться по Интернету и который был выгоден для розничных торговцев материалами эротического или порнографического содержания, включая:

— передачу содержания (картинок, фильмов, прямых репортажей) без необходимости использовать дорогостоящие методы доставки;

— всемирный доступ, достигающий намного большего числа потребителей, чем магазины розничной продажи.

Интернет часто считается анонимной средой передачи, что является ошибочным, — это аспект, который в силу доминирующих взглядов общества очень привлекателен для потребителей порнографии.

В различных странах материалы эротического и порнографического содержания считаются незаконными до различной степени.

В некоторых странах разрешен обмен порнографическими материалами между взрослыми, и преступлением считаются случаи, когда доступ к материалам такого типа получают дети. Таким образом в этих странах стремятся защитить молодежь. Исследования показывают, что доступ детей к порнографическим материалам может негативно сказаться на их развитии. Для того чтобы обеспечить выполнение этого закона, были разработаны системы «подтверждение взрослости». В других странах преступлением считается любой обмен порнографическими материалами даже между взрослыми, без специального внимания к отдельным группам населения, например молодежи.

Детская порнография. Интернет стал основным способом распространения детской порнографии. В 1970-е и 1980-е гг. правонарушители, занимающиеся обменом материалами с детской порнографией, столкнулись с серьезной угрозой. В это время рынок коммерческой детской порнографии был сосредоточен в основном в Европе и США, и материал был местного производства, дорогой и малодоступный. Способы покупки или продажи детской порнографии предполагали некоторые риски, которые больше или по крайней мере в значительной степени не существуют на сегодняшний день. В прошлом производители не имели возможности проявлять фотографии и пленки. Они зависели от услуг коммерческих компаний, что увеличивало шансы обнаружения детской порнографии правоохранительными органами через отчеты, которые предоставляли компании, занимающиеся проявкой. Доступность видеокамер впервые изменила данную ситуацию. Но риски были связаны не только с производством материала. Получение доступа к детской порнографии было также сопряжено с рисками для правонарушителя. Заказы размещались посредством ответа на объявления в газетах. Средства общения между продавцом и собирателем, а значит, и с самим рынком, были ограничены. До середины 1990-х гг. материалы с детской порнографией доставлялись преимущественно по почте, и успешные расследования привели к поимке значительного числа преступников.

Ситуация резко изменилась с появлением приложений для обмена данными через Интернет. В то время как раньше правоохранительные органы имели дело с аналоговым материалом, сегодня большинство обнаруженного материала представлено в цифровом формате. С середины 1990-х гг. преступники стали широко использовать сетевые услуги с целью распространения порнографии. Возникшие в результате этого проблемы в плане обнаружения и расследования случаев детской порнографии были приняты во внимание. Сегодня Интернет — это основной способ торговли обычной, а также детской порнографией.

В отличие от различных взглядов на взрослую порнографию детская порнография повсеместно преследуется, и правонарушения, связанные с детской порнографией, считаются преступными деяниями. В борьбе против онлайновой детской порнографии участвуют международные организации (Интерпол, Европол и др.), существует несколько международных правовых инициатив, включая, помимо прочего, Конвенцию ООН о правах ребенка 1989 г., Рамочное решение Совета Европейского Союза 2003 г. по борьбе с сексуальной эксплуатацией детей и детской порнографией и Конвенцию Совета Европы 2007 г. о защите детей от сексуальной эксплуатации и сексуального насилия.

Два главных фактора использования ИКТ для передачи материалов с детской порнографией представляют трудности для расследования этих преступлений:

— *использование виртуальных денег и анонимные платежи.* Оплата наличными позволяет покупателям некоторых товаров скрыть свои данные. Поэтому во многих преступных делах используются преимущественно наличные деньги. Спрос на анонимные платежи привел к разработке систем виртуальной оплаты и виртуальных денег, обеспечивающих анонимные платежи. Виртуальные деньги могут не требовать ни идентификации, ни подтверждения, что мешает органам правопорядка отследить денежные потоки в направлении к правонарушителям. В последнее время многие расследования детской порнографии были успешными в обнаружении правонарушителей за счет использования следов, оставленных платежами. Однако там, где правонарушители осуществляют анонимные платежи, отследить правонарушителей очень трудно. При использовании преступниками таких анонимных денег правоохранительные органы имеют ограниченные возможности по выявлению подозреваемых путем отслеживания денежных переводов, например в случаях, связанных с коммерческой детской порнографией;

— *использование технологии шифрования.* Нарушители все чаще шифруют свои сообщения. Органы правопорядка отмечают, что правонарушители используют технологии шифрования для защиты информации, хранящейся на их жестких дисках, что серьезно мешает расследованию преступлений.

В дополнение к широкому судебному преследованию деяний, связанных с детской порнографией, в настоящее время обсуждаются другие подходы, например наложение на поставщика услуг доступа в Интернет обязательств по регистрации пользователей или по блокировке или фильтрации доступа на веб-сайты, связанные с детской порнографией.

Расизм, агрессивные высказывания, восхваление жестокости. Радикальные группы используют средства массовой информации, например Интернет, для распространения пропагандистских материалов. Количество веб-сайтов, предлагающих расистский контент и агрессивные высказывания, в последние годы увеличилось.

Распространение по Интернету дает правонарушителям несколько преимуществ, включая малую стоимость распространения, отсутствие специального оборудования и глобальную аудиторию. Среди примеров веб-сайтов, подстрекающих к насилию, — веб-сайты, содержащие инструкции по созданию бомб. Помимо пропаганды Интернет используется для продажи определенных товаров (например, нацистские предметы, такие как флаги с нацистской символикой, униформа и книги, свободно доступны на аукционных площадках и в специализированных веб-магазинах). Кроме того, Интернет используется для отправки электронных писем и новостных рассылок, а также для распространения видеоклипов и телевизионных программ с использованием популярных архивов, например YouTube.

Не во всех странах такие правонарушения преследуются по закону. В некоторых странах такой контент может охраняться принципами свободы слова. Мнения о том, до какой степени к определенным темам применимы принципы свобода слова, различны и часто препятствуют международным расследованиям.

Религиозные преступления. Растущее число веб-сайтов предоставляют материал, который в некоторых странах подпадает под положения, связанные с религиозными преступлениями (например, письменные антирелигиозные призывы). Хотя в некоторых материалах документируются объективные факты и тенденции, например уменьшение посещения церкви в Европе, эта информация в некоторых юрисдикциях может считаться незаконной. Среди других примеров — диффамация религии или публикация комиксов.

Различие законодательных стандартов по запрещенному содержанию отражает проблемы регулирования контента. Даже там, где публикация контента охватывается положениями, касающимися свободы слова, в стране, где этот контент доступен, доступ к этому материалу может быть получен из стран с более строгими законами. «Диспут о комиксах» 2005 г. показал потенциал конфликта. Публикация 12 комиксов в датской газете Jyllands-Posten привела к широким протестам в мусульманском мире[1].

Что касается запрещенного содержания, то в ряде стран доступность определенной информации или материалов является уголовным преступлением. Защита различных религий или религиозной символики различна в различных странах. В некоторых странах считается преступлением использование агрессивных высказываний в адрес пророка Мухаммеда или осквернение книг священного Корана, тогда как в других странах может быть принят более либеральный подход и такие деяния могут не преследоваться в судебном порядке.

[1] Публикация карикатур на пророка Мухаммеда во французской газете Sharli привела к расстрелу членов редакции в 2015 г.

Незаконные азартные игры и онлайновые игры. Интернет-игры и азартные игры — это одна из наиболее быстро растущих областей в Интернете. Отчеты показывают, что некоторые такие игры используются для совершения преступлений, включая передачу и воспроизведение детской порнографии, мошенничество, азартные игры в виртуальных онлайновых казино и клевету, например написание оскорбительных или клеветнических сообщений.

Рост доходов от онлайновых азартных игр в Интернете прогнозировался от 3,1 млрд долл. США в 2001 г. до 24 млрд долл. США в 2010 г.[1]

Интернет позволяет людям обходить ограничения на азартные игры. Онлайновые казино широко доступны, бóльшая их часть располагается в странах с либеральными законами или отсутствием законов об азартных играх в Интернете. Пользователи могут открывать свои счета в онлайновом режиме, пересылать деньги и играть в азартные игры. Онлайновые казино также могут использоваться для отмывания денег и в действиях по финансированию терроризма. Если правонарушители используют онлайновые казино на этапе пересылки денег, при которой не ведется записей, или они находятся в странах, где отсутствует законодательство против отмывания денег, то органам правопорядка очень трудно определить источники финансирования.

Клевета и фальшивая информация. Веб-сайты могут содержать фальшивую или клеветническую информацию, особенно на форумах или в «комнатах» чата, где пользователи могут оставлять сообщения без проверки их модераторами. Молодые люди все чаще используют веб-форумы и социальные сети, где такая информация также может быть размещена. Преступная деятельность может включать в себя, например, публикацию интимных фотографий или ложной информации о сексуальном поведении.

В большинстве случаев правонарушители пользуются преимуществами того факта, что поставщики, разрешающие дешевую или бесплатную публикацию, как правило, не требуют идентификации авторов или могут не проверять ID[2]. Это усложняет идентификацию правонарушителей. Более того, модераторы форума могут не регулировать или

[1] В 2015 г. доход в этой сфере составил в мире 37—41 млрд долл. США.

[2] Уникальный идентификатор, последовательность символов в адресной строке, характеризующая тот или иной компьютер, пользователя.

очень мало регулировать контент. Эти преимущества не препятствуют разработке ценных проектов, таких как Wikipedia — онлайновая энциклопедия, создаваемая пользователями, где существуют строгие процедуры регулирования содержания. Однако правонарушители могут использовать те же самые технологии для публикации ложной информации (например, о конкурентах) или раскрытия секретной информации (например, публикация государственных секретов или ценной коммерческой информации).

В тот момент, когда информация опубликована в Интернете, ее автор часто теряет контроль над этой информацией. Даже если эта информация корректируется или удаляется сразу после публикации, она уже может быть скопирована («зеркальная копия») и сделана доступной людям, которые не пожелают ее аннулировать или удалить. В таком случае эта информация может оставаться доступной в Интернете, даже если она была удалена или исправлена на первоначальном источнике. Примеры включают в себя случаи «электронных писем, отправленных не по тому адресу», в которых миллионы людей могут получить непристойные, вводящие в заблуждение или ложные электронные письма о людях или организациях, когда репутация может никогда не быть восстановлена, вне зависимости от того, является ли это письмо правдой или нет. Следовательно, необходимо сбалансировать свободу слова и защиту потенциальных жертв клеветы.

Спам и связанные с ним угрозы. Спам означает передачу незапрашиваемых сообщений. Несмотря на то что существуют различные способы обмана, наиболее широко используемым является спам в электронных письмах. Правонарушители рассылают пользователям миллионы электронных писем, которые часто содержат рекламу продуктов и услуг, но также часто и вредоносные программы. С тех пор как в 1978 г. было отправлено первое спамовое электронное письмо, поток спама в электронной почте значительно вырос. Сегодня поставщики услуг электронной почты сообщают, что от 85 до 90% всей электронной почты — спам.

Бóльшая часть поставщиков услуг электронной почты реагируют на растущие уровни спама в электронной почте путем установки антиспамовых технологий. Эти технологии идентифицируют спам с помощью фильтрации по ключевым словам или ведения «черных списков» IP-адресов спаммеров. Несмотря на то что технология фильтрации продолжает развиваться, спаммеры находят пути обхода этих систем, например избегая использования ключевых слов.

Успех в обнаружении спама в электронной почте зависит от изменений способов распространения спама. Вместо передачи сообщений с одного почтового сервера, что технически легче определяется поставщиками услуг электронной почты из-за ограниченного числа источников, многие правонарушители для распространения незапрошенных электронных писем пользуются сетевыми роботами. При использовании сетевых роботов, созданных из тысяч компьютерных систем, каждый компьютер может передавать только несколько сотен электронных писем. Это усложняет работу поставщиков услуг электронной почты по идентификации спама путем анализа информации об отправителях и усложняет органам правопорядка задачу по отслеживанию правонарушителей.

Вымогательство. Вымогательство не относится к разряду типичных киберпреступлений, а считается обычным правонарушением. Тем не менее в результате применения ИКТ появились атаки, которые часто называют кибервымогательством. За последние годы таким атакам подверглись как крупные компании, так и мелкие стартапы. Правонарушители все чаще прибегают к преимуществам, ставшим возможными благодаря использованию ИКТ, в отличие от традиционных способов совершения преступлений. Помимо технологий анонимной связи, применяемых с целью совершения преступлений, все большее количество правонарушителей прибегают к использованию виртуальных денег вместо банковских переводов наличных средств. По результатам исследования компании все еще недооценивают угрозу вымогательства.

Более автоматизированной формой вымогательства являются так называемые программы, требующие выкупа, — зловредные программы, инфицирующие компьютерную систему, блокирующие ее и выводящие на дисплей сообщение о том, что система будет разблокирована только после уплаты жертвой выкупа. Для большей убедительности преступники часто заявляют, что компьютер якобы был отключен правоохранительными органами из-за незаконной деятельности его пользователя.

Другие формы незаконного контента. Интернет используется не только для прямых атак, но и как площадка для подстрекательства, предложений и побуждения к совершению преступлений, незаконной продажи продуктов и предоставления информации и инструкций для незаконных действий, например по изготовлению взрывчатки.

Во многих странах приняты законы о торговле определенными продуктами. В различных странах применяются различные национальные законы и ограничения по торговле различными продуктами, например военным оборудованием. Аналогичная ситуация существует для лекарств: лекарства, которые продаются без ограничений в некоторых странах, в других могут отпускаться только по рецептам. Трансграничная торговля может нарушить порядок, при котором на определенной территории ограничен доступ к определенным продуктам. С учетом популярности Интернета эта проблема растет. Веб-ма-

газины, работающие в странах без ограничений, могут продавать продукты потребителям в других странах, где действуют запреты.

До появления Интернета большинству людей было сложно получить инструкции по созданию оружия. Необходимая информация была доступна, например, в книгах, рассматривающих химию взрывчатых веществ, но для того чтобы ее найти, требовалось время. Сегодня информация о том, как сделать взрывчатку, доступна в Интернете, и простота доступа к этой информации повышает вероятность атак.

Преступления, связанные с правами собственности и товарными знаками

Одной из главнейших функций Интернета является распространение информации. Компании используют Интернет для распространения информации о своих продуктах и услугах. Если говорить о пиратстве, то успешные компании могут столкнуться в Интернете с проблемами, сравнимыми с теми, которые существуют вне Сети. Престиж их марки и фирменный дизайн могут использоваться для сбыта поддельных продуктов, когда производители контрафакта копируют как логотипы, так и сами продукты и пытаются зарегистрировать домен, связанный с этой определенной компанией. Компании, распространяющие продукцию напрямую через Интернет, могут столкнуться с правовыми проблемами, связанными с нарушениями авторских прав. Их продукция может быть загружена, скопирована и распространена.

Преступления, связанные с авторскими правами. С переходом с аналоговых форматов на цифровые оцифровка позволила индустрии развлечений добавлять к фильмам на DVD (цифровых видеодисках) дополнительные функции и услуги, включая языки, субтитры, трейлеры и бонусный материал. Компакт-диски и DVD-диски доказали бóльшую жизнеспособность, чем аудио- и видеокассеты.

Оцифровка открыла новый способ нарушений авторских прав. Основой существующих нарушений авторских прав является быстрое и точное воспроизведение. До оцифровки копирование аудио- и видеокассет всегда приводило к некоторому снижению качества. В настоящее время можно скопировать цифровой источник без потери качества, а также в результате делать копии с любой копии. Наиболее часто встречающиеся нарушения авторских прав включают обмен в файлообменных сетях или посредством виртуального хостинга песнями, файлами и программным обеспечением, защищаемыми авторским правом, и обход систем управления цифровыми правами — DRM (Data Recording Device — устройство записи данных).

Файлообменные системы являются сетевыми услугами на основе одноранговых отношений, которые дают возможность пользоваться файлами совместно, часто с миллионами других пользователей. После установки программ для обмена файлами пользователи могут выбрать файлы для совместного использования и использовать программу для поиска файлов, предлагаемых в Сети другими пользователями, для скачивания с сотен источников. До разработки файлообменных систем люди копировали записи и пленки и обменивались ими, но файлообменные системы дают возможность обмениваться копиями гораздо большему числу пользователей.

Технология одноранговых — P2P — взаимоотношений играет в Интернете важную роль. Более 50% потребительского интернет-трафика было создано одноранговыми сетями. Число пользователей постоянно растет. В отчете, опубликованном ОЭСР, утверждается, что примерно 30% пользователей Интернета во Франции загружали музыку или файлы в файлообменных системах, другие страны ОЭСР демонстрируют те же тенденции. Файлообменные системы можно использовать для обмена компьютерными данными любого вида, включая музыку, фильмы и программное обеспечение. Исторически файлообменные системы использовались преимущественно для обмена музыкой, но обмен видеофайлами становится все более значительным.

Технология, используемая в файлообменных услугах, очень сложная и позволяет обмениваться большими файлами за короткий период времени. Файлообменные системы первого поколения зависели от центрального сервера, что позволяло органам охраны правопорядка действовать против незаконного файлообмена в сети Napster. В отличие от систем первого поколения (особенно известной службы Napster) файлообменные системы второго поколения более не размещаются на центральном сервере, представляющем список доступных пользователям файлов. Концепция децентрализации файлообменных сетей второго поколения намного усложнила блокирование их работы. Однако благодаря прямой связи можно отслеживать пользователей Сети по их IP-адресам. Органы охраны правопорядка достаточно успешно расследовали нарушения авторских прав в файлообменных системах. Более новые версии файлообменных систем позволяют создавать анонимные связи и еще более усложняют расследования.

Файлообменная технология используется не только обычными людьми и преступниками, но и обычными компаниями. Не все файлы в файлообменных системах нарушают авторские права. Примеры их правомерного использования включают обмен законными копиями или иллюстрациями на некоммерческой основе.

Тем не менее использование файлообменных систем бросает вызов индустрии развлечений. Непонятно, до какого уровня снизятся

продажи CD-, DVD-дисков и билетов в кинотеатры из-за обмена фильмами в файлообменных сетях. В результате исследования были выявлены миллионы пользователей файлообменных сетей и миллиарды загруженных файлов. Копии фильмов появляются в файлообменных сетях раньше их официального проката в кинотеатрах, что отражается на доходах правообладателей. Недавнее появление анонимных файлообменных систем еще более затрудняет работу как правообладателей, так и органов охраны правопорядка.

Индустрия развлечений ответила внедрением технологий, предназначенных для предотвращения изготовления пользователями копий CD- и DVD-дисков, таких как система защиты от копирования (CSS), в которой технология кодирования мешает копированию содержимого DVD-дисков. Эта технология является важным элементом новых бизнес-моделей, предназначенных для более четкого распределения прав доступа пользователям. Управление цифровыми правами (DRM) означает внедрение технологий, позволяющих правообладателям запрещать использование цифровых носителей, когда пользователи покупают только ограниченные права, например право воспроизведения песни на одной вечеринке. DRM предлагает возможность внедрения новых бизнес-моделей, более точно отражающих интересы правообладателей и пользователей и позволяющих уменьшить снижение прибыли.

Одной из главных проблем данных технологий является то, что технологии защиты авторских прав можно обойти. Злоумышленники разработали программные инструменты, дающие возможность пользователям делать файлы с защитой от копирования доступными в Интернете бесплатно или по небольшой стоимости. Как только с файла снята защита DRM, его можно копировать и воспроизводить без ограничений.

Попытки защитить содержимое не ограничиваются песнями и фильмами. Некоторые телестанции, особенно платные телеканалы, кодируют программы для гарантии того, что программу смогут получать только абоненты, заплатившие за это. Хотя технологии защиты очень сложны, злоумышленники успешно подделывают аппаратные средства, используемые для получения контроля или взлома кодирования при помощи программных инструментов.

Маловероятно, что обычные пользователи смогут совершать подобные преступления, не имея программных инструментов. Судебные разбирательства о нарушении авторских прав касаются не только файлообменных сетей и обхода технической защиты, но и создания, продажи и обладания «нелегальными устройствами» или инструментами, предназначенными для предоставления пользователям возможности совершать нарушения авторских прав.

Преступления, связанные с товарными знаками. Такие преступления — хорошо известный аспект международной торговли, они похожи на нарушения авторских прав. Преступления, связанные с товарными знаками, перешли в киберпространство, и в уголовном праве разных стран они преследуются по закону. Наиболее тяжкие преступления включают в себя использование товарных знаков в совершении преступлений с целью введения пользователей в заблуждение и преступления, связанные с доменами или именами.

Доброе имя компании часто напрямую связано с ее товарными знаками. Злоумышленники используют фирменные и товарные знаки обманным путем для некоторых действий, включая фишинг, когда пользователям Интернета отправляются миллионы электронных писем, аналогичных электронным письмам от законных компаний, например включая товарные знаки.

Другим вопросом, относящимся к преступлениям с товарными знаками, являются преступления, связанные с доменами, например киберсквоттинг, который представляет собой процесс незаконной регистрации доменных имен, идентичных или похожих на товарные знаки продукции или компании. В большинстве случаев злоумышленник стремится продать домен по высокой цене компании или использовать его для продажи продукции или услуг, вводя пользователей в заблуждение при помощи их предполагаемого отношения к данному товарному знаку. Другим примером преступления, связанного с доменом, является «угон домена» или регистрация доменных имен, которые были случайно утеряны.

Преступления, связанные с применением компьютеров

В эту категорию входят некоторые преступления, для совершения которых требуется компьютерная система: мошенничество, связанное с применением компьютеров, подлог, связанный с применением компьютеров, фишинг и кража личных данных, а также неправомерное использование устройств.

Мошенничество и компьютерное мошенничество. Это одно из самых распространенных преступлений в Интернете, так как позволяет правонарушителю применять для сокрытия своей личной информации автоматизацию и программные инструменты.

Автоматизация позволяет злоумышленникам получать большие преимущества при условии выполнения нескольких небольших действий. Одной из стратегий, используемых злоумышленниками, является уверенность в том, что финансовые потери каждой жертвы ниже определенного уровня. При небольших потерях жертвы с меньшей

вероятностью будут тратить время и энергию для заявления о таких преступлениях и их расследования.

Хотя эти преступления совершаются с помощью компьютерных технологий, большинство систем уголовного права рассматривают их не как преступления, связанные с применением компьютеров, а как обычное мошенничество. Основным различием между мошенничеством, связанным с применением компьютеров, и обычным мошенничеством является жертва мошенничества. Если злоумышленники пытаются повлиять на человека, преступление обычно классифицируется как мошенничество. Если целью злоумышленников являются компьютерные системы или системы по обработке данных, то преступления нередко классифицируются как мошенничество, связанное с применением компьютеров. Те системы уголовного права, которые охватывают мошенничество, но пока не включают в себя махинации с компьютерными системами в мошеннических целях, часто все-таки могут предусматривать уголовное наказание за вышеупомянутые преступления. К наиболее распространенным мошенническим правонарушениям относятся следующие.

Мошенничество с онлайновыми аукционами. Онлайновые аукционы в настоящее время являются одними из самых популярных услуг электронной коммерции. Покупатели могут получить доступ к разным товарам или товарам определенной категории из любой точки мира. Продавцы получают предложения со всего мира, благодаря чему стимулируются спрос и повышение цен.

Злоумышленники, совершающие преступления на аукционных площадках, могут использовать отсутствие личного контакта между продавцом и покупателем. Трудность, связанная с нахождением различия между настоящим пользователем и злоумышленником, привела к тому, что мошенничество с аукционами стало одним из самых популярных видов киберпреступлений. К двум самым распространенным методам относятся выставление на продажу несуществующих товаров и требований авансовой оплаты покупки до ее доставки, а также покупка товаров и просьба доставить без намерения оплатить.

В ответ поставщики услуг аукционов разработали системы защиты, например систему отзывов/комментариев. После каждой сделки покупатели и продавцы оставляют отзывы для других пользователей в качестве нейтральной информации о надежности продавца/покупателя. В таком случае «репутация — это все», и без достаточного количества положительных комментариев злоумышленникам трудно принудить жертвы либо к оплате несуществующих товаров, либо, наоборот, к отправке товара без предварительной его оплаты. Однако преступники обошли эту защиту посредством использования счетов третьих лиц. В такой афере, называемой «захват счета», злоумышленники пытаются завладеть именами пользователей и паролями законных пользователей для осуществления мошеннической покупки или продажи, что усложняет их идентификацию.

Мошенничество с предоплатой. В мошенничестве с предоплатой злоумышленники отправляют электронные письма адресату с просьбой о помощи в переводе больших сумм денег третьим лицам и обещанием процента за согласие произвести перевод через свой личный счет. Затем злоумышленники просят перевести небольшую сумму денег для подтверждения данных о его банковском счете, основываясь на поведении людей при участии в лотерее, — респонденты могут пожелать понести небольшие, но определенные затраты в обмен на бóльшую, но неопределенную выгоду, или просто просят выслать данные о банковском счете. Как только жертва переведет деньги, она больше никогда вновь не услышит о злоумышленнике. Если будет передана информация о банковском счете, злоумышленники могут использовать эту информацию для мошеннической деятельности.

Подлог, связанный с применением компьютеров. Это преступление касается махинаций с цифровыми документами. Оно совершается путем создания документа, который, как кажется, исходит от надежной организации; подделки электронных изображений, например изображений, используемых в качестве доказательств в суде, или путем изменения текстовых документов.

Фальсификация электронных писем является неотъемлемым элементом фишинга, сложной проблемой для правоохранительных органов по всему миру. Используя фишинг, злоумышленники стремятся заставить свою жертву раскрыть личную/секретную информацию. Часто они отправляют электронные сообщения, которые выглядят как сообщения от законных финансовых учреждений, используемых жертвой. Электронные письма создаются так, что жертве трудно определить, что это ложное электронное сообщение. В электронном письме получателя просят раскрыть и (или) подтвердить определенную конфиденциальную информацию. Многие жертвы следуют совету и раскрывают информацию, позволяя злоумышленникам делать онлайновые переводы и проч.

В прошлом уголовные преступления, включающие подлог, связанный с применением компьютеров, были редкостью, так как большинство юридически значимых документов были материальными. Цифровые документы играют все более важную роль и используются все чаще. Замена классических документов цифровыми поддерживается законными средствами, например путем законного подтверждения цифровой подписи.

Преступники всегда старались подделывать документы. Цифровые документы теперь можно копировать без потери качества, причем

легко их подделывать. Судебным экспертам трудно доказать цифровые махинации, если не используются технические средства защиты для защиты документов от подделки.

Кража идентичности. Под понятием кражи идентичности, которое не имеет четкого определения и четкого использования, подразумевается преступное деяние по мошенническому получению и использованию идентичности личности. Эти действия могут осуществляться без помощи технических средств, а также с использованием интернет-технологий.

Активное освещение в СМИ, результаты различных исследований, анализирующих масштабы распространения и размеры ущерба, причиняемого кражей идентичности, а также данные многочисленных правовых и технических экспертиз, опубликованные в последние годы, могут привести к заключению о том, что преступления против идентичности являются феноменом, возникшим в XXI в. Однако такое мнение ошибочно, так как правонарушения, связанные с персонацией и фальсификацией или неправомерным использованием документов, удостоверяющих личность, существуют уже более столетия. Еще в 1980-е гг. в прессе неоднократно появлялись сообщения о ненадлежащем использовании личных данных. Появление понятия «цифровая идентичность» и активное применение информационных технологий лишь изменили методы и цели преступников. Интенсивное использование цифровой информации открыло новые возможности для получения правонарушителями доступа к личным данным. Таким образом, процесс перехода от индустриализированного общества к информационному оказал большое влияние на развитие правонарушений, связанных с кражей идентичности.

Тем не менее, несмотря на значительное количество случаев кражи личных данных посредством сети Интернет, цифровые технологии не привнесли качественных изменений в само преступление, а лишь предложили новые цели и способствовали применению преступниками новых методов. Роль воздействия интернет-технологий представляется преувеличенной. Методический анализ преступлений против личных сведений показал, что кража идентичности нередко совершается не в режиме онлайн. Несмотря на последние разработки, проблема офлайновой кражи идентичности остается крайне острой. Интересно, что доля офлайновых преступлений по-прежнему велика, несмотря на то, что интенсивное применение цифровых технологий и глобализация сферы сетевых услуг привели к активному использованию цифровых личных данных.

Важность личных данных для экономики и социального взаимодействия чрезвычайно высока. В прошлом «доброе имя» и хорошие взаимоотношения играли решающую роль в ведении бизнеса в целом

и совершении отдельных деловых операций. С переходом на электронную торговлю непосредственная личная идентификация стала практически невозможной, и, как следствие, личные данные приобрели особую важность для участников социального и экономического взаимодействия.

Данный процесс, в ходе которого идентичность преобразуется в поддающиеся количественному определению личные данные, можно назвать инструментализацией. Этот процесс наряду с разграничением более философского толкования термина «идентичность» (определяемого как совокупность личных характеристик) и поддающихся исчислению личных данных, определяющих человека, представляет огромную важность. Процесс трансформации важен не только для краж идентичности, осуществляемых посредством сети Интернет, так как его воздействие выходит далеко за пределы компьютерных сетей. В настоящее время требования, предъявляемые к заочным сделкам, такие как доверие и безопасность, являются доминантами для всей экономики в целом, а не только для электронной торговли. Примером может послужить использование карт оплаты с ПИН-кодом (персональным идентификационным номером) для покупки товаров в супермаркете.

В целом преступления, направленные против персональных данных, проходят три различных этапа. На первом этапе преступник добывает информацию об идентичности. Эта часть преступления может, например, осуществляться с помощью вредоносных программ или фишинг-атак. Второй этап характеризуется взаимодействием с информацией об идентичности до ее использования при совершении преступлений. Примером может служить продажа информации об идентичности. Информация с кредитной карты, например, стоит более 60 долл. США. Третий этап заключается в использовании информации об идентичности при совершении преступления. В большинстве случаев доступ к данным идентичности толкает преступника к совершению новых преступлений. Поэтому преступники не фокусируются на содержании используемых данных, а используют возможность применить их для совершения преступлений. Примером такого преступления может быть подделка документов, удостоверяющих личность, или мошенничество с кредитными картами.

Способы, применяемые для получения данных в рамках первого этапа, охватывают широкий диапазон действий. Преступники могут использовать физические способы, например красть компьютерные запоминающие устройства, хранящие данные об идентичности, просматривать мусор («копание в мусоре») или воровать почту. Кроме того, они могут использовать поисковые системы для поиска данных об идентичности.

«Googlehacking» или «Googledorks» — термины, описывающие применение сложных поисковых запросов для фильтрации большого количества результатов поиска информации, связанной с вопросами компьютерной безопасности, а также частной информации, которая может быть использована мошенниками при краже идентичности. Одной из целей преступника может быть, например, поиск не защищенных паролем систем для получения данных из этой системы. Отчеты выявляют риски, которые возникают при легальном использовании поисковых систем в незаконных целях. Сходные проблемы касаются и файлообменных систем. Конгресс США недавно обсуждал возможность использования файлообменных систем для получения личной информации, которая может быть использована при краже идентичности. Кроме того, преступники могут использовать сотрудников организаций, которые имеют доступ к хранению информации об идентичности, чтобы завладеть ею.

Проведенное в 2013 г. исследование показало, что 23% электронных преступлений связаны с сотрудниками компаний, а 53% респондентов считают, что внутренние атаки наносят больше вреда, чем внешние. Наконец, преступники могут использовать психологические приемы для того, чтобы убедить жертву раскрыть личную информацию. В последние годы преступники разработали эффективные схемы мошенничества для получения секретной информации, например о банковском счете и данных кредитной карты, управляя пользователями с помощью методов психологического воздействия.

Виды данных, интересующих преступников, меняются. Наиболее важными данными являются:

— *номер социального страхования (SSN) или номер паспорта.* Номер социального страхования, используемый в США, является классическим примером того вида данных об идентичности, который интересует преступников. Несмотря на то что SSN был создан для ведения точного учета дохода, в настоящее время он широко используется для идентификации. Преступники могут использовать SSN или полученные паспортные данные, чтобы открыть финансовые счета, присвоить существующий финансовый счет, взять кредит или скрыться от долгов;

— *дата рождения, адрес и номер телефона.* Эти данные, как правило, могут использоваться для кражи идентичности, если они объединены с другими видами информации, например SSN. Доступ к таким дополнительным данным, как дата рождения и адрес, может помочь преступнику обойти процесс проверки. Одной из наибольших опасностей, связанных с этой информацией, является тот факт, что в настоящее время она общедоступна в Интернете, либо добровольно опубликована на различных форумах, связанных с идентичностью, либо основана на законных требованиях, таких как запись на веб-сайтах;

— *пароль к нефинансовым учетным записям.* Доступ к паролю к учетным записям позволяет преступникам изменить настройки учетной записи и использовать ее в своих целях. Например, они могут взять учетную запись электронной почты и использовать ее для отправки писем с незаконным содержанием или могут взять учетную запись пользователя на аукционе и использовать ее для продажи краденого;

— *пароль к финансовым счетам.* Как и SSN, информация, относящаяся к финансовым счетам, является популярной целью для кражи идентичности. К ней относятся чековые и сберегательные счета, кредитные карты, дебетовые карты и информация о финансовом планировании. Подобная информация является важным источником для кражи идентичности при совершении финансовых киберпреступлений.

Кража идентичности является серьезной и растущей проблемой. В 2012 г. Бюро судебной статистики объявило, что 7% всех жителей США в возрасте 16 лет и старше по крайней мере один раз становились жертвами кражи идентичности. В Великобритании кражи идентичности обходятся британской экономике в 1,3 млрд ф. ст. ежегодно. По оценкам, приведенным в отчете по исследованию мошеннических действий с идентичностью за 2013 г., потери США в 2012 г. составили 20,9 млрд долл. США. Убытки могут быть не только финансовыми, они могут включать ущерб репутации. В действительности многие жертвы не сообщают о таких преступлениях, в то время как финансовые учреждения часто не желают обнародовать печальный опыт клиентов. Фактическое число случаев кражи идентичности, вероятно, намного превышает число зарегистрированных потерь.

Кража идентичности основана на том факте, что имеется несколько способов установить личность пользователей через Интернет. Легче определять людей в реальном мире, но большинство видов онлайновой идентификации являются более сложными. Сложные средства идентификации, например с использованием биометрической информации, являются дорогостоящими и используются не везде. Существуют некоторые ограничения онлайновой деятельности, делающие кражу идентичности легкой и выгодной.

Одним из явлений, тесно связанных с разработками в области больших данных, является растущий объем «черного» рынка информации, имеющей отношение к идентичности. Если правонарушители взламывают базы данных с миллионами записей о клиентах, то значительная часть этой информации в последующем оказывается в продаже. В исследовании, опубликованном в 2014 г., отмечается, что количество связанной с идентичностью информации, предлагаемой на «черном» рынке кибернетического пространства и полученной в ре-

зультате утечки данных, измеряется 360 млн учетных записей, включая составляющие их документы.

Неправомерное использование устройств. Киберпреступление можно совершить при помощи всего лишь простейшего оборудования. Для таких преступлений, как онлайновые клевета или мошенничество, не требуется ничего, кроме компьютера и доступа в Интернет, и они могут совершаться из общественного интернет-кафе. Более сложные преступления могут требовать специальных программных инструментов.

Инструменты, требуемые для совершения комбинированных преступлений, легко доступны через Интернет, часто бесплатно. Более сложные инструменты стоят несколько тысяч долларов. С помощью таких программных инструментов злоумышленники могут атаковать другие компьютерные системы простым нажатием клавиши. Обычные атаки теперь малоэффективны, так как компании, производящие программы защиты, в настоящее время могут отражать простые хакерские атаки и подготовлены для их отражения. Высокоуровневые атаки часто разрабатываются специально для определенных целей. Существуют программные инструменты, с помощью которых правонарушители могут проводить DoS-атаки, создавать компьютерные вирусы, дешифровывать зашифрованные сообщения или получать незаконный доступ к компьютерным системам.

Второе поколение программных инструментов теперь автоматизировало множество киберафер и позволило злоумышленникам осуществлять множественные атаки за малое время. Программные инструменты также упростили атаки, позволяя совершать киберпреступления менее искушенным пользователям компьютеров. Доступны наборы инструментов для спама, которые позволяют практически каждому рассылать электронные письма со спамом. В настоящее время существуют программные инструменты, которые можно использовать для скачивания и закачивания файлов из файлообменных систем. С большей доступностью специально разработанных программных инструментов число возможных злоумышленников существенно увеличилось. Различные национальные и международные законотворческие инициативы были предприняты в отношении программных инструментов для киберафер, например преследование в судебном порядке за их создание, продажу или обладание.

Комбинированные преступления

Существует несколько терминов, используемых для описания сложных мошеннических действий, сочетающих в себе ряд различных правонарушений. Среди примеров — использование сети Интернет в террористических целях, отмывание денег с использованием компьютерных технологий и фишинга.

Отмывание денег с использованием компьютерных технологий. Для крупных сумм традиционные методы отмывания денег обладают целым рядом преимуществ, но Интернет имеет несколько достоинств. Онлайновые финансовые услуги предлагают возможность очень быстрого выполнения многочисленных финансовых операций по всему миру. Интернет помогает преодолеть зависимость от физических денежных операций. Безналичные переводы заменили переводы наличных денег и стали первым шагом в устранении физической зависимости от денег, но строгие правила выявления подозрительных безналичных переводов вынудили злоумышленников разработать новые методы. Выявление подозрительных сделок в области борьбы с отмыванием денег основано на обязательствах финансовых учреждений, принимающих участие в сделке.

Отмывание денег в целом подразделяется на *три стадии*: размещение, расслоение (разбивка крупных сумм денег на более мелкие) и суммирование.

Для размещения больших объемов наличных средств использование Интернета, возможно, не даст заметных преимуществ. Вместе с тем Интернет особенно востребован правонарушителями на стадии расслоения или маскировки. С этой точки зрения расследования отмывания денег особенно трудны, когда лица, отмывающие деньги, используют для расслоения онлайновые казино.

Регулирование денежных переводов в настоящее время ограничено, и Интернет дает правонарушителям возможность дешево и без налога перевести деньги за границу. Текущие трудности в расследовании методов отмывания денег с использованием Интернета часто обусловлены использованием виртуальной валюты и онлайновых казино.

Одним из ключевых факторов в развитии *виртуальных валют* были микроплатежи, например для загрузки из Сети статей стоимостью 10 центов США или меньше, для которых невозможно использовать кредитную карту. С ростом спроса на микроплатежи были разработаны виртуальные валюты, в том числе виртуальные золотые валюты. Виртуальные золотые валюты являются платежными системами, использующими счета, обеспеченные золотыми депозитами. Пользователи могут открыть электронный золотой счет в онлайновом режиме, часто без регистрации. Некоторые поставщики услуг даже разрешают прямой одноранговый (от лица к лицу) перевод или снятие наличных. Правонарушители могут открыть электронные золотые счета в разных странах и комбинировать их, усложняя использование финансовых инструментов для отмывания денег и финансирования терро-

ризма. Владельцы счетов могут также использовать неточную информацию при регистрации для сокрытия своей идентичности.

Помимо простых виртуальных валют также существуют валюты, в которых виртуальный аспект сочетается с анонимностью. Один из таких примеров — виртуальная валюта *Bitcoin* (биткойн), в которой используется одноранговая технология. Хотя эти системы платежей децентрализованные, т. е. не требуют посредников для гарантии законности операций перед властями, успешные хакерские атаки в 2011 г. доказывают уязвимость/риски подобных децентрализованных виртуальных валют. Если подобные анонимные валюты используются преступниками, это сужает возможности органов охраны правопорядка по выявлению подозреваемых путем отслеживания денежных переводов, например в случаях, связанных с распространением детской порнографии.

В отличие от реального казино для открытия *онлайнового казино* не требуется больших финансовых вложений. Кроме того, положения об онлайновых и реальных казино часто различаются в разных странах. Отследить денежные переводы и доказать, что средства были не выиграны, а отмыты, можно, только если казино хранит записи и предоставляет их органам охраны правопорядка.

Фишинг. Правонарушители разработали методы для получения личной информации от пользователей, начиная от программ-шпионов и заканчивая фишинговыми атаками. Существуют различные типы фишинговых атак, но фишинговые атаки с использованием электронной почты состоят из трех основных этапов. На первом этапе злоумышленники определяют законные предлагающие онлайновые услуги и общающиеся с клиентами в электронном виде компании, которые они могут выбрать для своей цели, например финансовые институты. Правонарушители создают подложные веб-сайты, напоминающие законные сайты, где от жертвы требуется выполнить обычные процедуры входной регистрации, что позволяет правонарушителям получить личную информацию, например номера счетов и онлайновые банковские пароли.

Для того чтобы направить пользователей на подложные сайты, правонарушители отправляют по электронной почте сообщение, напоминающее сообщение электронной почты от законной компании, что часто приводит к нарушениям торговой марки. В фальшивом электронном сообщении адресатов просят войти в систему для обновления или проверки безопасности, иногда путем угроз, например о закрытии счета, если пользователи откажутся сотрудничать. Фальшивое электронное сообщение обычно содержит ссылку, по которой жертва должна перейти на обманный сайт, что дает возможность избежать ввода пользователями правильного адреса своего законного

банка вручную. Правонарушители разработали передовые методы, предотвращающие осознание пользователем того факта, что он находится не на подлинном сайте.

Как только личная информация раскрыта, правонарушители входят в учетные записи жертв и совершают преступления, такие как перевод денежных средств, заявки на паспорта или новые счета и т. д. Рост числа успешных атак доказывает потенциал фишинга. В апреле 2007 г. Антифишинговая рабочая группа (APWG) сообщила о более чем 55 тыс. уникальных фишинг-сайтах. В январе 2014 г. количество выявленных уникальных фишинг-сайтов составило почти 43 тыс. Методы фишинга не ограничиваются только получением паролей для проведения онлайновых банковских операций. Правонарушители могут также запрашивать коды доступа к компьютерам, аукционным площадкам и номера социального страхования, которые являются особенно важными в Соединенных Штатах и могут привести к преступлениям «кража идентичности».

§ 3. Периоды развития киберпреступности

Международный союз электросвязи в исследовании 2014 г. предлагает рассматривать следующие этапы.

В *1960-е гг.* появление транзисторных компьютерных систем, которые были меньше по размеру и дешевле по сравнению с ламповыми вычислительными машинами, привело к более широкому использованию компьютерных технологий. На этом раннем этапе правонарушения сводились к физическому повреждению компьютерных систем и накопленных данных. О подобных случаях сообщалось, например, в Канаде, где в 1969 г. студенческие беспорядки привели к пожару, в результате которого были уничтожены данные, хранившиеся в университете. В середине 1960-х гг. в США начались дебаты по поводу создания центрального учреждения по хранению данных из всех министерств. В этом контексте обсуждалось возможное незаконное использование баз данных и связанные с этим риски конфиденциальности информации.

В *1970-е гг.* пользование компьютерными системами и данными стало еще более активным. По некоторым оценкам, на конец десятилетия в Соединенных Штатах в эксплуатации находилось около 100 тыс. универсальных ЭВМ. С падением цен компьютерные технологии все более широко применялись в государственном секторе и деловых кругах, а также среди общественности. Это десятилетие характеризуется переходом от доминировавших в 1960-е гг. традиционных имущественных преступлений против компьютерных систем к новым формам преступности. В то время как физическое повреждe-

ние оставалось распространенным видом правонарушений против компьютерных систем, появились новые формы компьютерной преступности. Сюда входило незаконное использование компьютерных систем, а также незаконные манипуляции с электронными данными. В результате перехода от совершаемых вручную операций к использованию компьютеров возникла еще одна новая форма преступности — мошенничество, связанное с применением компьютеров. Уже в то время подобные преступления приводили к многомиллионным убыткам. Мошенничество, связанное с применением компьютеров, являлось настоящей проблемой, и правоохранительные органы расследовали все больше и больше подобных случаев. Поскольку применение существующего законодательства к компьютерным преступлениям вызывало трудности, в различных частях света начались дебаты по поводу возможных юридических решений проблемы. В Соединенных Штатах обсуждался законопроект, разработанный специально для борьбы с киберпреступностью. Интерпол изучал само это явление и возможности для законодательного ответа.

В *1980-е гг.* все более и более популярными становились персональные компьютеры. С появлением этой разработки количество компьютерных систем, а значит, и количество потенциальных целей для преступников снова увеличилось. Впервые среди целей находились самые разнообразные типы критически важной инфраструктуры. Одним из подобных эффектов распространения компьютерных систем был возросший интерес к программному обеспечению, что привело к появлению первых форм программного пиратства и преступлений, связанных с патентами. Взаимозависимость компьютерных систем также стала причиной возникновения новых типов правонарушений. Благодаря сетям, для того чтобы войти в компьютерную систему, правонарушителям необязательно было находиться на месте преступления. Кроме того, получив возможность распространять программное обеспечение через сети, преступники пересылали вредоносные программные средства и обнаруживалось все больше и больше компьютерных вирусов. Страны начали процесс доработки своих законодательств, с тем чтобы они отвечали меняющимся криминальным реалиям. Международные организации также подключились к этому процессу. ОЭСР и Совет Европы создали исследовательские комиссии для изучения явления киберпреступности и оценки возможностей для законодательного ответа.

В *1990-е гг.* введение графического интерфейса (www), за которым последовал стремительный рост числа пользователей Интернета, привело к возникновению новых проблем. Информация, размещенная законным образом в открытом доступе в одной стране, становилась доступной из любой точки мира, т. е. даже в тех странах, где

опубликование подобной информации являлось преступлением. Другой связанной с онлайновыми услугами проблемой, которая особенно затрудняла расследование транснациональных преступлений, была скорость обмена данными. Наконец, распространение детской порнографии перешло от физического обмена книгами и видеозаписями к онлайновому распространению через веб-сайты и путем оказания интернет-услуг. В то время как компьютерные преступления носили в целом локальный характер, Интернет превратил электронные преступления в транснациональные. Как результат, международное сообщество стало более активно искать решение проблемы. Резолюция 45/121 Генеральной Ассамблеи ООН, принятая в 1990 г., и выпущенное в 1994 г. Руководство по предупреждению и контролю преступлений, связанных с применением компьютеров, — это лишь два примера предпринятых шагов.

Первое десятилетие нового тысячелетия прошло под знаком новых, крайне изощренных методов совершения преступлений, таких как рассылка подложных электронных сообщений (фишинг) и атаки бот-сети, а также распространение технологий, с которыми правоохранительным органам сложнее работать, таких как передачи голоса по IP-протоколу через Интернет (VoIP) и «облачный компьютинг». Изменились не только методы совершения преступлений, но и их масштаб. Поскольку правонарушители получили возможность автоматически совершать атаки, количество правонарушений увеличилось. Страны, а также региональные и международные организации предприняли ряд мер, чтобы разрешить усугубляющуюся ситуацию, и сделали борьбу с киберпреступностью своей первоочередной задачей. Новые разработки, такие как большие данные, дроны и носимые технологии, представляют собой области, которые, вероятнее всего, станут объектом внимания правонарушителей в будущем.

§ 4. Современные тенденции киберпреступности

В наиболее полном виде современное состояние мировой киберпреступности выражено в двух докладах Европола: «Организованная интернет-преступность. Главная угроза (IOCTA)» от 30 сентября 2015 г. и «Оценка угроз организованной киберпреступности (IOCTA)» от 28 сентября 2016 г.[1]

Европол сообщает об увеличении в 2015—2016 гг. масштабов организованной киберпреступности, нарастании ее технической оснащенности, растущем разнообразии форм и методов, а также ускорении темпов роста объема материального ущерба от киберкриминала.

[1] The Internet Organised Crime Threat Assessment (IOCTA). 2015. Europol, 30 September 2015; Internet Organised Crime Threat Assessment (IOCTA). 2016, 28 September 2016.

Согласно правоохранительной статистике, а также данным специализированных исследовательских организаций в 2015—2016 гг. в некоторых странах ЕС и Великобритании масштабы организованной киберпреступности превысили по объему материальный ущерб от традиционных преступлений.

Киберпреступники используют все более агрессивное и деструктивное кибероружие, затмившее по последствиям своего воздействия, например, привычные банковские трояны. ОПГ в странах ЕС и по всему миру все более активно переходят на модель «преступление как услуга». В рамках модели они предоставляют инструменты и услуги по ширящемуся спектру киберпреступности — от начального до верхнего уровня. Кроме того, организованная киберпреступность все более смыкается с крупной организованной преступностью, обслуживающей трафик нелегальной миграции в страны ЕС, наркотрафик и «черный» сексуальный рынок, взаимодействует с террористическими сетями, а также со спецслужбами государств, имеющих деструктивные по отношению к странам ЕС цели. Границы между организованной преступностью, террористами и деструктивными спецслужбами, включая их прокси-хакерские группы, все более стираются.

Многие из основных угроз остались в 2015—2016 гг. неизменными по сравнению с предыдущим периодом. Это, в частности, относится к кибервымогательству, мелким хищениям с помощью вредоносного «софта», использованию банковских троянов и т. п. В то же время против ожиданий перечисленные ранее виды «простой, своего рода уличной» киберпреступности не растворились в высокотехнологичном криминале, а продолжают нарастать по объемам и молодеть по возрасту. Представляется, что эта тенденция будет сохраняться еще несколько лет, вплоть до достижения преступным рынком в этих сегментах уровня равновесия.

Стремительно продолжает развиваться программно-аппаратная инфраструктура и нарастать число пользователей сетей теневого интернета — DarkNet. Это является основой увеличения объемов преступности, связанной с сексуальной эксплуатацией молодежи и детей. Одновременно организованная киберпреступность открыла для себя за два последних года новый преступный Клондайк, связанный с поиском, профессиональной обработкой и дистрибуцией самогенерируемого неприличного контента. Авторами контента являются сами дети. Кроме того, растут объемы видеоконтента, связанного с жестоким обращением с детьми, а также другими видами педофильских извращений.

Широкое распространение бесконтактных платежных средств, сложных систем идентификации платежных карт и т. п., в том числе с использованием биометрии, привело к некоторому снижению объ-

емов карточного мошенничества в странах ЕС и передислокации криминала, специализирующегося на этом виде преступлений, в другие регионы: в первую очередь в Восточную Европу, страны постсоветского пространства, а также Южную и Юго-Восточную Азию.

В то же время продолжают увеличиваться объемы мошенничества, связанного с обслуживанием банкоматов и преступным нарушением трафика платежных систем электронной коммерции, в первую очередь связанных с авиабилетами, прокатом автомобилей и платежами за туристические путевки. В 2016 г. правоохранительными органами ЕС были обнаружены первые свидетельства того, что ОПГ создали добропорядочные прокси-компании, разработавшие платежные системы на основе блокчейна.

Продолжает увеличиваться объем и эффективность фишинговых компаний. Если раньше в основном их адресатами были отдельные граждане, то в 2015—2016 гг. фишинговые атаки стали в больших масштабах осуществляться против частного сектора и даже правоохранительных органов.

Продолжает расти интенсивность и сложность DDoS-атак[1]. Все чаще они комбинируются с сетевыми атаками, использующими уязвимость программных продуктов. Особенно широко комбинированные DDoS- и сетевые атаки осуществляются в целях получения конфиденциальных данных из медицинских и страховых учреждений, а также налоговых органов. Часто DDoS-атаки используются как прикрытие сетевых атак, имеющих целью кражу интеллектуальной собственности.

Криптовалюты, в частности биткойн, по-прежнему широко используются киберпреступностью. Тем не менее в 2015—2016 гг. большинство ключевых членов сообщества биткойна и практически все разработчики программных средств и приложений на блокчейн не только начали активное сотрудничество с правоохранительными органами, но и сами все чаще стали оказываться жертвами киберпреступников.

В странах ЕС продолжается широкомасштабное и, более того, растущее злоупотребление анонимностью и услугами шифрования для препятствия полицейским расследованиям и судебным преследованиям. Многообразные и эффективные услуги по анонимности и шифрованию обеспечивают преступникам преимущество перед правоохранителями. В результате правоохранительные органы встали перед дилеммой. С одной стороны, эффективная анонимизация и сильные системы шифрования являются важнейшим программным усло-

[1] От англ.: Distributed Denial of Service — распределительный отказ от обслуживания. DDoS-атака — хакерская атака на вычислительную систему с целью довести ее до отказа.

вием обеспечения гражданских прав в странах ЕС, а также ведения безопасной коммерции. С другой стороны, они же препятствуют эффективному противодействию преступности.

Многие из процветающих видов киберпреступности базируются на эксплуатации уязвимостей, известных как минимум уже с десяток лет. Одним из наиболее ярких примеров являются многочисленные уязвимости в широко распространенном в Европе программном продукте Microsoft Office, которым с возрастающим успехом пользуются киберпреступники.

Следует отметить, что большинство зарегистрированных в странах ЕС в 2015—2016 гг. кибератак не являются ни сложными, ни продвинутыми. При этом в некоторых областях киберпреступники демонстрируют высочайший программно-технический и организационный уровень, подавляющая часть кибератак относится к своего рода «уличной киберпреступности» и использует вопиющую безграмотность индивидуальных и корпоративных пользователей.

В то же время в 2015—2016 гг. были обнаружены высокоинновационные подходы и средства, используемые преступниками. Впервые за долгое время им удалось успешно атаковать систему SWIFT, а также NFC нескольких эмитентов.

Наиболее заметной угрозой со стороны вредоносных программ стало использование программ — вымогателей паролей. Ущерб от этих программ затмил даже использование банковских троянов. Использование программ — вымогателей паролей наносит примерно одинаковый ущерб как бизнесу, так и частным пользователям. Как правило, программы — вымогатели паролей используют не крупные киберпреступные группы и разветвленные сети, а киберпреступники-одиночки, в основном в возрасте до наступления гражданской ответственности. Это создает серьезные затруднения для правоохранительных органов.

Простота вредоносных программ и, соответственно, низкая квалификация, требуемая для их использования, ведет к тому, что большинства юных киберпреступников нет в национальных и тем более международных базах по киберпреступности. Следовательно, их идентификация затруднительна. Главным направлением в борьбе с такого рода киберпреступностью является проведение профилактики в хакерской среде и просветительских кампаний среди населения.

В настоящее время смартфоны работают не как простые телефоны, а как мобильные компьютеры. Поскольку емкость памяти у них меньше, чем у других девайсов, пользователи часто не ставят на них мощные антивирусные программы. В условиях, когда пользователи синхронизируют все свои гаджеты, именно смартфоны в странах ЕС

являются главным источником заражения криминальными программами личных и общественных компьютерных сетей.

Сохраняется значительное расхождение в оценке источников наибольшей опасности киберпреступности. Правоохранительные органы, исходя из фактического положения дел, полагают, что в настоящее время наибольший ущерб не только гражданам, но и бизнесу наносит различного рода относительно простой в эксплуатации платный вредоносный «софт», а также действия криминала по модели «преступление как услуга».

В то же время компании, специализирующиеся в области интернет-безопасности, в значительной мере переключили свое внимание с защиты массового «софта» на дорогой «софт», ориентированный на крупный бизнес и государственные органы. В результате в то время как преступники используют все более эффективные, относительно дешевые и простые в эксплуатации вредоносные программы, индустрия интернет-безопасности не предоставляет массовому пользователю средств защиты от них, ориентируясь на богатых корпоративных потребителей.

Формируется международная трансконтинентальная сеть, соединяющая DarkNet, анонимные системы платежей и протоколы шифрованного трафика, обслуживающая рынок педофилии и жестокого обращения с детьми. Азиатские, латиноамериканские и отчасти африканские страны выступают поставщиками контента, Северная Америка и страны ЕС — его потребителями, а государства Восточной Европы и постсоветского пространства — операторами и отчасти владельцами этого рынка.

Положительным явлением стало снижение объемов криминального рынка, связанного с карточным мошенничеством в рамках ЕС, и эмиграция как преступников, так и финансовых потоков в страны за пределы ЕС.

Стабильно увеличивается онлайн-преступность, связанная с дешифровкой протоколов и нарушением целостности программных инфраструктур электронной торговли, в первую очередь продажи авиабилетов, проката автомобилей, заказа гостиниц и т. п.

В 2015—2016 гг. в ЕС начали действовать ОПГ, специализирующиеся исключительно на компрометации платежей бесконтактных (NFC) карт. Этот пример показывает, что наряду с широким распространением уличной киберпреступности каждая новая технология становится полем для криминального бизнеса высокообразованных и высококвалифицированных преступников.

Трендом 2015—2016 гг. в странах ЕС стало осуществление корпоративных преступлений, особенно в финансовом секторе, где киберпреступления были не исключительным, а одним из криминальных

инструментов наряду с коррупцией и использованием методов социального инжиниринга.

Продолжают нарастать масштабы и изощренность DDoS-атак в комбинации с сетевыми атаками по компрометации систем информационной безопасности.

В 2015—2016 гг. продолжилась тенденция увеличения доли преступлений против финансовых и инвестиционных институтов в общем объеме киберпреступности. Если ранее практически вся киберпреступность была направлена против электронной торговли и непосредственно граждан, то в настоящее время объем преступлений против финансовых институтов уже сравнялся в странах ЕС с киберпреступностью в сфере онлайн-торговли.

Экспоненциально растет количество, а главное — масштабы преступлений, связанных с кражей различного рода данных — от информации по интеллектуальной собственности и коммерческой тайне до персональных сведений и медицинской информации. Все более характерной является кража данных не для финансовой перепродажи, а как основа для осуществления сложных многокомпонентных мошенничеств, вплоть до вмешательства в деятельность государственных органов и в избирательные кампании.

В 2015—2016 гг. произошел качественный скачок в коммуникационной оснащенности киберпреступников. Если ранее они использовали преимущественно электронную почту, а также сети Tor и P2P, то в настоящее время все большую долю в коммуникациях занимают криптоустойчивые мессенджеры типа Jabber, а также шифрованные, не принадлежащие легальным корпорациям сервисы видеозвонков.

В 2015—2016 гг. в странах ЕС киберпреступники использовали все более сложные системы шифрования и анонимизации. Сложился быстрорастущий рынок программно-аппаратных комплексов для преступников, которые включают устройства с мгновенно уничтожаемыми компонентами памяти, оснащенные специальными операционными системами и встроенными на уровне «харда» шифровальными системами и т. п.

В 2015—2016 гг. полицейским органам в странах ЕС удалось осуществить ряд успешных крупномасштабных операций против киберпреступников, действующих в сетях Интернет и DarkNet. Эти успехи имели и оборотную сторону. Некоторые преступные группировки, ссылаясь на форс-мажорные обстоятельства, покинули онлайн-рынки с деньгами клиентов, часто также принадлежащих к преступному сообществу. В итоге в 2015—2016 гг. в преступном мире усилились войны и конфликты, последствия которых ощущаются и законопослушными гражданами.

Несмотря на ожидания, в 2015—2016 гг. террористические, экстремистские и преступные группы в странах ЕС не использовали киберсреду для разрушения или нарушения работоспособности IT-инфраструктуры, производственных предприятий и городских служб. Интернет, особенно социальные медиа, продолжают использоваться террористами и экстремистами преимущественно не как поле атак на физический мир, а для вербовки, пропаганды и отмывания преступных доходов.

В 2015—2016 гг. в большинстве стран заметно увеличилось количество кибератак на частные и бизнес-сети. В большинстве атак киберпреступники для взлома гаджетов и сетей использовали уже хорошо известные инструменты и сервисы. Наибольшее число атак было осуществлено с использованием программ — вымогателей паролей, программ-шпионов, а также программ, компрометирующих безопасные протоколы платежных систем.

Использование программ-вымогателей продолжает оставаться доминирующей проблемой для правоохранительных органов ЕС. Несмотря на то что полиции стран ЕС удалось в течение 2015—2016 гг. разгромить наиболее крупные группировки киберпреступников, специализировавшихся на программах-вымогателях, общее количество такого рода атак увеличилось. Это произошло за счет резкого снижения уровня организованности киберпреступности с распадом групп и переходом на одиночные действия параллельно со стремительным снижением возраста киберпреступников.

Сложилось два принципиально разных подхода к использованию программ-вымогателей. Если юные киберпреступники используют программы-вымогатели как самодостаточные, то небольшие хакерские группировки сочетают применение программ-вымогателей с «софтом» другого типа. Как правило, в таких случаях программы-вымогатели используются для получения доступа в личные кабинеты с последующим внедрением программ-шпионов, а затем «софта», позволяющего перенаправлять платежи.

В киберпреступности, направленной против корпораций, четко проявляются две тенденции. С одной стороны, уменьшается число инцидентов, связанных с успешным проникновением злоумышленников в корпоративные хранилища и базы данных, с другой — увеличивается суммарный и средний ущерб от кражи данных в корпоративных хранилищах.

В 2015—2016 гг. стремительно нарастало число атак на частные и корпоративные сети с использованием зловредного «софта», первоначально заразившего гаджеты. Согласно исследованиям, проведенным известными международными компаниями, до 70% мобильных телефонов в странах ЕС инфицировано различными «зловредами». Поскольку мобильные телефоны берут на себя все больше и больше

«умных» функций, постоянно растущее разнообразие мобильных «зловредов» создает серьезные угрозы не только отдельным гражданам и бизнесу, но и в целом государственным инфраструктурам.

По оценке ведущих компаний в области компьютерной безопасности, не менее 10% приложений, реализуемых через магазины Google Play и ITunes, либо инфицированы, либо созданы компьютерными компаниями и группами по поручению и за счет средств криминального бизнеса. Именно мобильные «зловреды» создают принципиально новую угрозу. Зараженный ими гаджет является не только воротами для преступников в личные и корпоративные информационные системы, но и выполняет функции шпиона в отношении их частной и производственной жизни в режиме 7/24.

Неприятным обстоятельством является быстрая смена поколений преступного «софта». Если в первой половине 2010-х гг. срок жизни и эффективного использования эксплойтов составлял три-четыре года, то во второй не превышает одного-двух лет. Надо быть готовым к тому, что значительная часть «софта» уже в 2018 г. канет в прошлое. Это большая проблема и вызов для правоохранительных органов, поскольку они в отличие от преступников зависят от бюджетных ассигнований, которые выделяются не на перспективу, а по итогам.

Главным направлением производства, распространения, продаж и выполнения хакерских работ как услуг станет вредоносный «софт» для мобильных устройств и все, что с ним связано. На начало 2017 г. на одного жителя стран ЕС приходится 1,4 гаджета. При этом доля гаджетов известных брендовых компаний-производителей составляет чуть больше 50%. Компании, занимающиеся интернет-безопасностью, полагают, что подавляющая часть небрендовых мобильных устройств не просто заражена вредоносным «софтом» — вредоносный «софт», в том числе отслеживающий активность и действия пользователя в физической среде, встроен в гаджеты на аппаратном уровне или по крайней мере предустановлен.

Имеются многочисленные признаки, что в 2016 г. в распоряжении преступных групп появились сверхсложные модульные программы, способные не только преодолевать антивирусную защиту и системы корпоративной информационной безопасности, не только красть данные, но и разрушать системы или даже брать на себя управление ими. Однако ни одна такая программа не была обнаружена на «черных» рынках хакерского «софта». Никто также не рекламировал возможность использования подобных платформ в рамках модели «хакерство как услуга». Специалисты высказывают предположение, что данные комплексы созданы закрытыми ОПГ исключительно для собственных нужд. Более того, подобные ОПГ, вероятно, целенаправленно пытаются скрыть практическое применение этих платформ как

в преступных целях, так и в рамках взаимодействия с террористами или спецслужбами.

Косвенным подтверждением расслоения европейской киберпреступности на уровни, различающиеся программной оснащенностью, кадровым обеспечением и применением организационных форм, стало использование методов стеганографии — сокрытие сообщений в графических изображениях. Эти методы ранее применялись исключительно спецслужбами. В 2015—2016 гг. было обнаружено использование подобных методов для защиты коммуникаций и передаваемых данных внутри и между особо продвинутыми преступными кибергруппами. В настоящее время эти методы используются элитой киберпреступности.

По данным Европола, большинство стран ЕС сообщили, что оценивают уровень угроз со стороны киберпреступников «облачным» государственным, коммерческим и общественным «облачным» инфраструктурам от среднего до высокого. Почти 50% сотрудников правоохранительных органов в странах ЕС, опрошенных в 2015 г., сообщили о необходимости принятия специальных законодательных актов, облегчающих сбор доказательств из национальных и международных «облачных» хранилищ.

В 2015—2016 гг. были зафиксированы первые криминальные кибератаки на европейские «облака». При этом в нескольких случаях они осуществлялись с целью получить деньги за возврат похищенных в «облаках» файлов. Киберпреступность в «облаках» создает правоохранительным органам целый ряд правовых, оперативных и технических проблем. Главная из них состоит в том, что собственными силами правоохранительные органы с этой проблемой не справятся. Со сдержанным оптимизмом можно констатировать тот факт, что практически все правоохранительные органы стран ЕС тесно сотрудничают по этой проблематике с научно-исследовательскими учреждениями, университетами и бизнесом.

В отчете 2017 г. компания Nexusguard указывает на проблему незащищенных сетей «Интернета вещей» (IoT-устройств). Тенденция касается множества устройств, задействованных в потребительских и промышленных целях, подключаемых к Сети без соблюдения должных мер безопасности.

В последние годы хакеры начали использовать большее количество уязвимых устройств для создания масштабных ботнетов из тысяч и миллионов зараженных девайсов: маршрутизаторов, Smart-TV и т. д. Уязвимость IoT-устройств подтверждается и в отчете «Лаборатории Касперского». Одним из примеров паразитирования называют ботнет Mirai. Подход, используемый его создателями, послужил основой для множества других бот-сетей.

В 2017 г. тип атак DDoS на «Интернет вещей» достиг критической массы — в каждом случае нападения задействованы сотни тысяч устройств, подключенных к Интернету. Борьба с этим явлением только начинает разворачиваться, хотя поставщики IoT-оборудования крайне медленно реагируют на угрозы.

Счетная палата США в мае 2017 г. выпустила отчет об оценке IoT-технологий, во многом сосредоточенный на уязвимости систем перед кибератаками. Среди основных факторов, сопутствующих распространению угроз, названы отсутствие контроля безопасности из-за невозможности спрогнозировать потенциальные проблемы, а также применение идентичного программного обеспечения в различных устройствах, что увеличивает эффективность эксплуатации технических уязвимостей. В связи с этим управление рекомендует разрабатывать IoT-устройства с обязательной возможностью обновления, причем в доступной форме, а не посредством сложного для пользователя процесса.

Уже сейчас устройствами, входящими в «Интернет вещей», пользуются около 4,9 млн человек. А, по прогнозам, к 2020 г. у потребителей будет 25 млн различных бытовых предметов, имеющих доступ в Сеть.

Чтобы установить, насколько опасны эти вещи, исследователи изучили шесть самых популярных устройств: Chamberlain MyQ Internet Gateway, Chamberlain MyQ Garage, Smart Things Hub, Ubi, Wink Hub и Wink Relay. Исследование показало, что обнаруженные в этих высокотехнологичных продуктах уязвимости могут дать злоумышленникам существенную информацию, которая поможет им планировать и осуществлять преступления против пользователей.

В частности, если хакер воспользуется брешью в системе безопасности и взломает устройство Ubi, которое позволяет владельцу квартиры голосом управлять разными функциями «умного» дома, то он узнает, когда хозяин находится дома, проанализировав уровень света и громкости звука в помещении.

Мало того, уязвимости в устройствах Wink Relay и Ubi могут приводить к тому, что хакеры будут подключаться к микрофонам внутри квартир и слушать все, что говорят их обитатели. В результате они завладеют конфиденциальными сведениями, которые послужат им для шантажа или шпионажа.

Еще одну подсказку для грабителей оставит взломанное устройство Chamberlain MyQ. Преступники будут в курсе, когда дверь придомового гаража открыта и закрыта.

В итоге исследователи установили, что все девайсы, кроме одного, имеют критические уязвимости, ставящие под угрозу безопасность обитателей дома. Киберпреступники могут воровать персональные данные и даже брать на себя управление гаджетами.

§ 5. Особенности современной киберпреступности в России

По данным МВД России, число киберпреступлений в России с 2013 по 2016 г. возросло в шесть раз. Причем рост произошел в первую очередь за счет роста числа совершаемых мошенничеств. Этот рост киберпреступлений обусловлен прежде всего доступностью программных средств, позволяющих даже слабо подготовленным пользователям совершать сложные киберпреступления. Наиболее распространенные схемы ориентированы на хищения денег как у клиентов банков, так и у самих кредитно-финансовых учреждений.

Эксперты компании Positive Technologies, специализирующейся на кибербезопасности, посчитали количество хакерских атак, совершенных в разных странах мира в 2017 г. Лидерство удерживают США, здесь совершается 41% всех кибератак. Россия занимает второе место — 10% всех атак. Третье место досталось Великобритании — на нее пришлось 7%.

Согласно исследованиям российской компании GROUP-IB[1] основные виды киберугроз в России выглядят следующим образом.

Угрозы для бизнеса

Основными мишенями целевых кибератак остаются государственный и финансовый сектор, а мотивом нападения — промышленный шпионаж или кража денег.

В 2015—2016 гг. главной мишенью киберпреступников в стране были небольшие региональные банки. Сами целевые атаки стали изощреннее и практически всегда происходят с использованием методов социального инжиниринга. Например, сотрудники одного из банков получили на рабочую почту рассылку о вакансиях в Центробанке. Многие не удержались и открыли зараженное письмо, вирус начал распространяться по внутренней сети.

Атаки на банки. Начиная с 2013 г. несколько разных групп русскоговорящих хакеров атакуют банки и платежные системы. Делают это они очень успешно. Причем если раньше информацию об этих инцидентах удавалось держать в секрете, то сейчас финансовые учреждения уже не могут хранить подобные инциденты в тайне из-за их масштабов.

Наиболее ярким примером является деятельность группы Anunak (также известной как Carbanak). Она успешно атаковала более 50 российских банков и пять платежных систем. Общая сумма хищений,

[1] См.: Киберпреступность в России и ее влияние на экономику страны, 2016 г.

к которым причастны эти мошенники, составляет более 1 млрд руб., бóльшая часть хищений приходится на вторую половину 2014 г.

В конце 2015 г. и начале 2016 г. группа Buhtrap успешно похитила у 13 банков 1,8 млрд руб. Средняя сумма хищения составила 143 млн руб.

Тактику действий данной группы можно представить следующим образом.

1. Атакующие отправляли письма с вредоносным вложением от имени Центрального банка России или потенциального клиента сотруднику банка. Если письмо отправлялось от имени потенциального клиента, то менеджеру в банке могли предварительно позвонить и рассказать о намерениях открыть счет в банке. Иногда письмо содержало эксплойт, иногда сразу вредоносную программу.

2. После открытия вредоносных вложений на компьютер устанавливались средства удаленного доступа, которые обеспечивали начальный доступ к сети финансового учреждения.

3. Далее атакующий начинал проводить внутренний аудит сети банка, постепенно собирая информацию о внутренних серверах, администраторах, операторах банковских систем.

4. На рабочие места операторов банковских систем устанавливались программы слежения, записывающие видеороботы с этими системами, которые создавали снимки с экранов и передавали всю информацию атакующим, что давало им возможность правильно повторять действия настоящих операторов систем.

5. В отдельных случаях злоумышленники добирались до сетей управления банкоматами и получали контроль над некоторыми из них. Как итог, у хакеров была возможность по команде выдавать всю имеющуюся наличность из этих банкоматов.

Позже у этой группы появились последователи. В результате количество инцидентов в банках и платежных системах увеличивается, суммы ущерба постоянно растут.

Атаки на брокера. В 2015 г. была проведена первая успешная атака на брокера, которая вызвала большой резонанс среди участников финансового рынка.

Для этой атаки использовался троян Corkow (также известный как Metel). Он предоставляет удаленный доступ к системе, что позволило злоумышленнику запускать программы, управлять клавиатурой и мышкой параллельно с оператором системы.

В результате несанкционированного доступа к терминалу торговой системы было выставлено пять заявок на покупку 437 млн долл. и две заявки на продажу 97 млн долл. Однако была исполнена только часть заявок, и в результате было куплено 158,536 тыс. и продано 93,925 тыс. долл. США.

Указанные действия вызвали очень большую волатильность в течение 6 минут, что позволило совершить сделку на покупку долларов по курсу 59,0560 руб. и через 51 секунду продать по курсу 62,3490 руб. На графике по торгам в тот день отчетливо была видна «свеча», показывающая разницу курса от 55 до 66 руб., что привело к ущербу для банка в 300 млн руб.

Через 14 минут после первой заявки хакер дал команду Corkow на удаление своих следов и вывод системы из строя.

Атака на расчетную систему. 16 августа 2015 г. произошел инцидент, в результате которого через банкоматы было похищено около 500 млн руб. Этот инцидент затронул около 15 крупных банков — участников одной из российских расчетных систем, которая объединяет около 250 банков и позволяет держателям карт банков-участников снимать средства с карт Visa и MasterCard по выгодным тарифам.

Как и во всех описанных выше случаях, использовались вредоносные программы, которые хорошо известны антивирусным компаниям, но обнаружить их работу вовремя стандартными средствами антивирусной защиты очень сложно. Эти вредоносные программы предоставляли удаленный доступ к нужным системам внутри защищенных сетей и открывали перед атакующими все возможности, доступные сотрудникам финансовых учреждений.

Атаки на оборонные предприятия. В декабре 2015 г. был опубликован отчет о шпионской кампании Roaming Tiger. О ней стало известно еще в конце 2014 г. По данным ESET, жертвами преступников являлись организации в Российской Федерации, Украине, Беларуси, Узбекистане, Казахстане, Таджикистане и Киргизии. С помощью вредоносных RTF-файлов злоумышленники инфицировали системы жертв вирусом «троян» семейства PlugX. Командно-контрольная инфраструктура указывала на китайское происхождение Roaming Tiger.

Злоумышленники атаковали предприятия стратегического назначения в странах СНГ с помощью тех же методов и векторов атак. Отличие заключается только в одном — на смену PlugX пришел совершенно новый инструмент под названием «BBSRAT». Оба трояна используют похожие механизмы заражения, но отличаются по архитектуре и модели поведения.

Как минимум в одной из атак злоумышленники рассылали фишинговые письма с вложенным вредоносным документом Word, эксплуатировавшим уязвимость в Microsoft Office (CVE-2012-0158), впоследствии устраненную. Эта же уязвимость использовалась в атаках Roaming Tiger. На этом совпадения не заканчиваются — C&C-архитектура у BBSRAT точно такая же, как у PlugX.

С помощью вредоносных писем злоумышленники пытались инфицировать системы научно-производственного центра «Вигстар», занимающегося производством оборудования для российских вооруженных сил и спецслужб.

Хищения через интернет-банкинг. Крайне опасной угрозой для бизнеса является хищение денежных средств с банковских счетов компании в результате компьютерной атаки. Такие инциденты случаются ежедневно, независимо от местонахождения компании, размера бизнеса, банка, банковской системы и используемых средств защиты. Практически все стандартные меры безопасности, применяемые банками, — защищенные токены (ключи для авторизации пользователя), отслеживание смены оборудования и мест отправки платежных поручений, СМС-подтверждение и т. п. — можно обойти. По данным ежегодного отчета Group-IB, в период со второй половины 2014 г. по первую половину 2015 г. ежедневно совершалось 16 атак на компании с целью хищения денежных средств с их банковских счетов. Почти во всех случаях доступ был получен именно к компьютерам бухгалтеров.

Вот некоторые из наиболее популярных способов совершения хищений.

Ручной перевод с компьютера владельца счета через удаленный доступ. Для того чтобы обойти защиту электронных цифровых подписей (ЭЦП), хранимых на защищенных токенах, а также системы обнаружения смены компьютера владельца счета, злоумышленники используют удаленное подключение к компьютеру владельца счета и совершают мошеннический перевод прямо с него. Процесс формирования платежного поручения начинается после того, как владелец счета подключил к ЭВМ токен с ЭЦП. При удаленном подключении преступника работа владельца компьютера не нарушается и может проходить одновременно. Удаленный доступ будет предоставлен атакующему, даже если все входящие соединения к компьютеру владельца счета будут запрещены. Это обеспечивается за счет того, что средства удаленного доступа сами устанавливают исходящее соединение с сервером преступника, а злоумышленник, используя это исходящее соединение, подключается к компьютеру владельца счета. Исходящие соединения с компьютером владельца счета, как правило, разрешены для обеспечения нормальной работы в сети Интернет.

Автоматический период (автозалив). Данный вариант совершения платежа является наиболее совершенным. Автозалив можно сделать двумя способами.

1. Непосредственно перед подписанием платежного поручения владельцем счета вредоносная программа заменит реквизиты платежа на мошеннические, при этом на экране будут отображаться данные,

внесенные владельцем счета. В результате владелец счета подпишет уже измененное платежное поручение и отправит его в банк.

2. Вредоносная программа дождется подключения токена с ЭЦП, сама запустит систему интернет-банкинга, войдет с использованием логина/пароля владельца счета, сформирует платежное поручение и отправит его в банк.

Для того чтобы троянская программа в автоматическом режиме перевела денежные средства, злоумышленник должен подготовить специальный файл настроек с указанием реквизитов для перевода. Данный файл настроек будет скачан вредоносной программой по команде с сервера управления бот-сети.

Метод социального инжиниринга. Основной задачей троянской программы является перенаправление пользовательских запросов при доступе к банковским сайтам на мошеннический сайт со страницами, внешне копирующими настоящий сайт банка. Фишинговый сайт используется для получения таких данных, как логин/пароль, номер телефона владельца счета. Переводы денежных средств необходимо подтверждать одноразовым кодом, который может быть получен владельцем счета по СМС, со скрэтч-карты или иным способом.

Для получения кода подтверждения злоумышленник показывает фишинговые страницы, требующие ввести код подтверждения под разными предлогами, например для отмены мошеннической операции. При нажатии на любую из кнопок (аннулировать или подтвердить) код подтверждения будет отправлен преступнику, и он сможет завершить перевод денежных средств.

Если пользователь не вводит полученный код подтверждения, то злоумышленник, используя номер телефона, который будет указан пользователем на фишинговом сайте, осуществит звонок владельцу счета от имени банка. Цель звонка — уговорить пользователя ввести код подтверждения перевода денежных средств на фишинговом сайте либо продиктовать код по телефону.

Программы-вымогатели. В России эта угроза стала серьезной проблемой для бизнеса относительно недавно. Основной задачей таких программ является шифрование файлов надежным методом, чтобы расшифровать их можно было только при наличии специального секретного ключа, находящегося у злоумышленника. И таких программ появляется все больше, они становятся дешевле и доступнее более широкому кругу лиц, которые хотят попробовать заработать на данном виде мошенничества. Шифрование, используемое этими программами, надежно, и найти альтернативный способ дешифрования, кроме как получить ключ расшифровки данных от атакующего либо с его сервера, невозможно. Главное — это зашифровать не просто файлы, а базы данных, рабочие документы, резервные копии и т. д.

После того как файлы зашифрованы, вам показывают сообщение, в котором описывают, сколько и куда необходимо перевести денег, чтобы получить ключ расшифровки. Как правило, оплата производится в биткойнах.

Сильнее всего компании страдают, когда злоумышленники шифруют базы 1С, общие файловые серверы, данные резервных копий. Когда зашифрованными оказываются такие данные, многие соглашаются заплатить вымогателям, лишь бы восстановить доступ к драгоценным данным, и тем самым поддерживают развитие данного направления.

Основной способ распространения таких программ — рассылки по электронной почте вложений под видом банковских выписок, счетов, актов-сверок, уведомлений о вызове в суд и т. п.

Некоторые хакеры, управляющие банковскими троянами, в первую очередь интересуются компьютерами с системами дистанционного банковского обслуживания и часто обнаруживают компьютеры бухгалтеров, которые привыкли работать удаленно в 1С. Поэтому они начали продавать информацию о таких компьютерах своим «партнерам», чтобы те шифровали данные и извлекали из этого прибыль.

Неправомерное использование бренда. Еще одной серьезной угрозой для бизнеса является неправомерное использование бренда. Наиболее очевидный пример — использование бренда для проведения фишинговых атак на клиентов, партнеров или даже внутренних сотрудников компании. Однако кроме фишинга для клиентов компании есть и другие опасные примеры неправомерного использования бренда.

В июле 2015 г. компания «Акрон» сообщила на своем сайте о возможном мошенничестве: злоумышленник создает поддельные сайты, акции которых торгуются на различных биржах. На таких сайтах публиковались недостоверные, заниженные финансовые показатели. Злоумышленники рассчитывали «уронить» цену акций предприятий, чтобы купить их, а после того как акции подорожают, продать. Проверка действий мошенников выявила, что они создали поддельные сайты таких известных компаний, как группа компаний «ГАЗ», ОАО «Газпром нефть», компания «Транснефть», АФК «Система» и многих других. Подобного рода мошеннические ресурсы наносят не только репутационный ущерб владельцам брендов, но и прямой финансовый ущерб.

Сейчас многие компании — банки, онлайн-магазины, такси, рестораны и т. д. — выходят на рынок со своими мобильными приложениями. Мошенники используют этот тренд, создавая фейковые мобильные приложения, которые пользователи устанавливают, среагировав на хорошо узнаваемые бренды и символику. Как правило, все они становятся жертвами мошеннических или вредоносных программ. Это не только наносит вред пользователям, скачавшим подобные приложения, но и подрывает доверие в Интернете к компаниям, которые не уделяют должного внимания защите своих брендов.

В Интернете всегда находятся люди, которые хотят быстро заработать, и этим также активно пользуются мошенники. Для таких любителей «бесплатного сыра» создаются различные хайп-проекты (HYIP — High Yield Investment Program) — по сути, та же финансовая пирамида. Для того чтобы привлечь людей в эти проекты, создатели подобных пирамид добиваются доверия клиентов и желания отдать («вложить») свои деньги. И в этом очень помогает использование имен, логотипов хорошо узнаваемых и надежных компаний.

Нельзя не вспомнить и о том, какой вред наносят производителям программного обеспечения различные активаторы, генераторы ключей и другие средства, используемые пиратами. Нередко такие средства являются вредоносными программами, которые позволяют пиратам получить доход от своего нелегкого труда по созданию этих средств, распространению их по Сети путем выкладывания на файлообменные ресурсы, торренты, рекламирования на специализированных ресурсах, посвященных пиратству, и т. п.

Угрозы для физических лиц

Фишинг. Каждый месяц в 2015—2016 гг. Group-IB фиксировала в среднем около 100 тыс. фишинговых ссылок. Примерно 50% этих фишинговых ссылок направлены на клиентов компаний из финансового сектора.

Стоит привести пример таких атак, чтобы стало понятно, почему пользователи очень легко попадают на удочку атакующих и как мошенники легко обходят меры защиты со стороны банков. Для этого мы опишем тактику действий одной из преступных групп.

1. Атакующие покупают списки уязвимых сайтов самой разной тематики. Таких сайтов на просторах российского Интернета очень много.

2. Обладая даже ограниченным доступом к такому сайту, они могут изменять его таким образом, чтобы часть его посетителей перенаправлялась на фишинговую страницу. Если пользователь зашел на «поломанный» сайт в результате поискового запроса в системах Google, Yandex, Bing, Rambler, Mail.ru, его перенаправляют на фишинговый сайт. При этом переход жертвы может быть на любую

страницу «поломанного» сайта, кроме главной, иначе перенаправление на фишинговый сайт не осуществляется.

3. Фишинговый сайт замаскирован под акцию по розыгрышу призов и информирует жертву о том, что она выиграла денежный приз и может получить деньги. Для этого жертву просят указать данные банковской карты.

4. Если жертва указывает данные карты, то на следующем шаге ее просят указать текущий баланс карты.

5. На сайтах разных банков есть услуга перевода с карты на карту. Для того чтобы перевести деньги, необходимо указать данные карты отправителя, получателя, сумму перевода и СМС-код подтверждения. Как только жертва указывает данные о своей карте, программа на сервере хакеров автоматически пытается сделать перевод с карты на карту.

6. Жертва должна подтвердить денежный перевод со своей карты с помощью СМС-кода. В этот момент на фишинговом сайте жертве показывают окно, информирующее, что для получения выигрыша нужно ввести СМС-код, полученный на мобильный телефон. Если жертва вводит данный код в поле фишингового сайта, злоумышленники используют его для мошеннического денежного перевода.

Схема очень проста. Она не требует использования вредоносных программ, очень легко масштабируема и позволяет атакующим зарабатывать миллионы рублей.

Сама схема требует, чтобы пользователь указывал все данные сам, но, как показывает исследование, на эти фишинговые страницы попадают тысячи пользователей ежедневно и среди этих тысяч всегда находятся доверчивые граждане, которые и становятся жертвой мошенников.

Кардинг. Этот сегмент продолжает развиваться очень быстрыми темпами. Сейчас угрозы можно разделить на две категории: поддельные POS-терминалы, трояны для POS-терминалов (Point of Sale — устройство для приема платежных карт) и сопутствующие им услуги.

Поддельные POS-терминалы. Злоумышленники осуществляют активный поиск инсайдеров в ритейле, которые готовы подработать за процент.

Анализ хакерских форумов показал, что злоумышленники построили целый бизнес по продаже прошивок к POS-терминалам, которые превращают данные устройства в скиммеры. Причем некоторые злоумышленники продают уже прошитые POS-терминалы, другие продают прошивки для них, третьи прошивают POS-терминалы за деньги или процент скомпрометированных дампов (англ.: dump — свалка — информация о состоянии компьютерной системы).

Когда пользователь расплачивается на кассе, есть риск, что данные его карты в этот момент передаются злоумышленнику.

Трояны для POS-терминалов. Сразу оговоримся: в примерах, описанных выше, необходимо использовать специальные POS-терминалы. И установить их в точках массовых продаж практически невозможно. Но превратить нормальный терминал в мошеннический можно с помощью специальных вредоносных программ.

Одним из первых троянов именно для POS-терминалов был Dexter, о котором сообщили в декабре 2012 г. Можно сказать, что с него и началось широкое распространение данного способа получения дампов карт. Рынок вредоносных программ для POS-терминалов сильно вырос за последнее время.

Сейчас на «черном» рынке продают не только сами вредоносные программы, но и отдельно доступ к терминалам, на которые эти программы можно установить. Программы совершенствуются, и появляются новые авторы. Получить доступ к POS-терминалам гораздо проще, чем к процессинговому центру, а вот результат также может быть внушительным. Компрометации POS-терминалов крупных ритейл-сетей позволяют злоумышленникам получать данные миллионов карт. Так, последние массовые утечки данных карт связаны именно с этим способом. В декабре 2013 г. из американской сети Target были похищены данные около 70 млн карт, а в сентябре 2014 г. сеть магазинов Home Depot сообщила о компрометации около 56 млн карт.

Сейчас на хакерском рынке большое количество разных программ, которые можно использовать для заражения POS-терминалов, и все данные карт, которые будут проходить через терминал, сразу станут известны злоумышленникам. Тактика действий у хакеров следующая.

1. Хакеры различными способами находят и заражают POS-терминалы. Для этого они могут использовать вредоносные программы, подбирать пароли к разным серверам, рассылать письма с вредоносными вложениями, использовать инсайдеров в точках, где установлены такие терминалы, и т. п.

2. После того как вредоносная программа успешно установлена, она начинает собирать из оперативной памяти терминала номера карт и данные магнитной полосы или чипа. Полученные данные отправляются на сервер злоумышленника.

3. Собранных данных достаточно для изготовления дубликатов карт, которыми можно воспользоваться при покупке товаров, снятии наличных и т. д.

Хищения через Интернет и мобильный банкинг. Самую большую угрозу для банковских счетов физических лиц представляют банковские трояны для Android-устройств. Более 80% смартфонов в мире

работает на платформе Android, неудивительно, что большинство вирусов пишутся именно под нее. Все новые банковские трояны, написанные под Android, умеют похищать деньги автоматически. Они собирают данные банковских карт, и уже не важно, клиентом какого банка является владелец телефона. Зараженный трояном смартфон фактически шпионит за своим владельцем: передает хакерам историю звонков и СМС, доступ к любым файлам на телефоне и информации в «облачном» хранилище, следит за геолокацией.

Жертва сама загружает и запускает вредоносную программу, иногда следуя инструкциям по установке. Чтобы заставить жертву выполнить эти манипуляции, атакующий распространяет такие программы под видом легальных, например пиратской версии навигатора, средств просмотра фото- или видеофайлов, обновлений операционной системы, расширений и т. п.

С мобильного устройства можно получить абсолютно все данные для совершения мошенничества:

— данные об остатках на банковском счете;

— номер банковской карты, срок действия и CVV (Card Validaton Value);

— СМС-коды для подтверждения платежей;

— сведения, подключен ли интернет-банк;

— коды восстановления пароля для доступа в интернет-банк.

Естественно, что злоумышленники начали атаковать именно эти мобильные устройства, получать доступ к описанным выше данным и активно похищать денежные средства. Ежедневно совершается около 70 успешных хищений со счетов владельцев зараженных мобильных устройств, и общий ущерб в 2015 г. составил 61 млн руб.

Одним из наиболее популярных способов хищения является перевод через СМС-банкинг. Пошагово процесс хищения можно представить следующим образом.

1. Троянская программа пересылает все СМС на сервер злоумышленника.

2. Злоумышленник ищет на сервере СМС с уведомлениями от банков. Например, такие СМС приходят после совершения покупок, и в них содержится информация о балансе банковского счета.

3. Если злоумышленник находит номер телефона с интересующим балансом и владелец телефона является клиентом банка, который предоставляет услугу СМС-банкинга, то злоумышленник создает задание вредоносной программе на отправку СМС с информацией о переводе денежных средств на номер банка. При этом все дальнейшие уведомления от банка будут скрываться на телефоне владельца счета и передаваться на сервер злоумышленника.

4. Банк отправляет код подтверждения операции на перевод денежных средств по СМС.

5. Троянская программа перехватывает СМС от банка, скрывает это СМС от пользователя и передает его текст на сервер злоумышленника.

6. Злоумышленник создает задание вредоносной программе на отправку СМС с кодом подтверждения на номер банка.

7. Вредоносная программа выполняет задание, в результате чего операция перевода завершается.

Описанные выше шаги часто автоматизируются, и деньги могут списывать с банковского счета небольшими суммами на протяжении нескольких дней.

Другим популярным способом является сбор данных на мобильном устройстве о банковских картах с последующим переводом с карты на счет хакера. Для сбора данных карт вредоносная программа показывает блокирующее окно, в которое необходимо ввести достоверные данные карты, как на примере ниже. Такие данные собираются на сервере у хакера, и в нужный ему момент он может начать переводить деньги. Все коды подтверждения платежей будут приходить на тот же номер телефона жертвы и немедленно пересылаться хакеру.

Программы-вымогатели. Программы-вымогатели существуют довольно давно. Раньше они показывали блокирующие окна, которые было сложно закрыть, а чтобы их убрать, необходимо было заплатить атакующему. Однако средства антивирусной защиты эффективно могли противодействовать таким вредоносным программам, антивирусные компании создавали специальные сайты, где можно было найти коды разблокировки. В любом случае пользователь всегда мог переустановить операционную систему, и его данные оставались в сохранности.

Однако ситуация изменилась, когда хакеры начали шифровать файлы и требовать деньги не за разблокировку компьютера, а за ключ дешифровки. Средняя сумма, которую требуют атакующие для расшифровки файлов, составляет 400 долл. США. Ситуация очень схожа с угрозами, характерными для бизнеса, но и тут есть свои отличия.

С развитием мобильных устройств часть очень важных для пользователя данных стала храниться в гаджетах. Поэтому хакеры начали делать аналогичные программы и для мобильных устройств.

На этом хакеры не остановились. Они поняли, что одними из самых платежеспособных пользователей являются владельцы iPhone, но заразить технику Apple сложнее из-за сильных ограничений на ус-

тановку программ из недостоверных источников. Для атак на владельцев iPhone хакеры пользуются следующей тактикой.

1. Они скупают или сами подбирают пароли от сервиса iCloud.

2. Получив доступ, они меняют привязанный адрес электронной почты к сервису iCloud и пароль.

3. В сервисе iCloud есть информация обо всех ваших устройствах и конечно же есть возможность блокировать их работу, что злоумышленники и делают. При этом Apple при блокировке устройства через iCloud позволяет задать сообщение, которое будет показано на заблокированном устройстве. В этом сообщении хакер указывает адрес, на который нужно написать, чтобы получить инструкции по оплате за разблокировку устройства.

4. Утрата доступа к данным и устройству является большой потерей для многих владельцев техники Apple, поэтому они достаточно быстро соглашаются на оплату.

Мошеннические интернет-магазины и сервисы. Это одна из самых простых схем мошенничества. На просторах Интернета существует множество мошеннических ресурсов, где предлагают купить товары по очень привлекательным ценам, но с предварительной оплатой. Многие пользователи идут на риск и в итоге остаются и без товаров, и без денег. Часто отмечаются всплески появления таких мошеннических ресурсов перед большими праздниками.

Кроме мошеннических магазинов есть и *сезонные мошенничества*. Например, перед сезоном отпусков появляются туристические операторы, сервисы по продаже авиабилетов или бронированию отелей. Иногда такие сервисы даже присылают вам электронные билеты и квитанции о брони отелей, но они являются поддельными, что выясняется в самый последний момент.

Глава 4. Кибертерроризм и киберэкстремизм

§ 1. Истоки использования террористами и экстремистами сети Интернет[1]

Международное джихадистское движение очень рано начало использовать Интернет в своих целях. В 1991 г. был создан сайт Исламского медиацентра (IMC), который, не ограничиваясь пропагандой, давал начинающим боевикам практические советы и рекомендации. Хотя Исламский медиацентр поддерживал джихадистов, он не являлся органом «Аль-Каиды». Только в феврале 2000 г. эта организация

[1] В данном параграфе использованы материалы исследования М. Экера, доктора политических наук Университета Пантеон-Сорбонна (2015).

обзавелась собственным веб-сайтом (сначала maalemaljihad.com, а с марта 2001 г. — alneada.com). Несколько недель спустя «Аль-Каида» основала свое информационное агентство Ас-Сахаб, выпускающее различные аудио- и видеоматериалы.

После теракта 11 сентября 2001 г. Соединенные Штаты и их союзники начали операцию «Несокрушимая свобода» (Enduring Freedom). Через несколько недель режим талибов был свергнут, а «Аль-Каида» лишилась базы в Афганистане. Тренировочные лагеря были уничтожены, многие боевики захвачены или убиты. У. бен Ладен и А. аз-Завахири спаслись бегством. Ради выживания «Аль-Каида» была вынуждена менять структуру: на месте централизованной организации с иерархическим устройством возникло множество разрозненных группировок. В 2004 г. в Ираке открылся первый филиал «Аль-Каиды», подчиненный А. М. аз-Заркави. Децентрализация затронула и Интернет: в октябре 2006 г., вскоре после образования в Ираке организации «Исламское государство», был создан фонд медиапродукции «Аль-Фуркан». По той же модели события развиваются и в других филиалах: например, отделение «Аль-Каиды» в странах Магриба (AQMI) обзавелось собственным медиацентром под названием «Институт медиапродукции Аль-Андалуз».

Децентрализации ресурсов джихадистов в Сети способствуют и два других фактора.

Во-первых, у крупных сайтов, связанных с «Аль-Каидой», шаткое положение. Они постоянно становятся объектами контртеррористических действий и судебных преследований со стороны правительственных служб или общественных активистов. Так, в 2002 г. сайт alneada.com прекратил деятельность, чтобы позднее открыться под другим именем. Дублирование контента с помощью создания «зеркальных» ресурсов и частичной передачи данных на сайты сторонников джихадистов рассматривается ими как один из способов укрепить присутствие в Интернете.

Во-вторых, децентрализации способствует эволюция интернет-технологий. Переход от модели Интернета web 1.0 к модели web 2.0 во многом обусловлен развитием технологий, сделавших возможным публикацию контента в режиме онлайн. Ряд пользователей цифровых ресурсов, которые ранее довольствовались лишь чтением веб-сайтов, созданных другими, сами превращаются в создателей веб-контента. Радикальные организации тоже не остались в стороне: джихадизм в его новой версии 2.0 распространяется главным образом через постоянно множащиеся исламистские форумы и социальные сети, где все более заметно присутствие групп, объединенных идеями джихада. К началу 2015 г. около 46 тыс. аккаунтов в твиттере принадлежало членам «Исламского государства» (ИГИЛ) или их сторонникам.

§ 2. Пропаганда как главный метод, используемый террористами и экстремистами в Интернете[1]

Одним из основных направлений использования Интернета террористами является пропагандистская деятельность. Обычно пропагандистские материалы имеют форму мультимедийных коммуникаций, содержащих идеологические или практические наставления, разъяснения, оправдания или рекламу террористической деятельности. К ним могут относиться виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, а также электронные игры, разрабатываемые террористическими организациями или их сторонниками. Тем не менее являющиеся террористической пропагандой материалы, в отличие от законной публичной защиты той или иной точки зрения, нередко носят характер субъективных оценок.

Поощрение насилия является обычной темой связанной с терроризмом пропаганды. Широкая область влияния распространяемой через Интернет информации в геометрической прогрессии увеличивает аудиторию, на которую она может воздействовать. Кроме того, возможность непосредственного распространения контента через Интернет уменьшает зависимость от традиционных каналов связи, таких как новостные агентства, которые могут предпринять соответствующие шаги в целях самостоятельной оценки достоверности предоставленной информации либо отредактировать и опустить аспекты, считающиеся недопустимо провокационными. Интернет-пропаганда также может включать такой контент, как видеосюжеты о насильственных террористических актах или создаваемые террористическими организациями видеоигры, имитирующие акты терроризма и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста.

Пропаганда экстремистской риторики с призывами к насильственным действиям также является общей тенденцией для все более широкого круга интернет-платформ, предоставляющих услуги по размещению информационного наполнения, создаваемого пользователями. Материалы, которые прежде могли распространяться лично или с помощью физических носителей, таких как компакт-диски (CD) и цифровые видеодиски (DVD), среди относительно ограниченной аудитории, все чаще переносятся в Интернет. Такие материалы могут распространяться с использованием широкого спектра инструментальных средств, таких, соответственно, как специализированные веб-сайты, целевые виртуальные чат-группы и чат-форумы, онлайн-журналы, платформы социальных сетей типа Twitter и Facebook, а также популярные видео- и файлообменные веб-сайты типа YouTube и Rapidshare. Использование служб индексации, таких как поисковые системы Интернета, также упрощает процесс нахождения и извлечения информационного наполнения, связанного с терроризмом.

[1] В параграфе приводятся положения доклада Управления ООН по наркотикам и преступности «Использование Интернета в террористических целях» (2013), а также материалы М. Экера.

Основная угроза, которую несет с собой террористическая пропаганда, связана с тем, как она используется и в каких целях распространяется. Распространяемая через Интернет террористическая пропаганда охватывает ряд задач и аудиторий. Она может быть приспособлена для воздействия, в частности, на потенциальных или реальных сторонников или противников той или иной организации или общих экстремистских воззрений, на прямых или косвенных жертв террористических актов или на международное сообщество в целом либо какую-то его часть. Ориентированная на потенциальных или реальных сторонников пропаганда может быть направлена на вербовку, радикализацию и подстрекательство к терроризму путем рассылки сообщений с выражением чувств гордости, удовлетворения от успехов и преданности экстремистским целям. Она также может использоваться в качестве доказательства успешного проведения террористических актов для тех, кто обеспечивает соответствующую финансовую поддержку.

Наиболее острую реакцию в мире вызывает стратегия устрашения, практикуемая ИГИЛ, и в частности казни граждан западных стран. Запись казней осуществляется профессионально. Члены ИГИЛ взяли на вооружение некоторые приемы из «исламистских снафф-фильмов» (термин «snaff movies», появившийся в 1970-е гг. в США, обозначает фильмы, в которых показаны реальные пытки или убийства) А. М. аль-Заркави более чем 10-летней давности. Например, во многих сценах заложники одеты в оранжевую робу, что должно напоминать об узниках американской базы Гуантанамо. Впрочем, между прежними фильмами и материалами ИГИЛ есть существенные отличия. Прежде всего в видеороликах ИГИЛ больше режиссуры: часто применяются спецэффекты, крупные планы и замедленная съемка. Кроме того, видеозаписей казней теперь больше, чем когда-либо раньше. «Исламское государство» разделило свою территорию на несколько административных единиц (вилайетов), каждая из которых распространяет собственные записи с казнями. В результате каждый месяц появляется несколько новых видео с экзекуциями. Среди них сравнительно редко можно видеть казни граждан запад-

ных стран, потому что у ИГИЛ не так много заложников с Запада. Зато очень часто показывают расправы над сирийскими солдатами, над «предателями», «коллаборационистами», «шпионами» и «неверными». И, наконец, применяемые ИГИЛ методы устрашения отличаются неслыханной жестокостью. Наряду с обезглавливанием практикуется сжигание заживо, сбрасывание с крыш домов, забивание камнями, утопление, а также использование в качестве палачей несовершеннолетних. Некоторые видеозаписи подобного рода предназначены для западной аудитории, другие — для региональной, третьи — для локальной (сирийских и иракских солдат, преследуемых меньшинств, суннитского населения, вынужденного подчиняться ИГИЛ). В зависимости об обстоятельств видеозаписи призваны либо внушать людям мысль о необходимости военного вмешательства, либо добиваться подчинения.

Однако ИГИЛ позиционирует себя не только как террористическая организация, но и как партизанское движение, действующее в соответствии с классическими принципами ведения революционной войны (как их в свое время определял Мао Цзэдун). ИГИЛ не пренебрегает идеологической (вернее, политико-религиозной) работой с населением. Ряд пропагандистских видео посвящен открытию религиозных центров, распространяющих исламское учение (дават), или деятельности проповедников, объезжающих подотчетные им округа. Мы видим, как отряды «религиозной полиции» объясняют населению, что дозволено исламскими нормами (в трактовке ИГИЛ), а что запрещено. Некоторые социальные действия, направленные на то, чтобы «завоевать сердца и умы» людей, также снимаются на камеру и выкладываются в Сеть. На других роликах показаны действия ИГИЛ по подрыву враждебных политико-административных структур, такие, например, как убийство политиков или представителей сил правопорядка. Кроме того, ИГИЛ стремится продемонстрировать свою боеспособность и умение вести партизанскую войну. Такие видеоролики часто бывают очень короткими и нечеткими: обычно вылазки боевиков снимают на камеру GoPro. Однако иногда используется гораздо более сложная аппаратура. Некоторые кадры сняты с помощью беспилотников. Часто применяются спецэффекты. Сошлемся, например, на серию видеоматериалов центра «Аль-Фуркан медиа», известную как «Clanging of Swords», а также на 60-минутный «документальный» фильм «Flames of War», выпущенный медиацентром «Аль-Хаят» в сентябре 2014 г. Сцены боев, сделанные как будто по образцу компьютерных игр типа «Call of Duty», пользуются особой популярностью и входят в число материалов, которыми наиболее интенсивно обмениваются в Twitter джихадисты. На некоторых видеороликах запечатлены действия террористов-смертников — таким образом воздается дань уважения «мученикам веры».

Кроме того, пропаганда ИГИЛ направлена на то, чтобы предстать в глазах мировой общественности полноправным государством. Особенно подчеркиваются суверенные права ИГИЛ. Например, право иметь собственную армию: ИГИЛ демонстрирует наличие таких видов оружия, которые может себе позволить только независимое государство. Речь идет об истребителях-бомбардировщиках, ракетных установках. Возможно, ИГИЛ и не умеет обращаться с высокотехнологичным оружием. Однако его наличие должно внушить зрителю образ мощной организации и представление о ее скорой победе в борьбе с правительственными силами. Другой функцией суверенного государства, которую хочет присвоить себе ИГИЛ, является правосудие. Джихадисты утверждают, что, требуя строгого соблюдения законов шариата, они, по сути, создают «государство исламского права». Сцены с казнями, с распятием людей, с отрезанием голов воспринимаются в мире как настоящее варварство. Однако для части местного населения казни символизируют определенную форму правосудия. Хотя такое правосудие далеко от западных норм, оно позволяет членам ИГИЛ претендовать на роль восстановителя закона и порядка посреди царящего вокруг хаоса.

Известно, например, что, когда иорданский пилот, принимавший участие в бомбардировке Сирии в составе сил международной коалиции, был взят в плен и сожжен заживо, прежде чем расправиться с пленным, представители ИГИЛ консультировались с местным населением относительно методов казни, а в Twitter шло активное обсуждение данного вопроса. Стремясь казаться настоящим государством, ИГИЛ объявило о намерении чеканить собственную монету. В пятом номере англоязычного журнала «Дабик» и первом номере франкоязычного «Дар аль-Салам» представлены изображения новых золотых динаров, прообразом которых послужили монеты, имевшие хождение в VII в., во времена халифа Абд аль-Малика.

Кроме того, ИГИЛ стремится выполнять административные функции. В социальных сетях регулярно появляются фотоснимки официальных документов, которые выпускает «Исламское государство» (удостоверения личности, свидетельства о рождении, дипломы и т. д.). Некоторые видеоролики призваны продемонстрировать заботу «Исламского государства» о населении подконтрольных ему территорий: ИГИЛ строит новые дороги, восстанавливает электроснабжение и т. д. Именно этой стороне деятельности ИГИЛ посвящен «документальный фильм», снятый британским журналистом Дж. Кэнтли (который находится у исламистов в заложниках) в Алеппо и распро-

страненный «Аль-Хаятом» в феврале 2015 г. Зрители видят мукомольный завод, узнают о системе исламского образования, внедренной ИГИЛ.

В основе подобной пропаганды лежит особая идеология, «джихадистский салафизм». Он представляет собой политико-религиозное учение, которое призывает к неукоснительному следованию шариатским нормам на территориях с мусульманским населением и стиранию установленных западными державами государственных границ ради возрождения исламского халифата. Адепты такой революционной идеологии (конечной целью объявляется свержение существующего порядка и замена его новым, пусть даже новый «порядок» обернется хаосом) считают идеалом ислам VII в., а всю последующую его эволюцию рассматривают как отклонение от истинного пути.

С точки зрения идеологии «Аль-Каида» и ИГИЛ близки друг другу, несмотря на конфликт между их лидерами и кровопролитные столкновения отрядов «Исламского государства» с «Фронтом ан-Нусра». Игиловцы постоянно ссылаются на У. бен Ладена как на высший авторитет; обе организации ставят целью установление исламского халифата и объединение уммы. Однако их представления о том, когда эти цели могут быть достигнуты, разнятся. Для «Аль-Каиды» провозглашение исламского халифата остается отдаленной перспективой, о которой можно думать только по окончании борьбы, в то время как «Исламское государство» создавало исламский халифат летом 2014 г., стремясь придать джихадистскому движению новое дыхание.

Это событие сопровождалось мощной пропагандистской кампанией по отмене границ, доставшихся в наследство от соглашений Сайкса — Пико, и по объединению уммы. Отголоски кампании можно увидеть в видеозаписях казней сирийских солдат, выложенных в Сеть в ноябре 2014 г., где показано, как два десятка игиловцев перерезают жертвам горло. Палачами, совершившими это жуткое деяние, были представители разных стран (в казни участвовали гражданин Франции М. Ошар и британский подданный «Джихади Джон»). Нет сомнений, что целью было продемонстрировать миру, какое влияние имеет ИГИЛ на представителей разных государств.

§ 3. Вербовка, подстрекательство и радикализация новых членов террористических и экстремистских организаций через Интернет

Вербовка. Интернет может использоваться не только в качестве средства для публикации экстремистской риторики и видеоматериалов, но и как способ установления отношений с теми, кто наиболее склонен поддаваться на целенаправленную пропаганду, и поиска их

поддержки. Террористические организации все чаще используют пропаганду, распространяемую через такие платформы, как защищенные паролем веб-сайты и чат-группы ограниченного доступа в Интернете, в качестве средства тайной вербовки. Совокупная аудитория Интернета обеспечивает террористическим организациям и их сторонникам глобальный резерв потенциальных новобранцев. Интернет-форумы ограниченного доступа становятся для новообращенных тем местом, где они могут узнать о террористических организациях и предложить им свою поддержку, а также приступить к непосредственным действиям, чтобы способствовать террористическим целям. Использование технологических барьеров для доступа к платформам, на которых осуществляется вербовка, кроме того, усложняет процесс отслеживания сотрудниками разведки и правоохранительных органов связанной с терроризмом деятельности.

Террористическая пропаганда нередко специально рассчитана на то, чтобы быть притягательной для уязвимых и маргинализованных групп общества. В процессе вербовки и радикализации террористы, как правило, играют на имеющихся у человека ощущениях несправедливости, изоляции или унижения. Пропаганда может также быть адаптирована таким образом, чтобы учитывать демографические факторы, например возраст или пол, социальные или экономические обстоятельства.

Интернет может служить особенно эффективным средством вербовки несовершеннолетних, которые составляют значительную часть пользователей. Распространяемые через Интернет в целях вербовки несовершеннолетних пропагандистские материалы могут принимать формы мультфильмов, популярных музыкальных видеозаписей или компьютерных игр. Тактика, применяемая на веб-сайтах, которые поддерживаются террористическими организациями или их сообщниками в целях вербовки несовершеннолетних, включает использование смеси мультфильмов и рассказов для детей с сообщениями, в которых поощряются и прославляются террористические акты, такие как миссия террористов-смертников. Аналогичным образом некоторые террористические организации разрабатывают действующие в онлайновом режиме видеоигры, предназначенные для использования в качестве инструментов вербовки и обучения новичков. Такие игры могут служить средством пропаганды применения насилия в отношении государства или видных политических деятелей, предлагая награду за виртуальный успех, и могут выпускаться на разных языках в целях привлечения более широкого круга поклонников.

Подстрекательство. В то время как ведение пропагандистской деятельности само по себе обычно не запрещается, использование про-

паганды террористами для подстрекательства к актам терроризма во многих государствах — членах ООН считается противозаконным. В Интернете имеется множество материалов и возможностей для загрузки, редактирования и распространения информационного наполнения, которое может рассматриваться как незаконное прославление террористических актов или подстрекательство к их совершению.

Важно подчеркнуть различие между простой пропагандой и материалами, имеющими целью подстрекательство к актам терроризма. В ряде государств-членов, для того чтобы привлечь кого-либо к ответственности за подстрекательство к терроризму, требуется доказать наличие необходимого умысла и прямой причинно-следственной связи между предполагаемой пропагандой и реальным заговором или осуществлением террористического акта.

Радикализация. Вербовка, радикализация и подстрекательство к терроризму могут рассматриваться как элементы в цепочке тесно связанных между собой явлений. Радикализация относится прежде всего к процессу идеологической обработки, который нередко сопутствует превращению завербованных неофитов в лиц, преисполненных решимости совершать насильственные действия на основе экстремистских идеологий. Процесс радикализации часто включает использование пропаганды, которая на протяжении длительного времени ведется либо посредством личного общения, либо через Интернет. Продолжительность и эффективность пропаганды и других используемых средств убеждения варьируется в зависимости от конкретных обстоятельств и отношений.

§ 4. Финансирование террористических и экстремистских организаций посредством Интернета

Террористические организации и их сторонники также могут использовать Интернет для финансирования террористических актов. Методы, с помощью которых террористы используют Интернет для мобилизации и сбора средств и ресурсов, можно подразделить на четыре основные категории: прямые просьбы о пожертвованиях; электронная коммерция; использование действующих в Интернете платежных инструментов; посредничество благотворительных организаций.

В случае прямых обращений речь идет об использовании веб-сайтов, чат-групп, массовых рассылок и целенаправленных сообщений в целях передачи просьб о пожертвованиях от сторонников. Веб-сайты также могут использоваться в качестве интернет-магазинов, предлагающих сторонникам книги, аудио- и видеозаписи и другие товары. Платежные средства, предоставляемые в Интернете через специализированные веб-сайты или коммуникационные платформы, позволяют легко осуществлять электронный перевод средств между сторонами. Переводы средств нередко производятся с помощью электронных банковских переводов, кредитных карт или иных платежных средств, доступных через такие сервисы, как PayPal или Skype.

Онлайновые платежные средства также могут использоваться мошенническим путем с помощью таких приемов, как хищение личных данных, кражи кредитных карт, мошенничество с использованием электронных средств коммуникации, биржевое мошенничество, преступления против интеллектуальной собственности и мошенничество на аукционах. Примером использования незаконных доходов для финансирования террористических актов может служить дело «Соединенное Королевство против Юниса Цули». Прибыль от украденных кредитных карт была отмыта несколькими способами, включая перевод через электронную платежную систему e-gold («электронное золото»), которая была использована для пересылки средств транзитом через ряд стран, прежде чем они попали в пункт своего назначения. Отмытые деньги использовались как для финансирования зарегистрированных 180 веб-сайтов, на которых были размещены пропагандистские видеоматериалы движения «Аль-Каида», так и в целях приобретения снаряжения для террористической деятельности в ряде стран. Для незаконного получения примерно 1,6 млн ф. ст. на финансирование террористической деятельности были использованы около 1400 кредитных карт.

Финансовая поддержка, оказываемая, казалось бы, законным организациям, например благотворительным, также может быть перенаправлена на незаконные цели. Как известно, некоторые террористические организации создают подставные корпорации, маскируемые под благотворительные организации, чтобы ходатайствовать о предоставлении средств по электронным каналам. Эти организации могут утверждать, что поддерживают гуманитарные цели, тогда как на самом деле пожертвования используются для финансирования террористических актов. Примерами якобы благотворительных организаций, используемых в террористических целях, являются носящие безобидные названия «Беневоленс интернешнл фаундейшн», «Глоубал рилиф фаундейшн» и Фонд Палестины в целях оказания помощи и развития — все они пользовались полученными мошенническим путем средствами для финансирования террористических организаций на Ближнем Востоке. Террористы также могут внедряться в филиалы благотворительных организаций, которые используются ими в качестве прикрытия для распространения идеологии террористических организаций или для оказания материальной поддержки группам боевиков.

§ 5. Подготовка террористов и экстремистов в сети Интернет

В последние годы террористические и экстремистские организации все чаще прибегают к использованию Интернета в качестве альтернативной базы для подготовки террористов и экстремистов. Все более широкий спектр средств информации предоставляет платформы для распространения практических руководств в виде интерактивных учебных пособий, аудио- и видеоклипов, информационных сообщений и рекомендаций. На этих интернет-платформах также публикуются подробные инструкции, часто в легкодоступном мультимедийном формате и на нескольких языках, по вопросам о том, например, как вступить в террористические организации, как изготовить взрывчатые боеприпасы, огнестрельное и другие виды оружия или опасные материалы и как планировать и осуществлять террористические акты. Эти платформы выступают в качестве виртуальной учебной базы. Кроме того, они используются, в частности, для обмена специальными методами, приемами или оперативными знаниями в целях совершения террористических актов.

Например, журнал Inspire является интернет-изданием, предположительно выпускаемым «Аль-Каидой» на Аравийском полуострове с заявленной целью дать мусульманам возможность готовиться к участию в джихаде у себя на дому. В нем публикуется большое количество идеологических материалов, направленных на поощрение терроризма, в том числе заявления, приписываемые У. бен Ладену, шейху А. аз-Завахири и другим известным деятелям «Аль-Каиды». В осенний выпуск 2010 г. были включены практические учебные материалы о том, как приспособить полноприводной автомобиль для проведения акта нападения на представителей общественности и как боевик-одиночка может осуществить неизбирательное нападение, стреляя из огнестрельного оружия с высокого здания. В этом издании даже имелось предложение относительно того, какой город следует избрать для такой атаки, чтобы повысить шансы убить членов правительства.

В имеющихся в Интернете учебных материалах предлагаются инструменты для содействия контрразведывательной деятельности и неавторизованному доступу к компьютерным данным, а также для повышения уровня защищенности противозаконных коммуникаций и деятельности в Сети путем использования доступных средств шифрования и методов анонимизации. Интерактивный характер интернет-платформ помогает создать чувство общности между людьми, живущими в разных географических регионах и имеющими различное происхождение, способствуя созданию сетей для обмена материалами учебного и тактического характера.

§ 6. Планирование террористических операций и экстремистских акций через сеть Интернет

При планировании террористических актов обычно имеет место дистанционный обмен сообщениями между несколькими сторонами.

Через Интернет также могут предприниматься шаги для определения потенциальной цели нападения и наиболее эффективных средств достижения цели террористического акта. Эти подготовительные шаги могут варьироваться от получения инструкций в отношении рекомендуемых методов нападения до сбора информации о предполагаемой цели из открытых и иных источников. Открываемые в Интернете возможности для преодоления расстояний и границ и огромное количество имеющейся в киберпространстве общедоступной информации делают Интернет ключевым инструментом планирования террористических актов.

Секретная связь в процессе подготовки. Самой главной функцией Интернета является обеспечение удобства передачи информации. Террористы становятся все более искушенными в использовании коммуникационных технологий в целях обмена анонимными сообщениями, связанными с планированием террористических актов. В качестве электронного, или виртуального, «тайника» для доставки сообщений террористы могут использовать обычные учетные записи абонентов электронной почты в Интернете. Речь идет о создании черновика сообщения, который остается неотправленным и, соответственно, оставляет минимум электронных следов, но может быть доступен с любого интернет-терминала в любой точке мира для ряда лиц, обладающих соответствующим паролем.

Также существует множество более сложных технологий, которые затрудняют распознавание отправителя, получателя или содержания интернет-сообщений. В Интернете легкодоступны для скачивания средства шифрования и программное обеспечение для анонимизации трафика. Эти инструментальные средства способны, в частности, замаскировать уникальный адрес по протоколу Интернет (IP), идентифицирующий каждое используемое для доступа в Интернет устройство и его местоположение, перенаправить интернет-сообщения через один или несколько серверов в юрисдикции с более низкими уровнями правоприменения в отношении террористической деятельности и (или) зашифровать данные трафика, относящиеся к посещаемым веб-сайтам. Также может использоваться стеганография.

Общедоступная информация. Организации и частные лица нередко публикуют в Интернете значительные объемы информации. В случае организаций это отчасти может быть вызвано желанием создать рек-

ламу своей деятельности и оптимизировать свое взаимодействие с общественностью. Через поисковые системы в Интернете, способные каталогизировать и извлекать не имеющую надлежащей защиты информацию с миллионов веб-сайтов, можно также получить доступ к некоторому количеству секретной информации, которая может использоваться террористами в противозаконных целях. Кроме того, интерактивный доступ к подробной логистической информации, такой как производимые в режиме реального времени съемки замкнутых телевизионных сетей, а также такие прикладные программы, как Google Earth, предназначенная для физических лиц и в основном используемая ими в законных целях, могут использоваться в неблаговидных целях теми, кто стремится воспользоваться преимуществами свободного доступа к получаемым с помощью искусственных спутников Земли изображениям, картам и информации о местности и сооружениях в высоком разрешении для ведения рекогносцировки потенциальных целей с удаленных компьютерных терминалов.

В частности, в эпоху популярных социальных медиасетей, таких как Facebook, Twitter, YouTube, Flickr и блогерские платформы, частные лица также публикуют в Интернете добровольно или по неосмотрительности беспрецедентное количество конфиденциальной информации. Намерение лиц, распространяющих такие материалы, состоит в том, чтобы донести до своей аудитории новости или иные свежие сведения в информационных или социальных целях. Однако часть этой информации может быть незаконно присвоена и использована в интересах преступной деятельности.

Террористические атаки в Мумбаи в 2008 г., в результате которых погибли 164 человека, показали, что Интернет сыграл важнейшую роль на этапе планирования и во время осуществления этих атак. На этапе планирования террористы провели виртуальную разведку объектов с помощью сетевой картографической службы, что позволило им очень точно организовать выполнение задачи, включая определение входов и выходов, которые должны были использоваться на основных объектах атак, и выяснение географических координат объектов, которые были введены в программы устройств GPS.

В процессе самой атаки террористы использовали свои телефоны Blackberry для передачи информации исполнителям, а также для получения инструкций и новой информации от них, например данных о местоположении заложников, о международной реакции на атаки и о действиях полиции. Исполнители использовали каналы VoIP для того, чтобы скрыть свое местоположение. Уровень тактических деталей, о которых становилось известно из социальных сетей, таких как Twitter или Flickr, мгновенно обеспечивал террористам дополнительную ситуационную осведомленность. Опасаясь, что такая информация может помочь террористам, индийские власти даже сами опубликовали твит с просьбой немедленно прекратить публикацию прямых сообщений в Twitter о событиях в Мумбаи.

§ 7. Сбор разведывательных данных террористами и экстремистами через сеть Интернет

Террористы, подобные организаторам терактов в Мумбаи, могут анализировать данные, поступающие из разных источников, и способны сводить их к полезной тактической информации. Такая информация может поступать как из открытых источников, например из сервисов схем расположения или туристических сайтов, так и с сайтов социальных сетей, защищенных паролями. Суть в том, что террористы собирают, казалось бы, безобидную информацию из многочисленных источников, в результате получая полную картину, дающую им тактическую ситуационную осведомленность.

Признавая вероятность злоупотребления на первый взгляд незначительной личной информацией, американская армия в 2012 г. предупредила военнослужащих об опасности «геомаркировки». В частности, армейские руководители указали, что смартфоны имеют встроенные устройства GPS, а на сделанных с их помощью фотографиях автоматически выставляются показатели широты и долготы места, где они были сняты, и эта информация может дать преимущества террористам, обладающим необходимым программным обеспечением. Аналогичным образом платформы социальных сетей теперь дают пользователям возможность указывать их местоположение при публикации сообщений. В сочетании с последней информацией о ежедневных действиях человека и часто небрежным отношением многих пользователей социальных сетей к принятию «друзей» или к раскрытию собственных частных данных платформы социальных сетей потенциально дают террористам возможность эксплуатировать интернет-пользователей для собственной выгоды.

§ 8. Инструментарий, используемый террористами и экстремистами при совершении преступлений, связанных с Интернетом

Технологический прогресс предоставляет в распоряжение террористов множество современных средств, с помощью которых они могут злонамеренно использовать Интернет в противозаконных целях. Для эффективного расследования деятельности, связанной с использованием Интернета, требуются сочетание традиционных методов ведения следствия, знание доступных инструментальных средств для

осуществления незаконной деятельности через Интернет и разработка практических методик в целях выявления, задержания и судебного преследования виновных в совершении таких актов.

Связь на основе интернет-технологий

Протокол передачи голоса через Интернет. За последнее десятилетие выросла популярность приложений, позволяющих пользователям общаться в реальном времени с помощью системы телефонии по протоколу передачи голоса через Интернет (VoIP), видеочата или текстового чата, и они стали более совершенными. В некоторых из этих приложений предусмотрены продвинутые функции по обмену информацией, например позволяющие пользователям совместно работать над файлами или дающие им возможность в реальном времени на удалении наблюдать за экранной деятельностью другого пользователя. Система VoIP, в частности, все чаще используется в качестве эффективного средства общения через Интернет. К числу широко известных провайдеров услуг системы VoIP относятся Skype и Vonage, работа которых основана на преобразовании аналогового звука в сжатый цифровой формат, что позволяет передавать через Интернет пакеты цифровой информации, используя соединения по относительно узкополосным каналам.

Поскольку система телефонии VoIP предполагает передачу пакетов цифровых данных, а не аналоговых сигналов, а провайдеры услуг, как правило, формируют выставляемые абонентам счета за пользование Интернетом, исходя из совокупного объема данных, счета за межкомпьютерные вызовы в системе VoIP не выставляются за каждый отдельный вызов, как это делается в традиционных системах мобильной и фиксированной телефонной связи. Такое различие в практике выставления счетов может существенно воздействовать на ход расследований, касающихся обменов сообщениями с использованием системы VoIP, так как при этом правоохранительным органам труднее подтвердить такие обмены маркерами, указывающими, например, на время вызова и местонахождение участников. Однако в качестве средств для установления личности виновных в противозаконной деятельности в Интернете могут также служить другие показатели, такие как время передачи и объем трафика данных в Интернете. Кроме того, в то время как источник и адрес назначения обычных телефонных звонков можно проследить через коммутаторы стационарных линий или антенные мачты сотовой связи, где остаются следы геолокации, обмены сообщениями, осуществляемые с помощью целиком основанной на интернет-технологиях системы VoIP, например через беспроводные сети, могут создавать проблемы для ведущих

расследование. Дополнительными осложняющими факторами, связанными с использованием технологии VoIP, могут стать в том числе маршрутизация вызовов через одноранговые сети и шифрование адресов вызова.

Электронная почта. Службы электронной почты на базе интернет-технологий также предоставляют в распоряжение террористов средство скрытого обмена сообщениями, которое может быть злонамеренно использовано в противозаконных целях. Сообщения электронной почты, отправляемые сторонами друг другу, как правило, содержат ряд элементов, которые могут быть полезны для следствия. Типичное письмо электронной почты может состоять из заголовка конверта, заголовка сообщения, тела сообщения и любых связанных с ним вложений. Хотя в зависимости от настроек применяемого программного обеспечения отображаться может лишь сокращенный вариант заголовка конверта, полный заголовок конверта обычно содержит сведения о каждом почтовом сервере, через который сообщение проходило на пути к конечному адресату, а также информацию об IP-адресе отправителя. Информация, содержащаяся в заголовке конверта, менее подвержена фальсификации (хотя и не застрахована от нее), чем информация в заголовках сообщений, которая обычно состоит из сведений, предоставляемых пользователем, в таких полях, как «Кому», «От кого», «Обратный путь», «Дата» и «Время», фигурирующих на устройстве, с которого отправляется сообщение.

Одним из часто используемых методов для сокращения количества остающихся между сторонами электронных следов и, следовательно, вероятности обнаружения является поддержание связи путем сохранения неотправленных сообщений в папке черновиков учетной записи абонента электронной почты. Тогда эта информация становится доступной ряду лиц, использующих для доступа к этой учетной записи общий пароль. В целях избежания обнаружения могут также приниматься дополнительные меры, такие как использование для доступа к соответствующим проектам сообщений общественных терминалов удаленного доступа, например в интернет-кафе. Данный метод был использован в связи со взрывами бомб террористами в Мадриде в 2004 г.

Кроме того, при передаче сообщений по электронной почте могут использоваться методы анонимизации, например маскирующие IP-адрес, принадлежащий отправителю электронной почты. Могут также использоваться анонимные почтовые серверы, которые удаляют идентифицирующую информацию из заголовка конверта, прежде чем переслать его на последующий почтовый сервер.

Онлайновые службы обмена сообщениями и дискуссионные форумы. Онлайновые службы доставки и отправления сообщений и дискуссионные форумы являются дополнительным средством обмена сообщениями в реальном времени с различной степенью потенциальной анонимности. Онлайновые службы обмена сообщениями обычно позволяют поддерживать двустороннюю связь, тогда как дискуссионные форумы обеспечивают свободное общение между группами лиц. Регистрация в онлайновых службах обмена сообщениями, как правило, осуществляется на основе непроверенной информации, предоставленной пользователем; однако отдельные интернет-службы также фиксируют использовавшиеся при регистрации IP-адреса, которые могут быть затребованы правоохранительными органами на условиях соблюдения применимых правовых гарантий. Сообщения обычно идентифицируются по уникальному псевдониму, который может назначаться на постоянной основе при регистрации или ограничиваться использованием в ходе конкретного сеанса работы в Интернете. Провайдеры услуг, как правило, не записывают информацию, которой стороны обмениваются во время сеанса работы в онлайновых службах обмена сообщениями, и, следовательно, по завершении сеанса работы в Интернете эта информация может оказаться недоступной для извлечения, а для ее восстановления потребуется прибегнуть к судебной экспертизе жесткого диска одного из участников.

Для того чтобы способствовать развитию чувства общности в мировом масштабе, террористические организации и сочувствующие им могут использовать защищенные паролем дискуссионные форумы. Публикуемые в дискуссионных форумах сообщения могут быть подвержены более тщательному мониторингу и учету со стороны провайдеров услуг, чем двусторонние обмены сообщениями, что повышает потенциальную вероятность получения документальных доказательств в ходе расследований. В ряде юрисдикций сотрудникам правоохранительных органов в связи с проведением расследования разрешается на определенных условиях тайно зарегистрироваться и участвовать под псевдонимом в обсуждениях, которые ведутся в дискуссионных группах.

Файлообменные сети и «облачные» технологии. Файлообменные сайты, такие как Rapidshare, Dropbox или Fileshare, дают сторонам возможность без труда загружать мультимедийные файлы через Интернет, делиться ими, находить и получать доступ к ним. Методы шифрования и анонимизации, используемые в связи с другими формами интернет-связи, в той же мере применимы к файлам, обмен которыми осуществляется с помощью в том числе пиринговых технологий (P2P) и протокола передачи файлов (FTP). Некоторые файлообменные сети могут вести журналы передачи данных или сохранять информацию о платежах, которые могут представлять интерес в контексте расследования.

«Облачные» вычисления — это сервис, который предоставляет пользователям удаленный доступ к программам и данным, хранящимся или выполняемым на серверах данных, принадлежащих третьим сторонам. Как и обмен файлами, «облачные» вычисления представляют собой удобное средство для безопасного хранения, обмена и распространения материалов в Интернете. Использование «облачных» технологий для доступа к информации, хранимой на удаленных носителях, помогает сократить объем данных, хранящихся локально на отдельных устройствах, и, соответственно, уменьшить возможности получения потенциальных доказательств в связи с расследованиями, касающимися использования Интернета в террористических целях.

Серверы данных, используемые для оказания этих услуг, также могут физически находиться в иной юрисдикции, чем зарегистрированный пользователь, с иными уровнями регулирования и возможностями правоприменения. Поэтому для получения ключевых улик в целях проведения судебного разбирательства может быть необходима тесная координация с местными правоохранительными органами.

Методы шифрования данных и сохранения анонимности

Шифрованием данных называется защита цифровой информации от раскрытия путем преобразования ее в криптограмму с использованием математических алгоритмов и ключа шифрования, чтобы она была понятна только намеченному получателю. Средства шифрования могут быть реализованы на аппаратной или программной основе или на основе сочетания того и другого. После шифрования для получения доступа к информации могут потребоваться пароль, фраза-пароль, «программный ключ» или аппаратное средство доступа либо определенное их сочетание. Шифрование может применяться в отношении данных «в состоянии покоя», содержащихся в памяти таких устройств, как жесткие диски компьютеров, флэш-память и смартфоны, а также в отношении данных «в пути», передаваемых через Интернет, например с помощью VoIP-телефонии и сообщений электронной почты.

К числу примеров распространенных программных средств шифрования можно отнести службы, интегрированные в компьютерные операционные системы или прикладные программы, а также такие

автономные программы, как Pretty Good Privacy и WinZip. В рамках дела, слушавшегося в Бразилии, на основе международного сотрудничества и обмена информацией было начато расследование в отношении подозреваемого, которого обвиняли в том, что он участвовал в деятельности джихадистского веб-сайта, связанного с признанной террористической организацией, а именно с «Аль-Каидой», выступал там в качестве модератора и контролировал эту деятельность. На этом веб-сайте размещались видеоматериалы, тексты и обращения боевиков-экстремистов руководящего уровня в переводе на английский язык, чтобы охватить более широкую аудиторию; он также использовался для проведения акций по сбору средств и пропагандистских кампаний расистской направленности.

Полицейская операция, которая привела к задержанию этого подозреваемого, имела целью захватить подозреваемого врасплох, когда он был подключен к Интернету и активно занимался деятельностью, связанной с веб-сайтом. Задержав его в момент, когда его компьютер был включен и соответствующие файлы были открыты, следователи смогли обойтись без симметричных криптографических ключей и других средств шифрования и обеспечения безопасности, использовавшихся подозреваемым и его сообщниками. Таким образом, следователям удалось получить доступ к цифровому контенту, который в противном случае мог бы оказаться недоступным или им было бы труднее овладеть, если бы компьютер был выключен и защищен.

Сокрытие деятельности в Интернете или личности причастных к ней пользователей также может осуществляться с помощью передовых технологий, включая маскирование IP-адреса источника, ложное представление под IP-адресом другой системы или перенаправление интернет-трафика на скрытый IP-адрес. Прокси-серверы позволяют пользователям скрытно выполнять косвенные запросы к другим сетевым службам. Некоторые прокси-серверы позволяют сконфигурировать браузер пользователя таким образом, чтобы трафик браузера автоматически направлялся через прокси-сервер. Прокси-сервер отправляет запросы на сетевые услуги от имени пользователя, а затем задает маршрут доставки результатов снова через прокси-сервер. Использование прокси-серверов может способствовать достижению тех или иных уровней анонимности. Прокси-сервер способен скрыть личность пользователя, выполняя запросы на сетевые услуги без раскрытия IP-адреса, с которого исходит запрос, или намеренно предоставляя искаженный IP-адрес источника. Например, такие прикладные программы, как The Onion Router, могут использоваться в целях защиты анонимности пользователей путем автоматического перенаправления деятельности в Интернете через сеть прокси-серверов, для того чтобы замаскировать ее первоначальный источник. Перенаправление сетевого трафика через несколько прокси-серверов, потенциально находящихся в разных юрисдикциях, повышает степень трудности точного установления отправителя исходящих сообщений.

В качестве альтернативы подозреваемый может взломать IP-адрес законной организации и просматривать информацию в Интернете, используя взломанный адрес. Любые следы такой деятельности были бы связаны с IP-адресом пострадавшей организации. Через взломанный компьютер подозреваемый также может получать доступ к тем или иным веб-сайтам или хранить на взломанных веб-сайтах вредоносные программы (используемые, например, для получения сведений о кредитных картах или другой личной финансовой информации) в целях избежания опознания.

Существует множество компьютерных программ, которые могут использоваться для сокрытия или шифрования данных, передаваемых через Интернет в противозаконных целях. Эти программы могут включать использование такого программного обеспечения, как «Камуфляж», для маскировки информации с помощью стеганографии или шифрование и парольную защиту файлов с помощью такого программного обеспечения, как WinZip. Может также использоваться многоуровневая защита данных. Например, программа «Камуфляж» позволяет скрывать файлы путем их скремблирования (от англ.: scramble — шифровать) и последующего прикрепления в конце файла-носителя по своему выбору. Файл-носитель сохраняет свои первоначальные свойства, но используется в качестве носителя для хранения или передачи скрытого файла. Данное программное обеспечение может применяться к широкому диапазону типов файлов. Скрытый файл, однако, можно обнаружить путем анализа первичных данных файла, который покажет наличие прикрепленного скрытого файла.

Европол в докладах 2015—2016 гг. сообщает о все ширящемся использовании террористами и экстремистами изощренных систем шифрования, включая *шифрованные коммуникаторы*. Террористические и экстремистские группы в настоящее время используют различного рода шифрованные приложения, в основном для коммуникаций, а также проведения финансовых операций. Существуют также свидетельства, полученные правоохранительными органами стран Южной Азии, что террористы во время атак на объекты городской инфраструктуры активно пользуются шифрованными мессенджерами и шифрованными скайпоподобными платформами.

Известно также, что некоторые террористические группы, принадлежащие к европейской периферии ИГИЛ, в P2P-сетях размещали заказы на разработку шифрованных приложений, позволяющих в открытой сети опознавать членов организации, присутствующих в общедоступных социальных сетях.

Уязвимым местом террористов является невысокий на сегодняшний день уровень компьютерной грамотности и осведомленности в высоких технологиях. Однако представляется, что данная ситуация в ближайшие два-три года изменится, и террористы, базирующиеся преимущественно в странах Ближнего Востока, откроют для себя мир кибероружия.

Уже сегодня террористы широко используют сеть Tor для монетизации террористических трофеев, рекрутинга и обучения неофитов. Также известно, что более двух третей граждан стран ЕС, отправившихся воевать на Ближний Восток в составе террористических подразделений, как минимум несколько раз посетили рекрутинговые и учебные ресурсы ИГИЛ в сети Tor.

Беспроводные технологии

Беспроводные сетевые технологии позволяют компьютерам и другим устройствам получать доступ в Интернет с помощью радиосигналов, а не через постоянное соединение, например по кабелю. Чтобы получить доступ к сети Wi-Fi, необходимо находиться на относительно небольшом расстоянии от сетевых ресурсов, которое зависит от силы беспроводного сигнала. Беспроводные сети могут быть сконфигурированы таким образом, чтобы позволялся открытый доступ в Интернет без регистрации, или же они могут быть защищены с использованием парольной фразы или различных уровней шифрования. Доступ к беспроводным сетям, зарегистрированным на физических лиц, предприятия или государственные структуры, нередко можно получить из общественных мест. Анонимный доступ к защищенным или незащищенным сетям Wi-Fi может позволять преступникам скрывать связь между их деятельностью в Интернете и идентифицирующей информацией.

Кроме того, в последние годы появился ряд провайдеров услуг, таких как Fon, которые позволяют зарегистрированным пользователям делиться частью пропускной способности своих домашних каналов связи Wi-Fi с другими абонентами в обмен на взаимный доступ к сетям Wi-Fi абонентов по всему миру. В ходе расследования осуществление деятельности в коллективно используемых сетях Wi-Fi существенно затрудняет процесс установления причастности к совершению

того или иного деяния единственного правонарушителя, который может быть идентифицирован.

Один из нестандартных методов связан с использованием программно определяемых высокочастотных радиоприемников с улучшенными рабочими характеристиками, конфигурируемых через компьютер. Таким образом не происходит обмена данными через сервер и не создается никаких журналов регистрации. Правоохранительным и разведывательным органам сложнее перехватывать сообщения, отправляемые с использованием данного метода, как в плане установления местонахождения передатчиков, так и в плане предсказания в реальном времени частоты, на которой передаются сообщения.

Использование террористами и экстремистами инструментов социальных сетей

Еще в 2011 г. появились сообщения, что 90% террористической и экстремистской деятельности в Интернете осуществляется с помощью инструментов социальных сетей. В настоящее время почти вся их деятельность ведется в условиях относительной открытости социальных сетей, а также в сети Yota. Террористы и экстремисты превратили дешевые и легкодоступные социальные сети в стратегическое средство для коммуникации, поддержания связей, подстрекательств, планирования и т. д. Сами по себе социальные сети потенциально могут действовать как фактор повышения боевой эффективности, увеличивающий организационные способности террористических и экстремистских организаций, их возможности по формированию общественных идей, а также как средство привлечения внимания потенциальных сторонников.

Инструменты сетей, которыми злоупотребляют террористы и экстремисты, включают:

— *тематические чаты*. Они позволяют не только «жителям» Интернета, негосударственным гуманитарным организациям, организациям гражданского общества, но и террористическим группам общаться с единомышленниками и сторонниками по всему миру, вербовать новых последователей и делиться информацией, почти не подвергаясь риску разоблачения властями. Например, среди террористов стал особенно популярен открытый сервис тематических чатов PalTalk, который включает голосовые и видеовозможности. Помимо цели получения поддержки тематические чаты также служат для распространения тактической информации среди «экспертов», поскольку в них даются прямые ответы на такие вопросы, как собрать бомбу или как взломать компьютерную систему;

— *блоги*. В докладе, подготовленном 304-м батальоном военной разведки армии США, подчеркивается, что такие блог-сервисы, как Twitter, могут стать для террористов эффективным инструментом координации атак, что было продемонстрировано во время атак 2008 г. в Мумбаи. В отчете также говорится о возможных сценариях использования террористами этого онлайн-формата, включая получение информации о местоположении потенциальных объектов атаки практически в режиме реального времени или, например, взлом страницы солдата и общение с другими солдатами от его имени;

— *сайты социальных сетей*. Виртуальные сообщества становятся все популярнее, особенно среди молодежи. Веб-сайты социальных сетей позволяют террористам обращаться к восприимчивой возрастной группе, которая может сочувствовать их идеям. Кроме того, многие пользователи социальных сетей неосторожно принимают запросы на включение в список «друзей», что может дать террористам возможность получить доступ к их личной информации. Также существуют различные террористические группы, имеющие открытые страницы на сайтах социальных сетей, где любой интересующийся может ознакомиться с размещенной там информацией, почитать дискуссии, посмотреть пропагандистские видеоролики и вступить в такую группу;

— *распространение видеоматериалов*. Террористы используют сетевые платформы, на которых размещаются и распространяются видеоматериалы. Помимо этого, в результате исследования, посвященного высказываниям и комментариям по поводу сетевых видеоматериалов, было установлено, что сетевые видеоматериалы получают глобальную аудиторию, особенно среди молодых зрителей, и такой террористический контент распространяется далеко за пределы своей предполагаемой основной базы поддержки.

Социальные сети, помимо прочего, служат средством распространения практических советов и рекомендаций по использованию всевозможного оружия. Уже не первый год существуют сайты, где можно найти подробные инструкции по различным формам ведения вооруженной борьбы. Некоторые составляют из таких материалов настоящие «энциклопедии» войны, насчитывающие по несколько сотен страниц; таковы, например, «Энциклопедия джихада» (mawsu' at al-jihad), «Большая энциклопедия оружия» (mawsu' at al-asliha al-kubra), «Энциклопедия военной подготовки» (mawsu' at al-i dad) и т. д.

Не остались в стороне и сетевые журналы. В 2003—2004 гг. приверженцы «Аль-Каиды» из Саудовской Аравии запустили интернет-журнал под названием «Лагерь Аль-Баттар» (mu' askar al-battar) с целью создать нечто вроде виртуального тренировочного лагеря для

джихадистов. В тот период тренировочные лагеря «Аль-Каиды» в Афганистане были уничтожены, и перед членами организации из Саудовской Аравии маячила перспектива ареста, поэтому об открытии реальных лагерей подготовки боевиков нельзя было и думать. Спустя несколько лет аравийское отделение «Аль-Каиды» (AQPA) инициировало выпуск англоязычного веб-журнала Inspire, где в некоторых статьях давались конкретные советы по организации терактов. Так, во втором номере журнала, вышедшем в свет осенью 2010 г., некто Яхья Ибрахим советует будущим джихадистам из западных стран начинать с простого, ибо попытки осуществить какую-нибудь сложную операцию имеют мало шансов на успех. Он рассматривает несколько возможных вариантов, вроде использования в качестве орудия смерти обыкновенного автомобиля, на котором начинающему джихадисту предлагается въехать в толпу людей[1]. Иногда ради большей наглядности подобные инструкции представлены в форме видеороликов. Так, в 2005 г. «Глобальный исламский медиафронт» выпустил видео, показывающее, как собирать и разбирать АК-47.

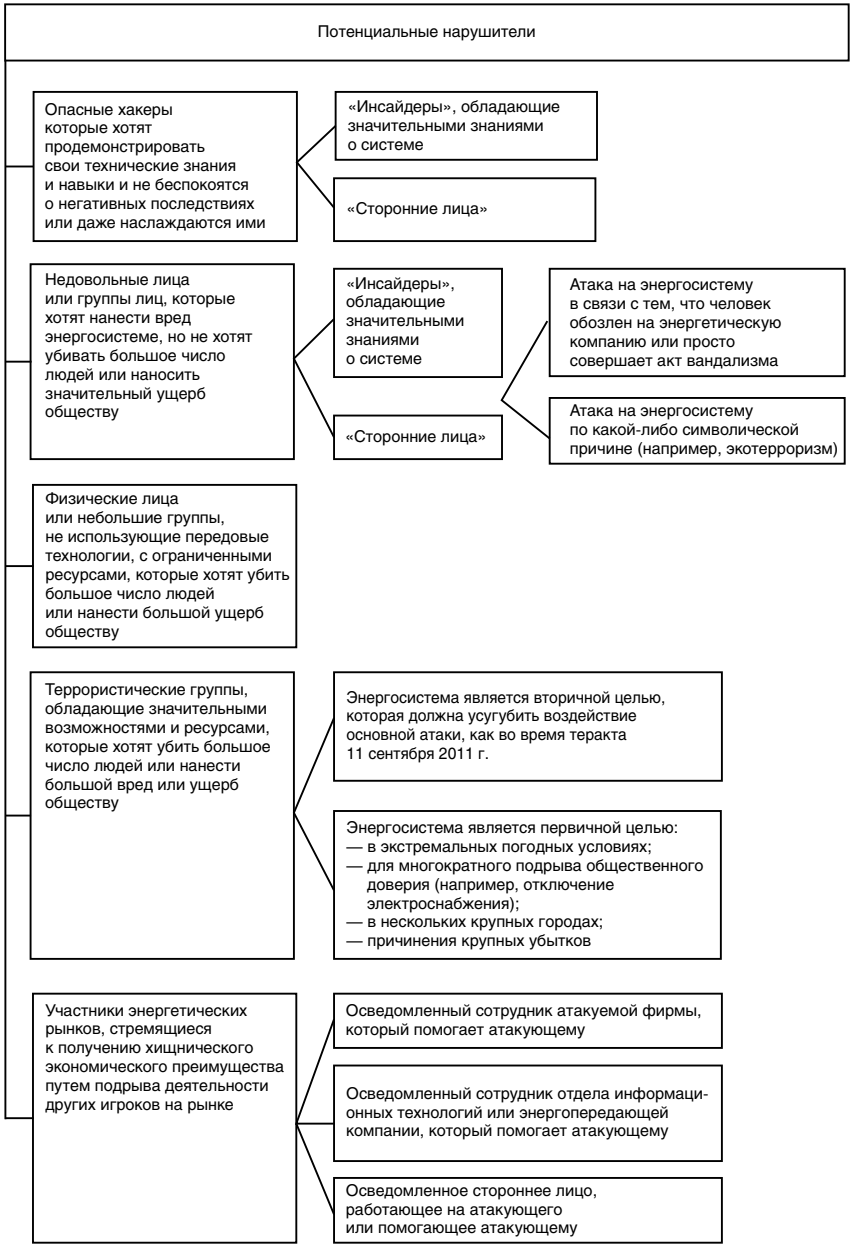
§ 9. Террористические угрозы в киберпространстве, направленные на важнейшие объекты инфраструктуры[2]

Как показали многочисленные нападения групп боевиков на наземные нефте- и газопроводы в таких странах, как Колумбия, Ирак и Нигерия, энергетические сети могут быть уязвимы для предварительно спланированных атак. Трубопроводные сети часто имеют протяженность тысячи километров, поэтому отслеживание их состояния становится непростой задачей, а значит, и надлежащее обеспечение их безопасности представляет собой сложный, дорогостоящий процесс.

В последние годы энергетическая цепь поставок стала более автоматизированной и, как следствие, более зависимой от компьютерных систем контроля. Это обеспечивает более эффективное и надежное функционирование современной энергетической инфраструктуры, но в то же время повышает уязвимость сети, поскольку современные сети становятся все более связанными друг с другом и все чаще управляются удаленно. Несмотря на то что использование открытых стандартов программного обеспечения позволяет снизить затраты на

[1] Как известно, такие уроки были усвоены и реализуются террористами в европейских городах с 2015 г.

[2] В параграфе использованы материалы Руководства по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства (ОБСЕ, 2013).



эксплуатацию сетей, оно также делает энергетическую сеть более уязвимой для кибератак, поскольку злоумышленники получают доступ к известному или открытому исходному коду, а значит, могут использовать его в собственных целях.

Представленная на рисунке классификация потенциальных нарушителей, которые могут атаковать энергетическую систему, взята из Руководства по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими из киберпространства.

Глава 5. Новые тенденции преступности эпохи третьей и четвертой промышленных революций

§ 1. Основные направления использования искусственного интеллекта криминальными сообществами[1]

В начале 2017 г. ФБР провело крупную конференцию, посвященную вопросам использования искусственного интеллекта правоохранительными органами и криминалом. На конференции было отмечено: данные Интерпола, Европола, ФБР и правоохранительных органов других стран, результаты исследований ведущих университетов позволяют говорить, что в настоящее время отсутствуют признаки целенаправленных усилий криминала по созданию собственных разработок в области искусственного интеллекта.

Это обстоятельство трактуется многими практиками следующим образом: в ближайшей перспективе ФБР и полиция, взяв на вооружение искусственный интеллект, получат решающее превосходство над киберпреступностью и другими видами организованного криминала.

Успешные преступники, работающие по-крупному в таких сферах, как финансы, крупномасштабная контрабанда, нелегальная купля-продажа интеллектуальной собственности и т. п., — люди предельно рациональные. На данном уровне разработок в области искусственного интеллекта у них нет необходимости привлекать внимание, вербуя в свои ряды команды наиболее продвинутых стартапов, за которыми охотятся военное и разведывательное сообщества, крупнейшие корпорации. Сегодня это не нужно. Почему?

[1] Более 70% внедрений в области искусственного интеллекта приходится на США и примерно 15% на Китай. Соответственно, основные примеры использования искусственного интеллекта криминалом можно почерпнуть из докладов и других источников, публикуемых правоохранительными структурами США (китайские источники более засекречены).

Прежде всего, стремясь минимизировать издержки и привлечь к развитию собственного продукта максимальное количество внешних, в значительной степени бесплатных, разработчиков, большинство ведущих производителей платформ искусственного интеллекта уже выпустили платформы с открытым кодом.

У киберкриминала есть из чего выбрать для создания собственных мощных платформ искусственного интеллекта. Практически все разработки искусственного интеллекта с открытым исходным кодом представляют собой контейнеры. Контейнер — это платформа, на которой при помощи API могут монтироваться любые сторонние программы, сервисы, базы данных и т. п. Если раньше каждый при создании собственной программы или сервиса должен был от начала до конца первоначально разработать алгоритмы, а затем, пользуясь тем или иным языком программирования, перевести их в код, то сегодня возможно создавать продукты и сервисы так же, как строители строят дом — из стандартных, доставленных на стройплощадку деталей.

Начиная с 2016 г. стремительно растет *сфера AIAS — искусственный интеллект как сервис*. Компании, разрабатывающие отдельные элементы искусственного интеллекта, и в первую очередь хранилища данных, алгоритмы глубокого обучения, алгоритмы нейронных сетей, включая глубокие, а также программы обработки естественного языка и многомерных расчетов, более чем в двух третях случаев предусматривают возможность использования их разработок через API. Более того, некоторые компании сегодня позволяют за относительно небольшую плату брать напрокат свое программное обеспечение в области искусственного интеллекта. Если в случае API при необходимости правоохранители могут установить характер использования программы, то при аренде такое невозможно.

Наконец, еще пять-семь лет назад в мире имелось 17 университетов, в которых студенты получали первоклассную подготовку в области исследований и практических разработок, связанных с искусственным интеллектом. В те времена правоохранители вполне могли держать на учете каждого человека, специализировавшегося в профессии с повышенным уровнем опасности для среды, и могли отслеживать его карьеру на протяжении всей жизни. Сегодня такой возможности больше нет. В Соединенных Штатах число университетов, обучающих компьютерным наукам на высоком уровне, увеличилось до 40, и подобного рода учебные заведения появились по всему миру. Образовалась целая отрасль онлайн-обучения. Сегодня для людей, обладающих необходимой начальной подготовкой, лучшие университеты

открыли бесплатные онлайн-курсы по всем компонентам искусственного интеллекта.

Изложенные факты косвенно указывают на активную подготовку криминала к овладению искусственным интеллектом. При этом криминал не собирается изобретать велосипед. Он озабочен тем, как научиться на нем ездить и выработать наиболее эффективные маршруты.

По мнению Интерпола и ФБР, использование искусственного интеллекта криминалом в Америке и других развитых странах в течение ближайших пяти лет будет иметь место в нескольких приоритетных сферах. Их объединяет наиболее благоприятное для криминала соотношение трех переменных: полученный преступный доход, совокупные приведенные издержки на подготовку, совершение и сокрытие преступления и уровень риска.

Основные направления использования искусственного интеллекта криминальными сообществами следующие.

1. Использование искусственного интеллекта для компрометации и имплантации вредоносного «софта» в платежные системы, в основном использующие протокол блокчейн и имеющие P2P-архитектуру.

Одноранговые платежные системы вытесняют процессинговые компании, и прежде всего за счет экономии издержек для клиентов. При этом по состоянию на 2016 г. из без малого 30 платежных сервисов, построенных на блокчейне, действующих в США, лишь семь удовлетворяли требованиям компьютерной безопасности. Соответственно, подсоединение к платежным сервисам и добавление к каждой транзакции примерно 0,1—0,3% принесет миллиардные доходы преступникам при отсутствии какого-либо риска.

Программы искусственного интеллекта в данном случае крайне важны. Они позволяют использовать методы глубокого обучения нейронных сетей для взлома и перепрограммирования платежных протоколов, построенных на блокчейне. Эксперименты, проведенные в Университете Санта-Фе и Дармурдском университете, показали, что программы искусственного интеллекта справляются с этой задачей эффективнее, чем люди-программисты. Уязвимость заключена в блокчейне. Он, как любой код, базируется на правилах и алгоритмах. Именно на них построены игры — от шахмат до покера, где искусственный интеллект победил человека.

2. На долю высокотехнологичного киберкриминала, извлекающего прибыль из торговых операций крупнейших финансовых институтов, приходится 40—50 млрд долл. США ежегодно. Это наиболее прибыльная, хотя и довольно рискованная сфера организованной киберпреступности.

Поскольку в последние несколько лет развернулась настоящая гонка финансовых вооружений, выражающаяся в совершенствовании всеми крупнейшими финансовыми институтами своих платформ на основе искусственного интеллекта, преступникам даже для того, чтобы хотя бы сохранить долю доходов, необходимо участвовать в этой гонке. В связи с этим использование ОПГ искусственного интеллекта для операций на финансовых рынках путем проникновения и компрометации торговых платформ не оставляет для криминала другой возможности, кроме как использовать лучшие решения с открытым кодом в сочетании с AIAS. В отличие от ситуации в платежном бизнесе, где в 2017—2020 гг. ожидается резкое увеличение размеров и доли преступных доходов в обороте платежных систем, в алгоритмическом трейдинге в краткосрочной перспективе доля преступников будет снижаться.

Есть основания полагать, что по мере развертывания технологической гонки интерес киберпреступников как внутри, так и вне США к интеллектуальной собственности будет только нарастать. Известно также, что для вскрытия сегодняшних мощных систем корпоративно-информационной безопасности все шире используются многофункциональные программы, в основе которых лежат самосовершенствующиеся алгоритмические модули. Подобные модули — это ключевой элемент искусственного интеллекта.

Сами руководители ФБР полагают, что Америка сегодня не готова к отпору хакерским группировкам, нацелившимся на интеллектуальную собственность, принадлежащую корпорациям, федеральному правительству и университетам.

3. В условиях технологической гонки внедрение новых продуктов, услуг и программ является императивом выживания. Понятно, что гораздо выгоднее купить украденную документацию, чертежи, программы, чем тратить огромные деньги на исследования и разработки. Совместное исследование Академии ФБР и фармацевтического гиганта Sanofi показало на примере Индии, что 1 долл. украденной интеллектуальной собственности в фармацевтике экономит производителям дженериков 17—20 долл. расходов на исследования и разработки.

Очевидно, что столь доходная отрасль является одним из ключевых кандидатов на использование искусственного интеллекта. Есть данные, что уже в настоящее время внутри корпоративных сетей лидеров американского хайтека и биотехнологий действуют многоцелевые и многофункциональные хакерские программные модули, построенные на основе самосовершенствующихся программ.

Указанные направления использования искусственного интеллекта преступниками очевидны. Они вытекают из применения к реальности тех критериев выбора сферы деятельности, которыми руководствуется организованная преступность во всем мире.

4. На первый взгляд четвертое направление многократно описано в фантастических романах и рассказах, а также легло в основу множества блокбастеров, начиная со знаменитого «Терминатора».

Идея использовать робота как орудие убийства — совершенно тривиальная. Первым человеком, погибшим от робота, стал американский рабочий С. Форд в 1970-е гг. Он работал на автоматизированном предприятии, выполнявшем покрасочные работы для автомобильной индустрии. В результате нарушения программы, отвечающей за координацию автоматических манипуляторов одного из роботов, последний вместо дверцы схватил за шею рабочего и удушил его. В 2016 г. произошло первое целенаправленное убийство с использованием робота. В палате интенсивной терапии госпиталя ордена иезуитов в Сан-Мигеле больной умер от подачи в капельницу смертоносного состава вместо предписанного лекарства. Полицейские не смогли бы обнаружить данное преступление, если бы не случайность. Программист, которого банда подрядила, чтобы взломать программу, управляющую автоматической раздачей лекарств, поделился информацией в одном из закрытых чатов. В нем присутствовал осведомитель городской полиции. Благодаря ему программист был задержан, а позднее прояснилась вся картина.

На открытых конференциях ФБР отмечалось, что в течение 2015—2016 гг. агенты под прикрытием и осведомители неоднократно сообщали, что преступные синдикаты прагматично-серьезно обсуждали различные варианты убийств, используя насыщенные электроникой автомобили, «умные дома», медицинские комплексы и т. п. Поскольку у преступников обычно мысли не расходятся со словом, а слово — с делом, вполне можно ожидать появления в Америке принципиально нового явления.

Правоохранители по всему миру всерьез готовятся к появлению подпольных синдикатов, специализирующихся на заказных высокотехнологичных убийствах, замаскированных под технические инциденты различного рода. Принимая во внимание объем рынка заказных убийств в Соединенных Штатах, составляющий около 2 млрд долл. в год, мы ожидаем появление такого сетевого синдиката, а скорее всего не одного, а нескольких, во временном интервале один-два года.

Главным инструментом подобных синдикатов могут стать не хакерские программы сами по себе, а искусственный интеллект. Тон-

кость здесь в следующем. Различного рода автоматизированные автономные системы в подавляющем большинстве управляются из единого вычислительного центра, функционирующего как искусственный интеллект. Это называется *роевым обучением*. Соответственно, подключиться и заместить команды одного искусственного интеллекта может только другой. Программисту это не под силу. Он будет распознан из-за большей медлительности и меньшей алгоритмичности действий и операций.

Кроме того, только искусственному интеллекту под силу замаскировать злонамеренное отключение или выполнение несанкционированных действий техническим отказом. Несмотря на некоторую экстравагантность, в ближайшее время данный преступный промысел может стать реальностью. Плохо то, что особенно на первом этапе подавляющая часть подобных убийств будет оставаться нераскрытыми. В отделах по борьбе с убийствами просто нет специалистов, способных на уровне профессионала разбираться в тонкостях нейронных сетей, глубокого обучения и активного тестирования.

Преступники не хуже университетских профессоров анализируют события и процессы и устанавливают причинно-следственные связи. Преступные организации понимают, что им не под силу разрушить и скомпрометировать информационные базы правоохранителей.

Однако прошлое не обязано повторяться в будущем. Если преступные сообщества не могут уничтожить базы правоохранителей, то они, очевидно, пойдут другим путем. В любой системе самый уязвимый фактор — это человек. Во всем мире правоохранители фиксируют попытки на «черном» рынке купить те или иные базы изображений с видеокамер, установленных в кафе, торговых центрах, рядом с полицейскими участками, зданиями ФБР и т. п. Это наводит на мысль, что преступники начали создание собственной базы данных с использованием примерно тех же решений искусственного интеллекта, что и правоохранительные органы. С учетом того, что объем их базы будет существенно меньше, ее вполне можно реализовать на платформах искусственного интеллекта с открытым кодом, соединив их с коммерчески доступными сервисами анализа связей, видео, текстов и т. п.

Преступники будут пытаться создать свои базы путем анализа потокового видео с мест, приближенных к зданиям правоохранительных органов. Прежде всего это база агентов под прикрытием и осведомителей.

Можно ожидать также попыток создания криминалом баз данных на сотрудников информационных центров полиции, т. е. людей, допущенных в «святая святых».

§ 2. Направления использования роботов криминальными и террористическими структурами

Вряд ли чешский писатель Карел Чапек, который в 1921 г. придумал слово «робот» (что на чешском означает «тяжелая работа», «крепостной») для описания мыслящей машины, мало отличимой от человека, мог предвидеть, что меньше чем через 100 лет тема робототехники станет одной из наиболее востребованных среди бизнес-сообщества, военных кругов, университетов и органов государственной власти, а теперь и криминологов.

В докладе «Угрозы и риски использования автономных автоматизированных систем и роботов преступностью, экстремистами и террористами», подготовленном в 2015 г. междисциплинарным коллективом исследователей из различных университетов США на базе MTI по заказу федеральных органов власти США, определены возможности, степени риска и разнообразие угроз использования робототехники преступниками, экстремистами и террористами[1].

В настоящее время в международном сообществе существует терминологический разнобой, связанный с применением таких категорий, как «автономные автоматизированные системы» и «роботы». Например, в документах ООН и Министерства обороны США используются в основном термины «автономные автоматизированные системы (ААС)» и «автономные смертоносные системы вооружений (АССВ)». В то же время бизнес, средства массовой информации в Соединенных Штатах и официальные документы НАТО и ЕС используют термины «роботы», «роботы-убийцы», «роботизированное оружие» и т. п.

При всей близости ААС и роботов они являются терминами, обозначающими несколько различные технические и программные устройства. Большинство специалистов в области информационных технологий и робототехники придерживаются следующей точки зрения: «ААС» являются более широким термином, чем «роботы»; ААС включают в себя программно-технические комплексы с различной степенью автоматизации; в свою очередь, роботы представляют собой высокоавтоматизированные ААС.

Продемонстрируем это на понятном для лиц, принимающих политические решения, примере. Так называемые беспилотные летающие аппараты (БПЛА), или дроны, без сомнения, с первых своих образцов должны быть отнесены к ААС. Однако нельзя забывать, что до последнего времени подавляющая часть дронов предполагала наличие оператора, который не только принимает решения о применении

[1] Подробнее см.: *Ларина Е., Овчинский В.* Роботы-убийцы против человечества. Киберапокалипсис сегодня. М., 2016.

вооружений, но и в отдельных случаях дистанционно пилотирует дрон. В этом случае конечно же ни о каком роботе речь идти не может. Такие дроны не являются роботами, хотя и представляют собой ААС.

Представляется, что теория автоматического управления уже к 60-м гг. прошлого века выработала эффективный критерий, позволяющий надежно выделять роботов в структуре ААС. Данным критерием является способ принятия решения, требующегося в тех случаях, когда перед программно-аппаратным комплексом встает необходимость сделать выбор из нескольких альтернатив. Любой программно-аппаратный комплекс независимо от своего функционального предназначения должен быть способен выполнять как минимум две операции: перемещаться в пространстве и реализовывать свою функцию, например эвакуации раненых, разминирования, получения информации, огневого поражения и т. п.

Соответственно, принципиально возможны четыре комбинации в принятии решений: первая — все решения дистанционно принимает оператор ААС; вторая — все решения принимаются программным комплексом ААС без участия человека; третья — решения относительно всех операций ААС могут приниматься как человеком, так и программным комплексом; четвертая — на различных стадиях и человек, и программный комплекс могут принимать решения, но решение человека или программного комплекса на каждой из операций имеет окончательный приоритет.

Без сомнения, к роботам можно отнести второй тип ААС и с некоторой натяжкой третий. Далее в тексте в тех случаях, когда будет использоваться специально термин «роботы», он будет использоваться в отношении ААС второго и третьего типов. Во всех остальных случаях термин «ААС» будет подразумевать все типы роботов.

Можно выделить следующие основные направления использования ААС и робототехники деструктивными организациями.

Разведка. До последнего времени использование радиотехнической, электронной, воздушной, подводной и иной технологически сложной разведки было прерогативой исключительно государственных структур, включая разведывательные службы, правоохранительные органы и т. п. В настоящее время положение дел коренным образом изменилось. Впервые в истории деструктивные организованные структуры получили возможность ведения разведки по своей технической сложности, а соответственно, и объему и качеству получаемой и обрабатываемой информации, не уступающей государственным структурам. В решающей степени это связано не только с распространением и развитием Интернета, но и с качественным скачком в ААС и робототехники. Если еще несколько лет назад БПЛА, оснащенный

универсальным разведывательным комплексом, включающим системы видеоразведки, наблюдения в инфракрасном диапазоне, средства перехвата телекоммуникационных сигналов, стоил 300—350 тыс. долл. США и изготавливался исключительно компаниями — подрядчиками Пентагона, то уже сегодня, а тем более завтра ситуация иная. В настоящее время такой комплекс может быть приобретен на легальном и нелегальном рынках любым платежеспособным клиентом, включая преступные и экстремистские структуры, менее чем за 50 тыс. долл. США. При этом изготовителями таких дронов-разведчиков-наблюдателей уже сегодня являются более 700 легальных компаний по всему миру, включая страны Азии, Африки и неизвестное число нелегальных производителей.

Также сегодня доступны для деструктивных структур передвижные наземные разведывательные комплексы, монтируемые на автомобили и маскируемые под внедорожники, минивэны, фургоны и т. п. Данные комплексы, которые (без цены автомобиля) можно приобрести в различных странах мира легально и на «черном» глобальном рынке, стоят от 15 до 30 тыс. долл. США. Они позволяют не только прослушивать информацию из закрытых помещений, используя акустические эффекты, но и снимать информацию с расположенных в зоне действия комплекса компьютеров, планшетов и т. п. В 2014 г. в Великобритании одной из преступных групп был заказан и использован разведывательный комплекс, который, будучи поставлен недалеко от банка-хранилища, позволял получать коды электронных банковских ячеек, снимая информацию при их открытии законопослушными клиентами.

Можно сделать прогноз, что в течение ближайших трех — пяти лет основная часть разведывательных комплексов, находящихся в руках деструктивных организаций, будет относиться к средствам воздушного и наземного базирования, соответственно, к дронам и разведывательным автомобилям. В более отдаленной перспективе следует ожидать освоение деструктивными структурами морских глубин и космического пространства.

Транспорт. Было бы удивительно, если бы преступные группы не воспользовались наиболее быстроразвивающимся сегментом военной и гражданской робототехники, а именно роботизированными транспортными средствами, не говоря уже о военном использовании автоматизированного транспорта для экспедиционных, эвакуационных и логистических нужд. По оценкам специалистов и бизнес-аналитиков, в автомобильной промышленности до 2020 г. не менее 25 производимых в развитых странах автомобилей будут иметь опцию автоводителя. Известно, что любая высокая технология имеет тройное применение — военное, гражданское и криминальное, поэтому

есть все основания полагать, что наиболее активно будут применять транспортных роботов террористы и преступные синдикаты.

Применительно к террористам данный тезис не нуждается в дополнительной аргументации. Террористические структуры, в том числе сетевого и роевого типа, уже сегодня имеют ресурсные технологические возможности, превосходящие потенциал многих государственных армий. В связи с этим террористы быстро и эффективно используют все виды вооружений и техники, которые применяются в современных армиях.

Что касается преступных транснациональных организаций, то использование транспортной робототехники позволяет им решить две важные задачи. С одной стороны, оно дает возможность разнообразить каналы доставки тех или иных грузов и свести к минимуму человеческий фактор в этом процессе. Последнее крайне важно. Например, по данным американских правоохранительных структур, не менее 70% случаев раскрытия преступлений и срыва поставок наркотиков в Соединенные Штаты связано с успешной агентурной работой или деятельностью агентов под прикрытием. Иными словами, чем больше роботов и меньше людей участвует в преступных акциях, тем сложнее силам правопорядка внедрить в преступные организации своих людей или завербовать там агентов.

С другой стороны, использование транспортной робототехники позволяет строить принципиально новые логистические системы. Согласно правительственным и неправительственным источникам в период 2000—2010 гг. всего 8% наркотрафика из Мексики и других латиноамериканских стран приходилось на воздушные перевозки. В 2011—2014 гг. эта доля возросла более чем в два раза. По оценкам специалистов, к 2020 г. не менее трети наркотиков будет доставляться по воздуху, прежде всего с использованием микродронов, летящих на небольшой высоте до 100—150 м, либо, наоборот, сверхвысоких дронов большей вместительности. В обоих случаях обнаружение таких дронов будет крайне затруднительным, особенно в условиях массового использования дронов в Соединенных Штатах как частными лицами, так и корпорациями. Если до недавнего времени более 80% зафиксированных дронов, пересекших американо-мексиканскую границу, не были идентифицированы как дроны, принадлежащие легальным организациям и частным лицам, то в ближайшем будущем ситуация коренным образом изменится. В воздухе будут барражировать множество дронов, принадлежащих законопослушным субъектам.

Бывший аналитик ФБР, а ныне сотрудник Google М. Гудман в книге «Будущее преступности»[1] отмечал, что еще в 2011 г. в Лас-Вегасе был представлен небольшой дистанционно управляемый самолет, имевший 11 антенн и оснащенный всеми возможными датчиками и камерами. Он получил название «WASP» и был специально разработан для того, чтобы перехватывать сигнал Wi-Fi всех, включая зашифрованные сети. Он был также оснащен небольшим бортовым сервером Linux, запускавшим различные хакерские устройства, включая словарь в 340 млн слов, используемый для взлома паролей. Камеры устройства позволяли вести панорамную съемку, а также съемку в инфракрасном излучении, т. е. снимать темную комнату за стеклом. Кроме того, устройство позволяло записывать все телефонные звонки в радиусе километра. Этот шпионский беспилотник можно было приобрести прямо на хакерском фестивале всего за 6 тыс. долл. США.

[1] *Goodman M.* Future Crimes. N. Y., 2015.

Гудман также пишет, что криминальные корпорации уже активно используют дроны для транспортировки наркотиков в Латинской Америке. Например, в одной из тюрем Сан-Пауло дроны использовались для доставки полкилограмма кокаина для заключенных с воли, при этом ежедневно. Подобные случаи зарегистрированы в Канаде и Австралии.

В 2014 г. в Мексике в одном из отдаленных районов столицы страны рядом с авиационным заводом компании «Бомбардье» благодаря агентурной разведке был раскрыт завод по сборке дронов различных конструкций, принадлежащих одному из наркосиндикатов. В ходе расследования выяснилось, что наркосиндикат подкупил руководство завода «Бомбардье» и оно, сетуя на низкую квалификацию мексиканских рабочих, списывало в брак до 15% продукции. Из деталей «Бомбардье» собирали в основном транспортные и наблюдательные дроны. При этом в ходе обыска Агентству по борьбе с наркотиками США (DEA) на заводе удалось захватить конструкторскую документацию, свидетельствующую о том, что наркосиндикат готовился наладить производство боевых дронов прикрытия. Эти дроны должны были сопровождать транспортные дроны и выводить из строя полицейские автомобили, оснащенные радарами воздушного наблюдения.

Начиная с 2012 г. DEA задокументировало сотни случаев использования наркосиндикатами дронов для переброски наркотиков, причем только в 7% случаев удалось пресечь доставку грузов.

Уголовные умельцы используют дроны так же, как платформы для размещения огнестрельного оружия. YouTube изобилует не только любительскими съемками действия самодельных боевых дронов, но и учебными фильмами по созданию такого рода боевых дронов. В сети Tor открыт даже видеоканал «Высокие преступные технологии», где для скачивания размещаются учебные фильмы по созданию боевых дронов, роботов и т. п.

Самый страшный сценарий связан с размещением на беспилотниках биологического, химического или радиологического оружия. Например, за 120 долл. США можно сегодня купить дрон с радиусом действия 10 км со смонтированным разбрызгивателем сельскохозяйственных удобрений. Комплект предусматривает, что режим разбрызгивания включается через пульт дистанционного управления при достижении определенного пункта GPS-навигации. Если вместо удобрения загрузить какой-то смертоносный вирус, то... (даже думать не хочется о том, что может произойти).

Дроны могут быть целенаправленно использованы не только против масс, но и против конкретных лиц. В конце 2013 г. канцлер Германии А. Меркель во время митинга в Дрездене была ошеломлена дроном, который сел к ее ногам на сцене. Атака была проведена Партией пиратов, которая заявила, что осуществила эту акцию, чтобы убедиться, что канцлер понимает, что говорит, когда произносит слова: «В Германии должны быть законодательно разрешены дроны для наблюдения за гражданами». Хотя никто не пострадал, все мировые агентства растиражировали эту новость. А на YouTube она превратилась в вирусное видео.

В октябре 2016 г. портал Life.ru сообщил, что российским спецслужбам стало известно, что в штабе ИГИЛ создано подразделение высокотехнологичных терактов. Боевики делают ставку на малые управляемые летательные системы: дроны с самодельными бомбами планируется использовать для терактов в странах Европы. Эксперты видят в этой тактике серьезную опасность: несмотря на несовершенство дронов и других боевых роботов, это направление терроризма будет только развиваться.

Руководит отделом некий У. Ар-Рифаи. В подразделении есть помощник, директор по обучению боевиков-одиночек, директор по планированию терактов, финансовый директор и другие специалисты, как рассказал источник в спецслужбах. Именно это подразделение готовит теракты с использованием малых управляемых летательных систем — дронов. Так боевики собираются обезопасить самих террористов и участников террористического подполья от гибели.

Перед командой, которая отвечает за разработку высокотехнологичных терактов, стоит задача: акций проводить больше, но самих террористов привлекать к ним меньше. Лучше всего, если это будут одиночные операторы. Это связано с тем, что в последние годы абсолютное большинство планируемых терактов с участием смертников было сорвано заранее, поэтому и делается ставка на одиночек.

Схема работы будет примерной такой: по указанию главаря оператор-одиночка снарядит дрон самодельной бомбой, привезет его к месту акции, запустит и будет управлять им дистанционно, как пояснил источник в спецслужбах.

Есть информация, что боевики ИГИЛ планируют обкатать высокотехнологичные теракты в странах Европы. Дроны будут заряжены самодельными бомбами или отравляющими веществами и управляться дистанционно. Когда аппарат окажется в людном месте или на объекте, бомба будет приведена в действие.

Дроны в руках террористов могут представлять опасность как для мест массового скопления людей, так и для различных охраняемых объектов. Даже если дрон заметят и собьют, то при падении он все равно успеет наделать бед. В нем может быть настроена система автоматического подрыва бомбы.

Кроме того, появление и быстрый прогресс транспортных дронов резко расширит географию преступности, особенно в части наркотрафика, контрабанды и, возможно, рынка торговли человеческими органами. В настоящее время в условиях крайне затруднительной логистики из многих районов традиционного выращивания наркокультур типа Бирмы, районов Афганистана, вовлеченных в военные действия, регионов Центральной Азии, принадлежащих постсоветскому пространству, и т. п. крайне затратно доставлять наркотики. Преступным синдикатам приходится нести высокие логистические издержки, связанные со сложностью и рисками доставки.

Уже имеющиеся в настоящее время транспортные роботизированные средства воздушного, наземного и подводного базирования позволяют недорого доставить любой относительно компактный груз из любой точки мира в любую точку мира. Известно, что в 2014 г. возобновлены крупномасштабные поставки высококачественных наркотиков из районов «Золотого треугольника». В логистике используются БПЛА и шагающие наземные транспортные средства.

В настоящее время в качестве транспортных средств наиболее широко используются дроны. Все чаще преступные группы заказывают шагающие транспортные средства. Известно также о разработке недорогих, доступных для любого коммерческого пользователя подводных беспилотных роботизированных транспортных устройств.

Роботы-коммандос. Роботы-коммандос являются гибридом разведывательных и транспортных робототехнических систем, оснащенных средствами выполнения и других целевых функций. Например, такие роботы способны взбираться по вертикальным поверхностям, бесшумно проникать в закрытые помещения и т. п. До настоящего времени считалось, что такими роботами обладают специальные подразделения армий США, Великобритании и Израиля. Известно так-

же, что близится к завершению производство аналогичных систем для вооруженных сил России, Китая и Южной Кореи.

Однако в конце 2014 г. британским тележурналистом в ходе боев между курдскими формированиями (Пешмерга) и боевиками ИГИЛ в окрестностях города Кабани на сирийско-турецкой границе удалось заснять двух роботов-коммандос, используемых ИГИЛ. Нет сомнения, что террористические организации различной локации в ближайшие годы получат в свое распоряжение роботов-коммандос.

Также можно прогнозировать по мере снижения их стоимости использование подобных робототехнических систем и преступными группами. В ближайшие годы это вряд ли произойдет, поскольку такого типа системы интересны прежде всего не для транснациональной, а для локальной, городской, уличной преступности. Она может использовать подобных роботов для проведения грабежей, нападений на квартиры и т. п. В настоящее время каждый робот-коммандос стоит до полумиллиона долларов. Снижение цены в 10 раз, когда они станут выгодными для уличной преступности, произойдет около 2020 г. или позже.

Боевые роботы. Не только в электронных и печатных СМИ, но и в правительственных документах их называют роботами-убийцами. Роботами-убийцами являются воздушные, наземные и водные и подводные системы, оснащенные боевым компонентом. До последнего времени, как правило, использование термина «робот» для этих устройств носило в подавляющем большинстве случаев некорректный характер. Вплоть до 2013 г. практически все системы, оснащенные боевым компонентом, предполагали участие человека в качестве оператора. Именно персонал в вооруженных силах США принимает решения о выборе цели и нанесении летального или нелетального удара. С 2014 г., согласно имеющимся данным, на вооружение «Цхакал» (Армии обороны Израиля) поступили не боевые ААС, а боевые роботы (в том терминологическом смысле, о котором говорилось выше).

Исходя из логики и истории развития вооружений, можно практически со 100%-ной вероятностью предсказать, что появление того или иного вида и типа оружия у любого внешнеполитического актора мгновенно переводит потенциальные возможности других акторов в состояние актуализации. То есть после того, как одна страна ставит на вооружение новый тип боевой техники, другие страны, располагающие соответствующим технологическим потенциалом, тут же мобилизуют его для производства аналогичных типов вооружений.

На конференции по борьбе с терроризмом, проходившей в октябре 2016 г. в Лондоне, было заявлено, что к 2025 г. в армии США будет больше боевых роботов, чем людей. США пытаются «действовать на

опережение», поставив под ружье в течение следующих нескольких лет тысячи солдат-роботов.

Большинство прототипов боевых роботов разрабатывалось Агентством перспективных оборонных исследований DARPA. Оно также занималось разработкой «суперсолдата» — человека, получившего с помощью средств кибернетики повышенные физические и умственные способности. Эти «улучшения» включают использование имплантатов мозга, которые, как надеются в DARPA, позволят «суперсолдатам» мысленно общаться друг с другом.

В ходе конференции было также отмечено, что в марте 2016 г. DARPA завершило проект создания автономного необитаемого корабля, предназначенного для выполнения различных задач, в том числе слежения за подводными лодками противника. Boeing как главный подрядчик Пентагона в апреле 2016 г. закончил разработку необитаемой подводной лодки, способной выполнять как исследовательские, так и боевые задачи. Другие компании, не имеющие отношения к военно-промышленному комплексу США, также занимаются разработкой автономных судов. Компания Rolls-Royce в июне 2016 г. объявила о планах создания «корабля-призрака» для транспортировки торговых грузов. DARPA также финансирует гражданские робототехнические проекты, например разработку крошечных летающих роботов, которые придут на замену находящихся под угрозой исчезновения популяций пчел.

Сегодня достигнуты большие успехи в миниатюризации роботов. Не только государственные, но и коммерческие структуры уже могут приобрести робота размером с большого жука, оснащенного видеокамерой, способной снимать не только днем, но и ночью, микрофоном, устройством дистанционной передачи на расстояние до 5 км звука и изображения и, естественно, устройствами для передвижения. В американские спецподразделения уже поступили робошмели, способные действовать в наиболее агрессивных средах, быть незаметными, проникать в здания, оснащенные пуленепробиваемыми стеклами, внутри не только фотографировать, но и поражать террористов.

В 2013—2014 гг. произошел подлинный прорыв в робототехнике, когда стало возможным создание роев боевых и гражданских роботов. Этот рой в своей деятельности имитирует поведение пчел, муравьев, стаи птиц. Используя передовые решения в области «облачной» коллективной памяти, распределенной вычислительной мощности и модульные конструкции, эти системы могут не только координировать деятельность и самообучаться друг у друга, но и собираться из маленьких устройств в крупные единые комплексы. В настоящее время производятся системы, ориентированные на поисково-спасательные,

военные и экологические операции. Значительный прогресс был достигнут в создании роевых роботов для разведки. В середине 2014 г. исследователи из Гарвардского университета создали разведывательный рой, включающий более тысячи крошечных роботов размером с цент, которые смогли собрать большой объем информации на одной из наиболее охраняемых и защищенных баз ВВС США на территории страны.

В 2014 г. завершилось создание первых двух модификаций боевых роев. Один рой предусматривает достижение объекта в качестве отдельных необнаруживаемых мини-структур со сборкой непосредственно над объектом атаки. После того как осуществляется сборка крупного боевого беспилотника из мини-роботов, этот беспилотник, нафаршированный смертоносным грузом, осуществляет атаку на объект.

В мае 2017 г. американские СМИ сообщили, что ученые уже создали роботизированных насекомых для борьбы с терроризмом. Батальоны роботизированных насекомых будут действовать более скрытно, чем любой беспилотник. Роботы-насекомые будут использоваться военными и разведывательными службами США. Современные технологии позволяют создать роботов, имитирующих движение насекомых. Они смогут выслеживать террористов, собирать необходимые доказательства и данные.

Стрекозы были выбраны в качестве основы, поскольку они распространены практически по всему миру и не вызовут подозрений. Каждый робот имеет «рюкзак», в котором находится система передовой навигации для сбора энергии и оптической стимуляции. Роботизированные насекомые также могут быть использованы в сельском хозяйстве. Они смогут опылять растения, если действий пчел окажется недостаточно.

Последнее обстоятельство весьма заманчиво для террористов, готовящих применение биологического оружия.

В 2015 г. инженеры из Научно-исследовательской лаборатории ВМС США представили рой мини-дронов. Беспилотники под названием «цикады» способны выполнять ряд важных функций во время боевых действий, при этом каждый из них умещается на человеческой ладони.

Главная особенность «цикад» заключается в том, что их будет настолько много, что враг не сможет устранить их всех.

Название роя дронов «CICADA» также является акронимом к словосочетанию Covert Autonomous Disposable Aircraft, т. е. «скрытые автономные одноразовые воздушные суда». Роботов спроектировали специально таким образом, чтобы они были меньше, дешевле и проще в конструкции, чем любые аналоги. Однако при этом они в состоянии справляться с основными военными задачами, стоящими перед беспилотниками.

Стоимость прототипа составила 1 тыс. долл. США за штуку, однако ее можно сократить и до 250 долл. У дронов отсутствуют двигатели, а вся конструкция состоит из 10 частей и внешне напоминает бумажный самолетик. Спущенные с военного самолета, воздушного шара или крупного беспилотника «цикады» будут ориентироваться по GPS и двигаться в направлении заранее заданных координат.

Ученые уже провели первые полевые испытания разработки в Юме (штат Аризона): дроны были выпущены с самолета на высоте 17,5 тыс. м и пролетели почти 18 км, прежде чем приземлиться в пределах 4,5 м от своей цели. Испытания также показали, что «цикады» способны развивать скорость до 74 км/ч и передвигаться практически бесшумно.

Со стороны рой таких дронов выглядит, стаей птиц, летящих к земле. Их очень трудно заметить и тем более идентифицировать как военный объект.

Во время испытаний беспилотники были оснащены датчиками, транслирующими информацию о температуре окружающей среды, влажности воздуха и давлении. К корпусу «цикад» можно прикрепить буквально любые датчики, в том числе и легкие мини-микрофоны.

«Цикады» похожи на роботизированных почтовых голубей: их отправляют на задание, и они летят туда, а возвращаются с новой информацией. Если оснастить дронов микрофонами и сейсмическими детекторами, то они смогут определить, где и в каком направлении движутся вражеские транспортные средства, а также с какой скоростью они едут. «Цикад» можно оснастить магнитными датчиками, чтобы они смогли следить за передвижениями подводных лодок противника и перехватывать коммуникации. В будущем можно будет дополнить дроны и функцией съемки.

Одним из самых главных преимуществ новых дронов является их повышенная прочность. Несмотря на то что выглядят «цикады» словно бумажные самолетики, они могут падать с 10-километровой высоты, врезаться в гравий, асфальт и песок и оставаться полностью работоспособными.

Возможности «цикад» выходят далеко за пределы военных операций. Дроны также могут использовать синоптики и метеорологи, например, для прогнозирования торнадо по показаниям температуры, давления и влажности.

Естественно, что новая разработка не останется незамеченной преступными и террористическими структурами.

«Групповая робототехника» нацелена на разработку разных технологий в управлении многочисленными группами роботов, которые, взаимодействуя во всех рамках определенного плана, выполняют совместными усилиями и сложные задачи. У ученых из Шеффилдского университета имеется ряд наработок в этой уникальной области и в области автоматического программирования, которые использованы на практике для точного управления 700 роботами из уже имеющегося в их распоряжении роя из 900 роботов, который является одним из самых многочисленных в мире.

Разрабатывая данный метод, исследователи использовали теорию диспетчерского управления (supervisory control), которая позволяет устранить весь человеческий фактор и избежать даже возникновения связанных с этим простых ошибок. Для описания всех задач используется специализированная простая программа, позволяющая в доступном и простом для понимания графическом виде представить задачу, которую требуется выполнить роботам.

Эксперименты, проведенные с роем всех роботов, показали ученым, что каждый из 600 роботов принимал свои собственные личные независимые решения для выполнения определенных и точных действий. При этом некоторое количество роботов самостоятельно даже объединялось в логически простые группы тогда, когда возможностей отдельно взятых роботов было недостаточно для выполнения простой текущей задачи.

Группа ученых из Гарвардского университета в 2016 г. представила рой из 1024 роботов, которые способны к самоорганизации. Размер робота сопоставим с размером монетки. Конструкция робота — это три тонкие ножки-палочки и два моторчика, с помощью которых устройство, благодаря вибрации, может перемещаться. Но главное — роботы могут «общаться» друг с другом.

Взаимодействие осуществляется посредством ИК-излучения и сигналов состояния, которое определяется цветом светодиода. Также у каждого есть датчик измерения освещенности. Набор этих средств коммуникации позволяет килоботам (название происходит от числа 1024) самостоятельно образовывать различные 2D-фигуры: «звезда», «гаечный ключ», буква «k».

Ученые и раньше пытались создать самоорганизующиеся системы из роботов, однако их число в рое не превышало до этого 100 единиц. Чтобы создать рой из большего числа, ученым пришлось кардинальным образом пересмотреть устройство отдельного робота и способы взаимодействия роботов друг с другом.

Нужно было, например, придумать, как зарядить тысячу килоботов или одновременно перепрограммировать их на выполнение новой задачи. Очевидно, что делать это вручную, нажимая кнопку на каждом роботе, не представлялось возможным. Решение тем не менее было найдено. Теперь зарядка килоботов происходит посредством их расположения между двумя проводящими поверхностями. А перепрограммирование осуществляется беспроводным способом. Информация об эксперименте поступает на контроллер, расположенный сверху килобота.

Одним из важных достижений разработчиков является создание алгоритма, который позволяет устройствам даже с очень ограниченными возможностями, но способным к коммуникации самоорганизовываться и создавать фигуры, необходимые пользователю.

Любопытно, что в алгоритме предусмотрен и сценарий взаимопомощи. Если во время выполнения задания какой-то из роботов выйдет из строя, его подменит работающий «коллега».

Обычно роботы сделаны из твердых материалов. Но уже появились и другие — эластичные, как резина. Над мягкими роботами, в частности, работают в лабораториях Гарвардского университета США. В 2016 г. ученые продемонстрировали публике изделие Х-образной формы, которое протискивалось в искусственные узкие щели, созданные на его пути. Робот преодолевал препятствие волнообразными движениями наподобие того, как пролезает в щель под забором кошка.

Используемый материал — это обычный эластомер, т. е. высокоэластичный полимер. Еще одно преимущество мягких роботов — простота и дешевизна производства. Так, пластиковые формы для отливки силиконовых частей гарвардские инженеры изготовили с помощью трехмерного принтера. Жидкий эластомер заливается в формы, выдерживается час при температуре 70°С — и деталь готова.

Чтобы изготовить такой же по конструкции, но вдвое больший по размерам прототип, уйдут не месяцы и даже не недели, а всего несколько дней. Ученым из института Криппса в Калифорнии удалось создать робота-медузу из силикона и... сердца крысы, — похожего на цветок с восемью лепестками-лопастями. На специальный силикон «нарастили» немного животного белка и мускульные клетки из крысиного органа. При пропускании через искусственный организм электрического заряда он приходит в движение.

Военный потенциал этих технологий — сбор разведданных и массовые диверсии на территории противника. Но это лишь начало пути. Силиконовые конструкции разных форм со смертоносным оборудованием, которые будут самостоятельно принимать тактические решения, — вот один из вариантов армии будущего.

Л. Дель Монте, известный ученый-физик, бывший руководитель разработок микроэлектроники в IBM, автор книги «Нанооружие: растущая угроза человечеству», прогнозирует, что к концу 2020-х гг. террористы смогут получить доступ к нанооружию и будут способны использовать наноботов (нанороботов) для совершения террористических атак, например для заражения систем водоснабжения крупных городов или отравления людей инъекциями. Нанодроны, по мнению Дель Монте, также могут стать инструментами биологической войны.

Еще в 2010 г. Пентагон высказывал опасения, что нанотехнологии приведут к созданию взрывоопасной искусственной микропыли, наноботы смогут доставлять биологическое оружие, выступать сами в роли оружия. Наноботы даже будут попадать при дыхании в легкие солдат и выводить их из строя.

Дель Монте в своей книге прогнозирует, что автономные наноботы будут в состоянии собирать свои копии, т. е. воспроизводить сами себя. Управление миллионами наноботов может стать огромной проблемой, а сбои в программном обеспечении могут привести к непредсказуемым последствиям.

Вообще, что касается использования боевых роботов деструктивными организациями, то есть основания ожидать, что это уже произошло либо произойдет в интервале от двух до пяти лет. Данная проблема имеет несколько аспектов. Боевой робот представляет собой комбинацию обычного многофункционального робота с добавкой боевого и управляющего компонентов. Они производятся и продаются раздельно как на легальных, так и особенно на нелегальных рынках. Нет никаких препятствий для того, чтобы террористические, преступные и экстремистские группы наняли конструкторов, программистов, которые приобрели бы нужную универсальную роботизированную платформу и смонтировали на ней те или иные боевые компоненты. Вероятно, что в ближней перспективе подобные кустарные боевые роботы будут уступать по своим характеристикам боевым роботам, находящимся в распоряжении вооруженных сил и сил правопорядка государств. Однако в перспективе в интервале от трех до семи лет можно ожидать выравнивания потенциала, возможностей и доступности боевых роботов для государственных сил и деструктивных акторов.

Боевые роботы разнообразного базирования различаются по типам оснащения вооружением. Наиболее широкое распространение получили боевые дроны, т. е. беспилотники, вооруженные ракетами для поражения, как правило, наземных целей. В 2014 г. на вооружение пограничной службы и береговой охраны США, а также полиции

нескольких штатов поступили боевые дроны, оснащенные нелетальным оружием, включая биобезопасные клеи, сети, слезоточивый газ, парализующие вещества и т. п. Поскольку так же, как в случае с боевыми дронами, подобные системы могут быть созданы небольшими группами специалистов, своего рода нелегальными стартапами, то есть основания полагать, что они либо уже имеются, либо в ближайшее время окажутся в распоряжении деструкторов.

В отличие от роботов-убийц, наиболее востребованных террористами и экстремистами, подобные роботы будут взяты на вооружение в первую очередь преступными группами. Они позволяют осуществлять различного рода акции без убийств людей. В случае пресечения или раскрытия подобных акций это, без сомнения, снизит сроки наказания для их организаторов и участников. Данное обстоятельство в большинстве случаев принимается во внимание организаторами преступных акций.

Подлинным кошмаром для разведывательных и правоохранительных структур всех стран мира являются боевые роботы, оснащенные биологическим и химическим оружием. Чтобы создать боевого робота, использующего биологическое оружие, достаточно использовать производимые в настоящее время дроны сельскохозяйственного назначения, заполнив соответствующие их емкости не удобрениями, а бактериями, вирусами или химическими соединениями. Стоимость сельскохозяйственного дрона с дальностью полета до 150 км и емкостью загрузки до 50 л составляет всего 6 тыс. долл. США, а емкостью до 200 л — менее 9 тыс. долл. Покупка такого дрона доступна не только террористической сети, но и отдельной группе фанатиков и экстремистов.

Что касается производства биологического и химического оружия, то сегодня нет никакой возможности своевременно распознать и идентифицировать подобные процессы, организованные на распределенной основе в лабораториях американских, западноевропейских и восточноазиатских университетов и т. п. Это является самой большой и самой недооцененной опасностью при использовании робототехники террористами и экстремистами. В отличие от террористов и экстремистов преступники могут использовать подобные средства для шантажа органов власти, правительств с целью получения крупных финансовых средств.

Еще более опасным в перспективе является создание боевых роботов, вооруженных специальными техническими устройствами бесконтактного заражения программно-аппаратных блоков различного типа, установленных на военных, гражданских, транспортных и иных объектах. В 2014 г. американские и немецкие программисты и технологи

сообщили о том, что им удалось создать системы заражения программных систем, даже не подключенных к Интернету и другим компьютерным сетям, через оптическую и акустическую среды. Представляется, что в ближней перспективе (до пяти лет) в силу экспериментального характера подобных работ и их мгновенного засекречивания вряд ли следует считать заслуживающей внимания вероятность оснащения подобным физико-программным оружием боевых дронов, находящихся в распоряжении деструктивных структур.

С 2013 г. началось оснащение боевых роботов, находящихся в распоряжении преступных и террористических организаций, средствами подавления систем обнаружения и контроля технических устройств, а также биологических объектов в приграничных зонах, территориях особой охраны и т. п. Такие системы были в 2013—2014 гг. неоднократно применены против правоохранительных подразделений США на американо-мексиканской границе, структур береговой охраны в районе Флориды и Мексиканского залива, береговой охраны Италии и т. п.

Гражданские роботы. Гражданские ААС и роботы можно разделить на три типа. Во-первых, это производственные роботы, осуществляющие те или иные операции в различных секторах экономики; во-вторых, бытовые или потребительские роботы и ААС, представляющие собой любые технические устройства с электронными компонентами управления, как правило подсоединенные к сети Интернет; в-третьих, программно-аппаратные комплексы управления и регулирования технически сложными производственными инфраструктурными и телекоммуникационными комплексами. Они объединены термином «критические государственные, коммунальные и бизнес-системы».

За последние 15 лет накоплено множество примеров использования ААС в преступной деятельности.

Как известно, любые ААС и роботы состоят из аппаратного и программного компонента. Для каждого из этих компонентов свойственны собственные тренды и тенденции изменений. К сожалению, практически все они ведут к расширению возможностей использования ААС и роботов террористами, преступниками и экстремистами.

Как отмечают эксперты в области применения дронов, теперь в любом крупном зарубежном магазине электроники по цене одного-двух смартфонов можно купить квадрокоптер, который после 10-минутной настройки будет точно и безопасно летать, делая фотографии и видео, доставлять грузы.

Основные факторы робототехники, значимые для криминологического анализа. Рассмотрим тенденции роботизации преступности и терроризма.

Технологизация уличной и неорганизованной преступности. Традиционно использование сложных технических устройств и приспособлений являлось прерогативой организованной преступности. В последние годы ситуация коренным образом изменилась. С появлением «Интернета вещей», по сути, весь окружающий мир превратился из мира вещей в мир ААС. Это в полной мере относится не только к сегодняшним сложным системам управления домом, но и к телевизорам, холодильникам, пылесосам, автомобилям и т. п. В ближайшие пять — семь лет ожидается появление массового рынка бытовой робототехники. Из дорогостоящих игрушек и статусных устройств для богатых бытовые роботы станут обязательной принадлежностью дома и квартиры средней американской семьи.

М. Гудман в книге «Будущее преступности» приводит пример, произошедший на Тайване в середине 2014 г. Полиция попыталась арестовать известного наркоторговца, который окружил свой дом сетью роботов-видеонаблюдателей, вооруженных поражающими электрошоковыми устройствами и слезоточивым газом. Обескураженная полиция столкнулась с необычным сопротивлением, а наркоторговец скрылся через заранее подготовленный подземный ход.

В последние пять — семь лет по экспоненте растет число преступлений — от грабежей до убийств — с использованием ААС. Значительная часть подобных преступлений, зафиксированных в полицейских отчетах, остается нераскрытой. Это связано с тем, что подобные высокотехнологичные преступления, совершаемые отдельными лицами или небольшими криминальными группами, в корне отличаются от традиционных правонарушений. Правонарушения, с которыми привыкла иметь дело полиция, полностью происходят в реальном мире. Соответственно, преступник оставляет улики, или, более того, он фиксируется в прошлом свидетелями либо в последние годы различного рода системами видеонаблюдения.

Преступность с использованием ААС и роботов предполагает, безусловно, физические действия. Но сигнал, который приводит в действие те или иные аппаратные средства, передается в электромагнитной среде и носит виртуальный характер. Сегодня для того, чтобы совершить преступление, не надо присутствовать на его месте. Можно находиться не за десятки, а даже за сотни и тысячи километров. Правоохранительные органы не привыкли работать в таких условиях, и, соответственно, их деятельность не слишком эффективна.

Не говоря уже о преступных синдикатах, даже отдельные, как принято говорить, уличные преступники отдают себе отчет в неспособности полиции противостоять высокотехнологичным преступлениям. Именно поэтому они берут на вооружение ААС и роботов как орудия преступлений.

Например, российские киберпреступники стали применять новый способ хищения данных банковских карт с помощью внешних интерактивных голосовых ответов (IVR). Мошенники используют специально запрограммированных роботов, звонящих клиентам финансовых организаций. Программа выдает себя за сотрудника банка и без труда выведывает всю необходимую информацию (учетные данные, PIN-коды, CVV-коды и т. д.).

Как правило, IVR используются для ответа на входящие звонки (приветствия клиентов, предложения перезвонить на внутренний номер сотрудника банка и проч.). Мошенники стали применять данную технологию для исходящих звонков. Представившись сотрудником финансовой организации, робот просит ничего не подозревающего абонента сообщить данные либо для уточнения некоторых моментов, либо из-за сбоя системы.

С целью скрыть свои следы злоумышленники запускают роботов в «облачных» дата-центрах (центрах хранения и обработки данных). Для того чтобы избежать подозрений со стороны жертв, время от времени программа перенаправляет их звонки на живых людей.

Данная схема весьма эффективна, поскольку большинство клиентов банков не догадываются о способности роботов звонить.

Повышение вероятности крупномасштабных террористических актов. Длительное время крупномасштабные террористические акты требовали долгой подготовки, вовлечения множества участников, затрат значительных и разнообразных ресурсов и, наконец, физического присутствия террористов в зоне актов устрашения и насилия. Наиболее яркими примерами стали акт 11 сентября 2001 г., взрывы в метро в Лондоне и на вокзале в Мадриде. Все они имели отмеченные выше черты. Силам национальной безопасности не удалось предотвратить эти акты, но указанные выше характеристики позволили им выйти на планировщиков и исполнителей варварских актов и наказать их. Эти же черты позволили силам национальной безопасности различных стран предотвратить в последние 15 лет несколько десятков крупномасштабных террористических актов, которые по своим последствиям могли не уступать и даже превзойти случившиеся события.

Однако с повсеместным внедрением ААС, а в последующем робототехнических комплексов ситуация резко и неблагоприятно изменилась. В последние годы происходит активная автоматизация и роботизация производственной сферы и сферы обеспечения жизнедеятельности. Наряду с повышением технической надежности и экономией затрат этот процесс влечет и крайне негативные последствия. Сегодня в развитых странах мира, особенно в Соединенных Штатах, жизнь миллионов людей, фактически всего населения страны, решающим образом зависит от объектов и сетей критической инфраструктуры. В их число входят не только федеральные объекты государственного управления и т. п., но и практически все системы жизнеобеспечения, включая энергетику, тепло- и водоснабжение, связь и т. д.

Энергетические сети независимо от того, в чьей собственности и юрисдикции они находятся, управляются ААС, соединенными с Интернетом, как и системы городских водопроводов, канализации, теплоснабжения. Самое опасное состоит в том, что за последние пять — семь лет эффективными роботизированными системами оснащены все АЭС, крупнейшие плотины и т. п.

В связи с этим даже не тревогу, а ужас у специалистов в США вызвали известия о том, что за последние годы неопознанные хакеры неоднократно вторгались в систему энергоснабжения, комплексы автоматизированного управления и хранилища данных гидросооружений и даже атомных станций США. В результате у неизвестных лиц или организаций имеется федеральная информация об уязвимостях и недостатках систем управления и обеспечения безопасности всеми плотинами и гидротехническими комплексами на территории США, системами водоснабжения многих крупных и крупнейших городов страны, региональных энергосистем.

В случае же, если информация об уязвимостях в критических инфраструктурах и системах управления ими уже попала или попадет в распоряжение террористических организаций, экстремистских сообществ и с несколько меньшим риском — преступных синдикатов, могут произойти непредсказуемые по своим последствиям акты. Причем на сегодняшний день у структур национальной безопасности нет способов предотвратить их. Более того, затруднена будет идентификация нападающего.

Согласно отчету компании Trend Micro (май 2017 г.) в мире насчитывается свыше 83 тыс. доступных через Сеть промышленных роботов, и в 5 тыс. из них отсутствуют механизмы аутентификации пользователей. Исследователи обнаружили в роботах 65 уязвимостей, в том числе позволяющих обойти механизмы аутентификации, модифицировать ключевые настройки и изменить режим работы устройства.

Все вышеизложенное относится только к роботам, непосредственно доступным через Интернет. Однако, как подчеркивают исследователи, злоумышленники также могут получить доступ к не подключенным к Сети устройствам, предварительно взломав промышленные маршрутизаторы, используемые на высокотехнологичных предприятиях.

Последствия кибератак на промышленных роботов могут быть катастрофическими. Согласно отчету Trend Micro в результате подобных атак в производимых продуктах могут возникать дефекты. Злоумышленники способны вмешиваться в производственный процесс и требовать от производителя выкуп за его восстановление, портить продукцию, причинять вред механизмам и их операторам, а также похищать хранящуюся в памяти роботов информацию (исходный код, параметры продукции и другую интеллектуальную собственность).

В подтверждение своих опасений исследователи осуществили показательную кибератаку на промышленного робота в лабораторных условиях. Эксперты продемонстрировали, как с помощью атаки можно незаметно изменить движение устройства. Программный код остается неизменным, а изменение движения невозможно уловить невооруженным взглядом. Тем не менее малейшее отклонение в производственном процессе может привести к серьезным последствиям.

Новые измерения финансового терроризма и преступности. Если на потребительском рынке продаются первые мелкосерийные полноценные роботы, а в военной сфере на вооружение поступают первые единичные образцы, то в сфере финансов полностью роботизированные системы — торговые роботы — за последние пять лет стали обычными на большинстве финансовых рынков Америки, Великобритании и Японии.

Торговые роботы представляют собой интеллектуальные программно-аппаратные комплексы, которые оснащены не только модулями сбора, обработки, анализа информации, но и самостоятельного, без человека, принятия решений сообразно алгоритмам. На последнее хотелось бы обратить особое внимание. Не только среди политиков, военных и бизнесменов, но даже среди части специалистов по информационным технологиям бытует заблуждение, что торговые роботы представляют собой предтечу искусственного интеллекта и вплотную приблизились к нему. Внешне дело выглядит именно таким образом, поскольку все решения о купле-продаже акций, индексов, валют, деривативов и т. п. принимают непосредственно программно-аппаратные комплексы — торговые роботы. Но если обратиться к сути дела, то выяснится, что решения они принимают не по собственным правилам, которые создали сами, а по алгоритмам, которые заложены в них людьми — программистами, разработчиками, математиками, аналитиками и т. п. Поэтому об искусственном интеллекте говорить пока преждевременно, хотя решения на финансовых рынках принимаются роботами без непосредственного участия человека.

Если в 2010 г. не более трети операций на американских финансовых рынках осуществлялось торговыми роботами, то в настоящее время более 70% сделок на биржевых и внебиржевых финансовых

рынках, торгующих биржевыми финансовыми продуктами, осуществляются не людьми, а торговыми роботами.

Экспансия торговых роботов, которые могут стоить 10 млн долл. и более, связана с двумя обстоятельствами. С одной стороны, торговля на финансовых рынках требует регулярной обработки огромных массивов информации. При краткосрочном трейдинге, а на него приходится основная часть операций, люди просто не успевают обработать и проанализировать разнородные и разноформатные массивы информации. Более эффективно это делают торговые роботы, которые принимают решения на основе некоторых правил. В этом смысле торговые роботы являются наследниками и более универсальными вариантами компьютеров, которые в прошлом обыгрывали чемпионов мира по шахматам. В обоих случаях в основе программ лежат определенные алгоритмические правила, построенные на основе иерархии принятия решений.

С другой стороны, сегодня известно, что источником доходов на финансовых рынках является сверхкраткосрочный временной арбитраж. Если кто-то успевает среагировать на рыночные известия быстрее других, то он получит выгоду от более раннего знания той или иной новости. Если со времен Ротшильдов до середины XX в. шла гонка за скорость получения информации, то с середины прошлого века до нашего времени началась гонка за скорость реагирования на информацию.

Как было показано на примере боевых роботов, автоматизированные системы способны быстрее людей реагировать на любую внешнюю информацию. Соответственно, с середины 2010-х гг. стали создаваться не только все более совершенные алгоритмически, но и все более быстродействующие торговые роботы. В настоящее время торговые роботы крупнейших американских банков, которые сто́ят уже не десятки, а сотни миллионов долларов, окупаются чуть более чем за четыре месяца за счет того, что способны опережать других роботов на сотые миллисекунды.

Господство торговых роботов на финансовых рынках создало новые угрозы для финансовой системы и национальной безопасности США и Запада. В 2014 г. федеральная Комиссия по ценным бумагам (SEC) выпустила доклад, в котором обратила внимание не только финансистов, но и политиков и структур, занимающихся национальной безопасностью, на настораживающий факт. Если в течение нулевых годов в среднем за год фиксировалось чуть менее девяти необъяснимых колебаний курса акций, в разы превышающих их нормальную волатильность, то в 2011—2012 гг. подобных колебаний фиксировалось уже в среднем 36 за год, в 2013 г. — 41 и в 2014 г. — 74. Доскональный анализ, проведенный SEC, показал, что эти колебания не

были связаны с какими-либо событиями или новостными поводами, связанными с соответствующими компаниями. Эти колебания были результатами действий торговых роботов, принимавших решения о купле-продаже в соответствии с некоторыми алгоритмами.

После публикации доклада ряд крупнейших финансовых институтов и независимых трейдеров, чьи торговые роботы активно участвовали в операциях по купле-продаже, приведших к подозрительной сверхволатильности в 2013—2014 гг., с привлечением специалистов Комиссии, работников Агентства национальной безопасности (АНБ) и независимых фирм по компьютерной безопасности осуществили программно-технологический аудит своих роботов. В результате выяснилось, что в большинстве случаев (точное количество по соображениям коммерческой тайны и национальной безопасности озвучено не было) торговые роботы принимали ошибочные решения в том смысле, что действовали не по алгоритмам, а в результате заражения специальными зловредными программами, срок существования которых измерялся секундами.

После обнародования данной информации ФБР и независимые эксперты сделали вывод о том, что во всех отмеченных случаях имело место не просто хакерство, а тщательно спланированные и виртуозно осуществленные финансовые преступления с использованием программно-аппаратных комплексов. Доступные исследователям и общественности факты говорят о том, что с каждым годом количество и масштабы такого рода преступности, связанной с заражением, а в будущем, возможно, и перехватом управления торговыми роботами, будет только нарастать.

Пока достоверно известно лишь о фактах финансовой преступности с использованием торговых роботов. Однако учитывая кластеризацию деструкции, есть основания полагать, что с каждым годом будет увеличиваться опасность крупномасштабных, а возможно, и глобальных актов финансового терроризма. Имитационные модели, разработанные в Массачусетском технологическом институте и Финансовой лаборатории в Швейцарии, в Цюрихе, свидетельствуют, что уже сегодня целенаправленный перехват управления торговыми роботами может вызвать глобальное крушение финансовых рынков, за которым последует согласно эффекту домино коллапс мировой финансовой системы.

§ 3. Криминальная 3D-печать

3D-печать подобно Интернету принесет в жизнь и новые риски. Естественно, первым объектом преступников в мире 3D-печати станет кража интеллектуальной собственности. До настоящего времени

пираты крали музыку, видео, игры, программное обеспечение. Теперь ситуация в корне изменится. Хотя уже несколько десятилетий мошенники специализируются на поддельных сумках, одежде знаменитых фирм, изготовлении поддельных часов Картье и т. п., все они легко распознавались из-за плохого дизайна и дешевых материалов. Однако в будущем достаточно будет отсканировать любую, самую совершенную, модель, распознать, какой материал используется, и в точности воспроизвести его на 3D-принтере.

Цифровое производство также будет благом для взломщиков и воров. Уже сегодня, воспользовавшись фотографией из дома или офиса, где изображены ключи от них, случайно оставленные на столе, можно продублировать ключ при помощи 3D-печати. В 2012 г. полицейские обнаружили программное обеспечение для изготовления ключей, позволяющих преступникам сменить цифровые браслеты, одеваемые на них при домашних арестах.

В будущем 3D-печать найдет большое применение в наркоторговле. Ученые уже разработали так называемый *химпьютер*, который по требованию печатает на 3D-принтере из заготовки ибупрофен. Мафиозные структуры, несомненно, адаптируют технологию 3D-печати для своих нужд.

Возможно, одним из самых острых вопросов является способность 3D-принтера производить огнестрельное оружие. К. Уилсон, 26-летний бывший студент, анархист и либертарианец, поклонник Страшного пирата Робертса, создал проект «Wiki-оружие». Он соединил его с биткойном, разместил в «темном» вебе и организовал распределенную онлайн-сеть по проектированию, дизайну и печати на 3D-принтере различных образцов оружия.

Его крупнейшим достижением стали автоматическая винтовка, которая смогла сделать 600 выстрелов, и боевой пистолет, стреляющий стандартными пулями. К настоящему времени всю документацию, необходимую для печати пистолета на домашнем 3D-принтере, скачали 100 тыс. человек по всему миру. Отвечая на вопросы в прессе, зачем он это сделал, Уилсон сказал: «Компьютер, Интернет и 3D-принтер дали мне возможность реализовать американскую Конституцию, предусматривающую право граждан вооружаться».

Пластиковое огнестрельное оружие особо опасно, поскольку незаметно для стандартных детекторов безопасности, установленных в правительственных зданиях, аэропортах и т. п. Лишний раз это доказала команда израильских отставных военных, которые два раза подряд пронесли в хорошо охраняемое и защищенное поясами безопасности здание Кнессета напечатанный на 3D-принтере пистолет. Аналитический центр ФБР крайне обеспокоен тенденцией производства 3D-оружия и недавно скупил все существующие модели 3D-принте-

ров, чтобы исследовать, какие из них террористы могут использовать для изготовления самодельного огнестрельного оружия и взрывных устройств. Уже сегодня сложные промышленные принтеры, которые тем не менее продаются всем платежеспособным клиентам, позволяют изготовить не только мелкое, но и крупное оружие, включая основные детали для пусковых установок ракет «земля — земля» и «земля — воздух».

В условиях цифрового производства инспекция на государственной границе становится бессмысленной. Если можно просто напечатать пушки, таблетки, бомбы, то зачем переходить границы и рисковать. 3D-печать ставит принципиально новые вопросы перед международной безопасностью. Надо понимать, что в условиях миниатюризации производства, многофункциональных роботокомплексов и 3D-печати больше невозможно будет устанавливать эмбарго на поставку оружия или чего-то подобного в те или иные регионы.

Первопроходцем в создании оружия на 3D-принтерах стал уже упомянутый американец К. Уилсон, представивший в мае 2013 г. свое изобретение — однозарядный пистолет Liberator (по-русски означает «Освободитель»), чертежи которого свободно стали «разгуливать» по Сети. Очень скоро это заставило власти США принять закон, который запрещал создавать подобные устройства, а также ввести 10-летний мораторий на изготовление оружия без добавления металла.

Это решение оказалось своевременным, но малоэффективным. Распечатанный на 3D-принтере пистолет несет большую опасность для общественного спокойствия. Пластмассовые детали, из которых он распечатан, никогда не «запищат» на металлодетекторе, а это значит, что пронести его на борт самолета или войти с ним в здание будет весьма просто.

Также такой пистолет можно легко утилизировать — достаточно сжечь орудие преступления, и никаких следов его существования не останется. А самозарядная винтовка Shuty, созданная американским энтузиастом под ником Derwood, положила начало эпохе автоматического и полуавтоматического оружия. Теперь такие устройства способны выдержать от 10 до 30 выстрелов и не расплавиться.

Чисто теоретически для изготовления самострела подойдет любой, даже самый простейший FDM-принтер, т. е. устройство, печатающее пластиковым прутком. Это самая доступная, а потому и самая распространенная технология 3D-печати. Простой конструктор китайского производства можно приобрести примерно за 15 тыс. руб., а килограммовая катушка ПЛА или АБС-пластика хорошего качества обойдется еще в 1000—1500 руб.

В 2014 г. 28-летнего японца отправили в тюрьму за изготовление пистолетов на 3D-принтере. Окружной суд Йокогамы приговорил Йосимото Имуру к заключению по обвинению в незаконном владении оружием.

Как пишут местные СМИ, органы правопорядка заинтересовались молодым человеком после видеозаписи. На ней он стрелял из изготовленного оружия в лесу и рассказывал о его характеристиках. Суд счел, что практика печати пистолетов на 3D-принтере ставит под угрозу безопасность других людей.

В 2015 г. 3D-печатное оружие (и детали от него) было найдено у людей, связанных с австралийскими криминальными группировками. А в 2016 г. полиция задержала байкера, у которого дома были найдены 3D-принтер и оборудование для изготовления 3D-печатного огнестрельного оружия.

В начале 2015 г. во время полицейской облавы в Голд-Косте (Австралия) было найдено несколько комплектов для сборки 3D-печатных пистолетов. Чуть позже полиция обнаружила заряженный пистолет в Мудгеерабе, пригороде того же города. В последнем случае тоже было арестовано несколько байкеров.

После этого австралийское правительство решилось на крутые меры. С ноября 2015 г. в штате Новый Южный Уэльс было запрещено хранить у себя даже чертежи 3D-печатного оружия. Теперь по закону жители этого штата могут получить до 14 лет лишения свободы за хранение подобных цифровых чертежей. На недавно проведенной пресс-конференции полиция Нового Южного Уэльса продемонстрировала два 3D-печатных пистолета, сделанных по чертежам «Освободителя» (Liberator), взятым из Сети. На их печать требуется всего 27 часов, после чего достаточно установить стальной стерженек, выполняющий роль бойка ударника.

§ 4. Биотехнологии, терроризм и преступность

Направления криминального использования достижений биотехнологий. Можно много говорить и писать о перспективах гуманистического использования био- и нанотехнологий, о «светлом будущем» человечества, о либеральной евгенике, об излечении наследственных заболеваний, продлении человеческой жизни бесконечно. Но все это касается лишь легальной части био- и нанотехнологической революции. А существует, и уже длительное время, нелегальная (и практически всегда криминальная) ее составляющая.

Даже когда эту нелегальную часть реализует государство, пусть даже самое суперлиберально-демократическое, оно всегда это делает втайне от своих граждан, своих демократических институтов. И все-

гда такая деятельность фактически противоправна и преступна. Преступна потому, что представляет собой деятельность, запрещенную международно-правовыми документами и национальным уголовным законодательством (табл.).

По оценкам экспертов, лаборатория по производству биологического оружия в современных условиях вместе со всем оборудованием может стоить в пределах от нескольких десятков до нескольких сотен тысяч долларов США, а в качестве биологического оружия могут быть использованы и те патогены, которые конвенционально не запрещены для применения в исследовательских целях, получения диагностических систем, вакцин и других медицинских препаратов.

Наиболее значимыми угрозами биотерроризма являются резкое увеличение числа специалистов по биотехнологиям, доступность информации по рецептурам биологических и бактериологических препаратов, а также возможность легендирования отдельных актов биотерроризма под проявления естественных эпидемий и инфекций.

В конце 2005 г. генетик Р. Брент из Калифорнийского института молекулярных наук (Molecular Sciences Institute — MSI) провел эксперимент, доказывающий, что сегодня технологии в генной инженерии достигли уже такого уровня, когда один толковый лаборант с небольшим объемом «правильных» ресурсов может изготовить биологическое оружие с гибельной мощью, не уступающей атомной бомбе.

Брент утверждает, что искусственно сконструировать оспу, или сибирскую язву, или, может, даже эболу сейчас можно в простой лаборатории, используя свободно продающиеся исходные компоненты и, таким образом, не вызывая подозрений.

Например, через Интернет на сетевом аукционе можно приобрести любые модели ДНК-синтезаторов (DNA synthesirer): от 5 до 43 тыс. долл. США. Чтобы собрать геном оспы, нужно через Интернет закупить сырья на 200 тыс. долл. США. Генетическую последовательность можно также легко найти на публичных ресурсах Интернета. Кроме того, сейчас существует немало биотехнологических фирм, которые синтезируют генетические последовательности по заказу и высылают клиенту почтой.

Американский ученый Р. Карлсон, физик и биолог, работавший некоторое время с Брентом в MSI, прогнозирует, что примерно в течение десятилетия создание биологического оружия с нуля станет столь же легким и дешевым, как построение сайта.

В июне 2006 г. сотрудники британской газеты The Guardian выяснили, что создать биологическое оружие сегодня может буквально любой заинтересованный в этом житель Соединенного Королевства.

Направления теневого (криминального) использования результатов биотехнологической революции и субъекты, их осуществляющие[1]

Направления	Субъекты				
	Военные и спецслужбы	Мафиозные структуры	Террористы	Параученые (ученые-маньяки)	Фашисты и расисты
Разработка биологического, генетического («этнического» и т. д.) оружия	+	+	+	+	+
Создание «сверхчеловека» (сверхсвойств человека: повышенная агрессия, выносливость, нечувствительность к боли и т. д.)	+	+	+	+	+
Разработка нейрофармакологических средств для контроля поведения	+	+	+	+	+
Создание клонов человека	+	+	+	+	
Создание человекоподобных химер	+	+	+	+	
Торговля человеческими органами и тканями под видом продуктов генной инженерии		+			
Индустрия криминальных абортов (использование эмбрионов для экспериментов со стволовыми клетками)		+			
Использование генной инженерии для выведения устойчивых сортов наркотикосодержащих растений		+			
Использование достижений синтетической биологии по созданию трансгенных дрожжей в качестве сырья для опиатов		+			

Внимание журналистов привлек сайт компании VN Bio Ltd, занимающейся поставкой оборудования и расходных материалов для биологических лабораторий. В одном из каталогов биосырья были найде-

[1] Более подробно см.: *Овчинский В. С.* Криминология и биотехнологии. М., 2006.

ны весьма странные «товары» — на продажу выставили фрагменты ДНК смертельно опасных для человека вирусов оспы и испанского гриппа. Для оформления заказа на ДНК оспы понадобилось лишь назвать адрес, номер мобильного телефона и адрес электронной почты — уже через три часа в редакцию The Guardian позвонил курьер и сообщил, что заказ доставлен. Никаких проверок того, кому отправляется потенциально опасный груз, проведено не было — получателем мог бы оказаться как законопослушный ученый, так и возможный террорист.

В этих условиях контроль за биотехнологическим рынком в Сети должен стать важной новой задачей полицейских подразделений и спецслужб, контролирующих теневые криминальные рынки в Интернете.

Не меньшую опасность представляет разработка нейрофармакологических средств для контроля за поведением. О том, что и эти работы проводились, написано достаточно много книг на весомом фактическом материале. По существу, речь здесь идет о разработанных видах психотропного оружия на основе биотехнологий.

Еще в конце 1950-х гг. А. Берл, в то время помощник государственного секретаря США, который участвовал в программах ЦРУ по контролю за поведением с помощью нейрофармакологии, в своем дневнике записал: «Я опасаюсь одного. Если ученые сделают то, что запланировали, то люди превратятся в манипулируемых муравьев».

Биотехнологии в эпоху биотерроризма. Фактически в XXI в. началась *эпоха биотерроризма*. Первый случай был связан с рассылкой в 2001 г. по почте спор сибирской язвы, в результате чего погибли пять человек из состава работников Конгресса США, имевших контакт со смертоносными конвертами. В 2014 г. спецслужбам США стало известно, что предположительно в Йемене и на севере Сирии «Аль-Каида» создала лаборатории по производству биологического оружия.

Еще в 1995 г. японская террористическая религиозная секта «Аум Синрикё», руководителей которой принимал и поддерживал один из тогдашних российских лидеров, провела химическую атаку в метро Токио, в результате которой погибли 300 человек и около 10 тыс. серьезно отравились. В ходе судебного процесса стало известно, что эта атака была лишь репетицией предполагаемой массированной биоатаки против Токио с использованием чрезвычайно опасного биотоксина, на разработку и производство которого секта потратила 10 млн долл. США.

Террористам больше не придется расходовать средства и искать специалистов, которые могли бы создать для них патогены и биологическое оружие. С появлением *синтетической биологии* им просто достаточно взломать те или иные серверы, скачать биопрограммную информацию и самим распечатать смертоносные вирусы. Представляется, что больших проблем в этой области у них не возникнет. Ведь, например, генетические коды вируса эболы и знаменитой испанки, унесшей жизни десятков миллионов людей, можно скачать в Национальном центре биотехнологической информации в США.

Еще пять лет назад синтетическая биология и генная инженерия были дорогостоящим занятием. Теперь они по карману небольшим и небогатым группировкам, а в ближайшие два года станут доступны каждому, кто потратит несколько недель на изучение соответствующей литературы и овладение навыками работы.

М. Гудман в книге «Будущее преступности» пишет, что биопреступники и биотеррористы не будут полагаться на существующие патогены, против которых есть средства борьбы. Они, безусловно, будут создавать еще более смертоносные новые вирусы, против которых нет антидотов. Что это нетрудно сделать, показали в 2013 г. исследователи из Нидерландов. При бюджете в 100 тыс. долл. США на основе штамма птичьего гриппа они смогли спроектировать и произвести новый штамм, который передается по воздуху и быстро усваивается человеком. В настоящее время птичий грипп для птиц и животных имеет показатель смертности 70%, но лишь один из тысячи человек заражается птичьим гриппом. Для нового штамма показатели составляли 98%, и из 100 инфицированных болезнь могла начаться более чем у 80%.

Таким образом, было создано по-настоящему страшное оружие, поскольку вирус передавался по воздуху. Исследователи провели работу исключительно для того, чтобы привлечь внимание научной общественности и политических деятелей к теме синтетической биологии и ввести запрет хотя бы на проведение частных исследований в этой сфере, а также в любых лабораториях, которые не подпадают под согласованный в ООН список. Свою работу с детальным изложением результатов проведенных экспериментов ученые разослали в целый ряд ведущих научных журналов. Но ни в одном статья не вышла. Вмешалось американское правительство и Научный совет ЕС, которые наложили вето на любые публикации в этой сфере. В итоге публикация разошлась среди биологов в виде почтового файла.

Биотеррор, несомненно, может иметь разрушительные последствия. Но вновь сошлемся на Гудмана. Он полагает, что с использованием достижений синтетической биологии вновь возродится индивидуальный точечный террор. Технологии синтетической биологии делают возможным не только создание персонифицированных лекарств, но и

персонифицированных орудий убийства. Для этого надо лишь синтезировать ДНК человека с конкретным вирусом или патогеном. В этом случае достаточно ввести сотую долю миллиграмма этого патогена в пищу, растворить в воздухе и т. п., и человек будет убит, а все остальные ничего не почувствуют.

Наркокартели и синтетическая биология. Выгодным направлением деятельности мафиозных структур уже стало использование генной инженерии для выведения устойчивых сортов наркотикосодержащих растений (повышение их урожайности, защита от вредителей и т. д.) и создание новых видов наркотиков на основе технологий синтетической биологии.

Один из главных доходов организованной преступности в XX и XXI вв. — производство и сбыт наркотиков. Как правило, наркокартели получают свой главный наркодоход не от розничной реализации, а от выращивания или синтеза наркотиков, их очистки, упаковки, транспортировки и оптовых продаж по всему миру. Это сложный бизнес, требующий высокого уровня логистики, организации, управления и способности реагировать на форс-мажорные обстоятельства. Поэтому еще с 50-х гг. прошлого века наркокартели финансируют науку, нанимают к себе на работу бывших высокопоставленных и профессиональных работников спецслужб и правоохранительных органов, первоклассных управленцев. Однако, по всей вероятности, на многих рынках привычные наркокартели доживают последние дни. По мнению М. Гудмана, в ближайшие 10 лет традиционные наркокартели будут ограничены в своих действиях рынками развивающихся стран.

Что касается самых емких рынков Америки, Европы, богатых стран Азии, то здесь наркокартели, базирующиеся на сельском хозяйстве, заменят высокотехнологичные сетевые структуры, производящие принципиально новые виды наркотиков, используя технологии синтетической биологии. Это позволит новым структурам резко повысить по сравнению с ныне существующими наркокартелями свою неуязвимость, сэкономить значительные ресурсы на логистике и организации системы продаж. Синтетическая биология будет использована преступниками не только для создания наркосиндикатов нового типа, но и для организации параллельной медицины.

На протяжении последних десятилетий мы видим неуклонный *переход от растительных наркотиков к синтетическим*. Однако при всей своей привлекательности для наркоманов они обладают таким числом побочных, нередко смертельных эффектов, что даже самые отпетые наркоманы подсаживаются на них лишь в конце своего наркопути.

Синтетическая биология позволяет, если можно так выразиться, соединить потребительскую эффективность искусственных наркотиков с привычностью и относительной мягкостью растительных. В рамках синтетической биологии больше не нужно будет выращивать растения. Достаточно будет взять генетические коды марихуаны, мака, листьев коки и т. п. и синтезировать их с дрожжами. Затем в принципе можно сделать наркотический хлеб, пиво или что угодно. Это не только снизит издержки и откроет новые рынки, но и сделает для правоохранительных органов крайне сложным распознавание систем сбыта наркотиков.

В 2014 г. М. Гудман в книге «Будущее преступности» приводил следующие примеры.

В лаборатории Северо-Западного университета США биоинженеры создали синтетическую бактерию, в которой активный ингредиент каннабиса был упакован в оболочку хорошо усваиваемой организмом бактерии для того, чтобы доставлять обезболивающее непосредственно в ходе операции, причем в дозировке, необходимой для тех людей, у которых есть аллергия на традиционные обезболивающие, делающая невозможным проведение им сложных хирургических операций. В Сан-Диего были разоблачены два докторанта Университета Беркли, которые купили пекарню, где в дрожжи добавлялись при помощи синтетической биологии опиум и марихуана. При этом выявить их удалось не благодаря работе полиции или тому, что кто-то из клиентов пожаловался в правоохранительные органы. Они были обнаружены вследствие того, что служба по борьбе с наркотиками Сан-Диего получила ориентировку на пекарню от внедренного в мексиканский наркосиндикат агента. Агент сообщил, что наркосиндикат, который ведет подневный статистический анализ потребления наркопродукции во всех локациях, отдельно по каждой торговой точке, обратил внимание, что в определенном районе Сан-Диего у него начался отток клиентов. Тогда наркосиндикат отправил на точку нескольких специальных наблюдателей. Они проследили, что клиенты сбытовиков наркосиндикатов не реже, чем раз в два дня заходят в определенную пекарню. После этого разведчики наркосиндиката произвели контрольную закупку и уже в химической лаборатории в Мексике в пирожных, пирожках и хлебе были выявлены опиум, LSD, кокаин и т. п. Наркосиндикат принял решение не просто совершить налет на эту пекарню, но и захватить двух неудачливых владельцев-докторантов, принудив их в дальнейшем поделиться своими производственными секретами и передать под пытками все ноу-хау наркосиндикату. Поэтому служба по борьбе с наркотиками в Сан-Диего решила сыграть на опережение и провела аресты с одновременным изъятием обо-

рудования пекарни, а также была вынуждена эвакуировать своего ценного агента под прикрытием из Мексики, доставив его назад в США.

Уже после выхода книги Гудмана, в 2015 г., группа биоинженеров из Стэнфорда переделала ДНК обычных («пекарских») дрожжей так, чтобы те синтезировали наркотики-опиаты. В природе дрожжи делают из сахара спирт, а здесь на входе все тот же простой сахар, а вот на выходе — очень похожая на героин молекула. Это серьезная новость для правоохранительной системы.

Опиаты — это очень сложные с точки зрения химической структуры молекулы. В 1947 г. только за выяснение этой структуры дали Нобелевскую премию, и понадобилось еще пять лет, чтобы химики научились синтезировать морфин с нуля — в 31 шаг, с выходом в 0,06%. Дрожжи в пробирке делают то же самое в разы быстрее.

Человек со щепоткой наркотика, украденного из лаборатории, имел именно щепотку наркотика. А человек со щепоткой генно-модифицированных дрожжей имеет запас наркотика на многие годы для себя, соседнего подъезда и всего района, потому что дрожжи — живой организм, который умеет размножаться, им можно поделиться, как пенсионеры делятся чайным грибом, а сам процесс синтеза не сложнее, чем варка пива. Значит, и предотвращать его нужно будет какими-то новыми способами, правилами и законами. Иначе готовые биомашины для производства наркотиков или патентованных лекарств будут распространяться так же неподконтрольно, как нелицензионные копии фильмов и музыки в торрент-сетях.

Биоинженеры из Университета Конкордии в Квебеке (Канада) сделали потенциально опасный шаг в сторону синтетических опиатов, пытаясь воспроизвести внутри дрожжей работу наиболее сложной части той цепочки ферментов, которая отвечает за производство морфина и прочих опиатов в клетках мака. Эта часть «конвейера» отвечает за сборку молекул так называемых бензил-изо-хинолинов (БИХ) — сложных органических молекул из трех углеводородных колец, составляющих основу морфина, кодеина, ряда других опиатов, а также несколько десятков антираковых и антиконвульсивных лекарств, которые можно найти внутри маковых головок.

В принципе любой человек, обладающий доступом к такому сорту дрожжей и базовыми навыками по их ферментации, сможет вырастить грибок, производящий морфин, используя обычный набор для домашнего пивоварения, считают эксперты-биотехнологи.

По этой причине все подобные исследования должны проводиться под контролем со стороны наркологических служб, и доступ к их выводам, а также к самим образцам дрожжей должен быть строго ограничен. Если такие дрожжи попадут в руки наркокартелей, то подавить производство таких опиатов будет практически невозможно.

Сочетание технологий синтетической биологии с технологиями 3D-печати приведет к тому, что можно будет просто заказать картридж с определенным набором химических элементов, выбрать в программе нужное вещество и печатать — можно и аспирин, можно и амфетамин.

Раздел III
ПРЕСТУПНИКИ И ДЕВИАНТЫ ЦИФРОВОГО МИРА

Глава 6. Хакеры и иные девианты цифрового мира

§ 1. Хакеры

Хакеры — это основная категория преступников и девиантов в цифровой среде.

Почему не всех хакеров следует называть преступниками? Дело в том, что в 60—70-е гг. XX в. хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым или элегантным способом. Слово «hack» пришло из лексикона хиппи, в русском языке есть идентичное жаргонное слово «врубаться» или «рубить в чем-то». Начиная с конца XX в. в массовой культуре появилось новое значение этого слова — «компьютерный взломщик», программист, намеренно обходящий системы компьютерной безопасности.

О. Б. Скородумова в развитии субкультуры хакеров выделяет ряд этапов[1].

Первый (60-е гг. XX в.) характерен установками на новаторский подход к исследованию программ, провозглашением принципа неограниченного бесплатного доступа для всех к информации, ценностей абсолютной свободы. На начальном этапе развития глобальной сети Интернет хакерское движение не носило деструктивного характера, отражало тенденцию творческого новаторства, исследования пределов систем, их потенциальных возможностей. Экспериментирование не преследовало достижения корыстных целей или нанесения ущерба. В этот период для сообщества хакеров, куда входили студенты и профессора крупнейших университетов и научно-исследовательских центров США, характерны дух взаимного сотрудничества, демократизм, собственный четко обоснованный этический кодекс. Важнейшая особенность субкультуры хакеров на данном этапе — представление о собственной избранности, элитарности. Многие из них оценивали себя как первопроходцев, создающих новое общество, основанное на ценностях глобального киберпространства.

[1] См.: *Скородумова О. Б.* Хакеры как феномен информационного пространства // Социологическое исследование. 2004. № 2.

Второй этап (конец 70-х гг. — начало 80-х гг. XX в.) — переход от новаторского исследования к несанкционированному вторжению в чужие системы, повышение агрессивности, использование знаний в целях протеста, удаление или изменение важных данных, распространение компьютерных вирусов и т. п. Для обозначения этой категории хакеров используется термин *кракер* (англ.: cracker — взломщик) — лицо, изучающее систему с целью ее взлома. Именно кракеры реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения. Они применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого обмена. Техническими и социально-экономическими причинами являлись: доступность компьютера широкому кругу лиц, в том числе и программистам-любителям; ужесточение конкуренции среди компьютерных фирм; машинная и программная несовместимость, ведущая к объективной потребности во взломе и доработке программ; повышенное внимание средств массовой информации к фактам взлома систем и создание ореола «героя» вокруг взломщика.

В зависимости от мотивов деятельности хакеров для этого этапа выделяются следующие группы:

— *«белые» хакеры* — малочисленная группа, оказывающая помощь программистам и пользователям в совершенствовании управления компьютером и виртуальными сетями, модернизации и создании новых программ, борьбе с «черными» хакерами;

— *«черные» хакеры*, или *кракеры*, занимаются несанкционированным доступом к сетям и информации.

В зависимости от целей деятельности в кракерской среде выделяются следующие группы:

— *вандалы*, главная цель которых — взломать систему для ее дальнейшего разрушения;

— *шутники* — действуют для достижения известности путем взлома компьютерных систем и внесения туда различных юмористических (с их точки зрения) эффектов;

— *взломщики* — профессиональные кракеры, действующие с преступной целью кражи или подмены хранящейся информации;

— *пираты* — воруют свежие программы с помощью средств, самостоятельно разработанных или заимствованных у взломщиков, и обладают определенной специализацией;

— *пираты-взломщики* — взламывают компьютерную защиту;

— *пираты-курьеры* — копируют ворованное программное обеспечение на свой компьютер;

— *пираты-дистрибьюторы* — занимаются распространением ворованного программного обеспечения;

— *шпионы* — охотятся за секретной информацией;

— *кардеры* — используют чужие (ворованные) кредитные карты для электронной оплаты товаров или услуг;

— *фишеры* — интернет-мошенники, выдающие свои страницы за сайты других;

— *фрикеры* — осуществляют взлом телефонных автоматов и сетей, обычно с целью получения бесплатных звонков или связи с Интернетом;

— *спамеры* — занимаются формированием и рассылкой непрошеной корреспонденции рекламного характера и обладают внутренней специализацией;

— *спамеры-кракеры* — создают программы для сбора адресов компьютеров пользователей с сайтов и форумов и превращения их в машины для рассылки спама;

— *спамеры — собиратели баз данных* — обслуживают нужды рассыльщиков и собирают для них почтовые адреса, которые объединяют в базы адресов;

— *спамеры службы рассылок* — рассылают спам.

В качестве социальной базы индустрии, обслуживающей кракеров, традиционно выступают:

— *клаберы* (постоянные посетители компьютерных клубов);

— *геймеры* (любители компьютерных игр) как агенты, разносящие вирусосодержащее программное обеспечение и спам[1].

Третий этап (80—90-е гг. XX в.) — стремление к созданию организованных структур, сращивание хакерской субкультуры с криминальным миром.

В этот период хакерское движение становится мощной силой, способной дестабилизировать общественные структуры, превращается в один из объектов изучения правоохранительными органами.

Хакеры точно рассчитывают рациональность методов взлома защиты компьютерной системы, разрабатывают программы действий, обеспечивающих анонимность атаки, никогда не действуя под собственным именем и тщательно скрывая свой сетевой адрес. Мировоззренческое обоснование взлома — отличительная черта хакеров этого периода. Наиболее распространенными становятся следующие виды атак: на системы управления базами данных, на операционные системы и сетевое программное обеспечение.

Хакеры широко применяют методы социальной инженерии, уделяя повышенное внимание манипулированию людьми и созданию программируемой модели поведения человека, о чем свидетельствует

[1] См.: *Масленченко С. В.* Субкультура хакеров как порождение информатизации общества: дис. ... канд. культурологии. СПб., 2008.

«обмен опытом» на хакерских сайтах. Они используют и целенаправленно формируют факторы, способные привести к сознательному или неумышленному соучастию в разрушении систем информационной защиты организации: неудовлетворенность сотрудника (сотрудников) социальным статусом или материальным положением; формирование политико-идеологических, нравственных, религиозных, бытовых ориентаций, противоречащих установкам фирмы; создание экстремальных ситуаций на личностном (семейном, сексуальном, финансовом и т. д.) уровне; давление на субъекта путем шантажа или обмана; имитацию ранговых различий с целью получения необходимой информации; воздействие на психофизические и физиологические системы организма с использованием гипноза, психотропных препаратов, наркотиков и т. п.

Четвертый этап (конец 90-х гг. XX в. — начало XXI в.) — институализация хакеров: создание крупных объединений, союзов, фирм, тесным образом сотрудничающих с криминальными и теневыми структурами.

Активизировано взаимодействие хакеров с мафиозными структурами и террористическими организациями. Сформировался и развивается *особый вид бизнеса — аренда хакеров*, хакерство как услуга.

В США примерно с 2008 г. все аресты по уголовным делам, связанным с киберпреступностью, преподносятся и в СМИ, и в официальных прокурорских документах, и даже в судебных решениях как разоблачение одной гигантской киберпреступной группы, что-то наподобие *кибер-орды*. Все подозреваемые и уже осужденные в США позиционируются как члены единой преступной организации[1].

После событий в Украине 2014 г. всех разоблаченных хакеров обвиняют в том, что они входили в одну группу, управляемую из Москвы. Американские СМИ пишут о том, что за 10 лет борьбы с киберпреступностью многие члены глобальной кибербанды арестованы, но часть преступников якобы находится в России под покровительством госструктур.

С июня 2016 г., когда газета Washington Post сообщила, что «российские хакеры, пользующиеся поддержкой государственных структур», проникли в серверы национального комитета Демократической партии США, Россия стала позиционироваться в США и ЕС как «империя киберзла».

Обвинение одной страны — России в покровительстве хакерам — это метод информационной войны. Ведь сегодня ни для кого не секрет, что спецслужбы стран, серьезно относящихся к киберпространству, в первую очередь США, ЕС и Китая, активно вербуют талантли-

[1] См.: *Муртазин И.* Кибер-орда // Новая газета. 2017. 28 июня.

вых хакеров для работы в «интересах государства», и гражданская принадлежность специалиста в этом случае не имеет значения.

Например, хорошо известна массированная кибератака на американские компьютерные сети, произошедшая в 1999 г. после авианалета ВВС США на Белград, когда в результате «фатальной ошибки» было уничтожено здание посольства Китая. Такая же мощная кибератака на США была произведена китайскими хакерами в 2001 г. после столкновения разведывательного самолета США с китайским истребителем. В 2003 г. хакеры из Китая провели операцию Titan Rain, атаковав компьютерные ресурсы Министерства обороны США.

В компьютерном мире хорошо известна китайская хакерская группа NCPH, создавшая десятки программ, использующих пробелы в Microsoft Office, для внедрения в систему вирусных подпрограмм, которые позволяют дистанционно управлять зараженными компьютерами, копировать нужные документы и передавать их по нужному адресу.

При этом NCPH — не единственная хакерская группа, действующая в интересах Китая. Подобных групп в КНР десятки.

Хорошо известны в компьютерном мире и хакерские группы, ведущие локальные кибервойны. Хакеры из Греции традиционно обмениваются ударами с хакерами из Турции. Пакистанские хакеры наносят удары на компьютерные системы Индии, а индийские, наоборот, по пакистанским.

Иногда сотрудничество оборачивается тем, что хакеры и курирующие их сотрудники спецслужб начинают совместно действовать уже в своих личных, преступных интересах. Яркий пример такого криминального «сотрудничества» — дело «Шалтая-Болтая», когда киберпреступники, специализирующиеся на взломе электронных почтовых ящиков, оказавшись под патронажем офицеров Центра информационной безопасности ФСБ, начали выставлять на продажу содержимое переписок российского политико-экономического бомонда.

«Крышевание» киберпреступников офицерами спецслужб — это не уникальное явление, присущее только России. Подобные истории периодически вскрываются в том числе и в США. Например, несколько лет назад получил всемирную известность агент Secret Service Ш. Бриджес, занимавшийся расследованием деятельности подпольного биткойн-рынка Silk Road. Выйдя на след кибербанды, Бриджес взял преступников под свой патронаж и в результате лишь двух кибератак получил свою долю биткойнов на сумму около 800 тыс. долл. США, которые затем обналичил[1].

[1] См.: *Муртазин И.* Указ. соч.

§ 2. Хактивисты

Хактивисты — это одна из разновидностей хакеров, преследующих не меркантильные, а политические цели.

Хактивизм (англ.: hacktivism — от «хакер» и «активизм») — использование компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации.

Исследователь хактивизма Ф. Паже полагает, что свои идеи хактивизм черпает из политического активизма, для которого характерен акцент на акции прямого действия. Примерами акций прямого действия могут служить акции членов «Гринпис», выходящих в открытое море, чтобы помешать ведению китобойного промысла; мирный захват парка в центре Нью-Йорка тысячами активистов по призыву организации Adbusters в рамках «Захвати Уолл-стрит» в июле 2011 г.

Если добавить к политическому активизму сетевую активность хакеров (действующих как с добрыми, так и со злыми намерениями), мы получим хактивизм. Существует мнение, что английское слово «hacktivism» впервые было использовано в статье Дж. Сэкаг, опубликованной в InfoNation в 1995 г. В 1996 г. этот термин появился в статье, опубликованной в Интернете членом американской группы Cult of the Dead Cow (cDc). В 2000 г. О. Раффин, другой член этой группы, написал, что хактивисты используют технику для защиты прав человека. Многие активисты, разделяющие *либертарианские идеалы* (стремление к сохранению свободы предпринимательства, гражданских свобод, свободы слова и свободы обмена информацией), выступают также в защиту свободы Интернета. Олицетворением хактивизма является *движение Anonymous*. С самого начала акции участников Anonymous были направлены на защиту своего понимания того, каким должен быть Интернет. Со временем они расширили свои формы борьбы, перейдя от интернет-акций к уличным протестам.

Ф. Паже выделяет в хактивизме три основные группы:

1) Anonymous — самая освещаемая в СМИ составляющая движения. Члены этой группы известны своей поддержкой свободы Интернета и выступлением против всех, кто, как они считают, мешает обмену информацией. К используемым ими методам относятся, как правило, взлом (включая DDoS-атаки), а также кража и распространение личной и (или) конфиденциальной информации. Они любят низкопробные шутки, а порой даже кажется, что они не преследуют никаких политических целей;

2) киберзахватчики — настоящие активисты. Они используют Интернет и социальные сети прежде всего для завязывания контактов, а также для пропаганды и распространения информации. К ним относятся кибердиссиденты, которые, как и их аналог в реальной жизни, больше не признают легитимность той политической власти, которой их заставляют подчиняться. Предпринимая попытки проведения крупных акций в Интернете, они надеются укрепить демократию и бороться с коррупцией в своих странах;

3) кибервоины, или патриоты, которые объединяются в «киберармии», процветающие во многих странах с тоталитарными тенденциями. Если верить их словам, то, поддерживая национальные и экстремистские движения, они действуют по поручению государственных органов своих стран. Основным методом их борьбы является искажение внешнего вида веб-сайтов. Помимо этого они делают все возможное для борьбы с диссидентами, используя для этого DDoS-атаки[1].

Подобно тому как некоторые активисты нелегально проникают на территорию атомных электростанций и другие объекты частной собственности, хактивисты нелегально проникают в частные цифровые зоны. Из-за отсутствия внутренней структуры некоторые проводимые хактивистами операции не выходят за пределы низкопробных шуток (lulz — лулзы), а есть и такие, которые могут быть связаны с мафиозной деятельностью (например, с кражей банковских данных). Подобные хакерские акции нередко имеют сомнительную ценность и сложны для понимания. Такая явная беспорядочность в выборе целей заставляет предположить, что некоторые из хактивистов ведут двойную игру, используя маску политического хактивизма для прикрытия противоправных действий. «Белые» хакеры отмечают: неэтичный характер многих операций заставляет предположить, что некоторые хактивисты, возможно, действуют по указке разведслужб ряда государств[2].

Хактивизм — как связанный с деятельностью Anonymous, так и не связанный с ней — стал значительным явлением современного мира. Если 10 лет зазад преступники поняли, что Интернет может стать одним из основных плацдармов для их деятельности, то в 2010 г. многие интернет-пользователи открыли для себя тот факт, что Интернет может стать общим пространством для организации протестов. В 2010 и 2011 гг., следуя примеру группы Anonymous, к тому времени уже взявшей на вооружение данную концепцию, хактивисты развили бурную деятельность.

[1] См.: *Паже Ф.* Хактивизм. McAfee Labs, 2014.

[2] Там же.

Ж. Носетти и Е. Черненко в записке Валдайскому международному дискуссионному клубу «“Киберкрит”, которого нет (пока)» (июнь 2017 г.) пишут, что в 2010—2011 гг. поднялся глобальный хактивистский бунт. Тогда тысячи хакеров, да и обычных пользователей со всего мира, объединили свои усилия, чтобы отомстить властям США и ряда других стран за давление на WikiLeaks. Основатель WikiLeaks Дж. Ассанж многими воспринимался как главный борец за свободу слова, а его детище — как символ новой эпохи, при которой государства не смогут утаивать информацию от граждан. Возмущенные утечкой в Сеть сотен тысяч секретных документов власти США пытались заставить компании отказаться от сотрудничества с WikiLeaks. Под давлением Вашингтона контракты с порталом разорвали несколько крупных платежных систем и хостинговых сервисов. Дж. Ассанжу стало куда сложнее принимать пожертвования и поддерживать доступность портала.

За WikiLeaks вступилось хактивистское движение Anonymous. К рубежу 2010—2011 гг. оно уже существовало несколько лет, но было известно лишь в узких кругах — в основном за счет нескольких успешных взломов электронных ресурсов Саентологической церкви, а также активными действиями в поддержку торрент-трекера Pirate Bay («Пиратская бухта»). Объявив о начале Operation Payback (Операция «Возмездие»), они стали собирать под своими знаменами тысячи неравнодушных пользователей со всего мира. Их девизом стали слова Дж.-П. Барлоу, одного из создателей правозащитной организации Electronic Frontier Foundation («Фонд электронных рубежей»): «Первая серьезная информационная война началась. Поле битвы — WikiLeaks. Солдаты — это вы».

Принять участие в наступлении на недружественные WikiLeaks сайты мог каждый желающий: пошаговые инструкции по тому, как осуществить DDoS-атаку при помощи простой программы (Low Orbit Ion Cannon или LOIC, «Низкоорбитальная ионовая пушка»), распространялись в тематических чатах и в сети микроблогов Twitter. В итоге к атакам на сайты MasterCard, Visa, Paypal и Amazon присоединились пользователи со всех континентов. Абсолютное большинство из них никогда раньше хакерством не занимались.

Массовость обеспечила успех кампании — несколько правительственных и коммерческих ресурсов удалось на время вывести из строя. В 2012 г. американский журнал Time включил Anonymous в список ста наиболее влиятельных людей года.

Многие эксперты тогда сочли, что хактивизм будет только набирать обороты и что впредь политически мотивированные пользователи будут подобным образом реагировать на любую несправедливость.

Однако вскоре эта волна стихла и в таком масштабе больше не повторялась.

Ж. Носетти и Е. Черненко считают, что причин тому, что за первым кибербунтом не последовали другие, несколько. Во-первых, у движения Anonymous не было лидера или хотя бы некоего ядра, которое взяло бы на себя координацию совместных действий и мотивировало участников на продолжение борьбы. В прессе от имени движения мог выступить любой из его членов. В чатах, где обсуждались цели и время атак, также все происходило довольно хаотично, а после первых успешных диверсий там начались ожесточенные споры относительно дальнейших мишеней. В то время как большинство «анонимов» с Запада продолжали дисциплинированно атаковать сайты отказавшихся от сотрудничества с WikiLeaks платежных систем, среди русскоязычных хактивистов начали раздаваться призывы «ударить по Пентагону».

Во-вторых, многие из тех, кто изначально симпатизировал Ассанжу, вскоре разочаровались в нем. Одних отпугнули предъявленные ему обвинения в сексуальных домогательствах. Других смутило, что WikiLeaks начали один за другим покидать ключевые сотрудники, обвинившие Ассанжа в нецелевом расходовании многомиллионных пожертвований. Третьи не согласились с решением Ассанжа выкладывать в Сеть секретные документы «без купюр», т. е. со всеми именами и адресами, несмотря на то, что это создавало угрозу жизни для некоторых из упомянутых лиц (например, информаторов американских войск в Афганистане).

В-третьих, как только Anonymous начали активно рекрутировать сторонников в Facebook и Twitter, их аккаунты были заморожены, а несколько их сайтов (например, Anonops.net) сами подверглись атаке и надолго «легли на дно». Лишенные площадки для общения «анонимы» долго не могли собраться с силами. Среда, благодаря которой хактивисты появились на свет, оказалась их ахиллесовой пятой.

Ну и, наконец, угасанию бунта явно способствовало преследование членов движения со стороны правоохранительных органов США. После нескольких громких арестов и показательных судебных процессов количество желающих поучаствовать в атаках заметно поубавилось. Примечательно, что действия хактивистов осудил и их кумир Дж.-П. Барлоу, назвавший DDoS-атаки «ядовитым газом киберпространства»[1].

Anonymous осуществили еще несколько «операций», уже не связанных с WikiLeaks, однако ни одна из них не была столь успешной, как «Возмездие». Сегодня под брендом Anonymous действует несколько разрозненных хакерских группировок, однако они все больше занимаются взломами «just for the lulz» — ради развлечения.

[1] См.: Валдайские записки. 2017. Июнь. № 68.

Угасание первой волны хактивизма не означает, что не будет второй и третьей. Судьба этого общественного феномена будет во многом зависеть от того, найдется ли такой же мощный объединяющий фактор, каким в свое время было желание поддержать WikiLeaks и тем самым отстоять свое право на доступ к информации. Можно предположить, что при наличии общей цели объединить людей в следующий раз будет даже проще, поскольку они уже знают, каких результатов можно добиться сообща. И не факт, что бунтовщики ограничатся одними лишь DDoS-атаками[1].

§ 3. Преступники в сфере детской порнографии

Личностный профиль человека, вовлеченного в изготовление, распространение и хранение детской порнографии с использованием компьютерной техники, может отличаться от личностного профиля киберпреступников в целом. Исследования по этой группе преступников в 2013 г. были представлены Виртуальной глобальной рабочей группой (ВГРГ) в виде ограниченной неслучайной выборки по 103 лицам, арестованным за скачивание и обмен детской порнографией через систему файлообмена.

Возраст и социальный статус. Все подозреваемые из контингента ВГРГ были представлены лицами мужского пола от 15 до 73 лет, средний возраст которых составлял 41 год. Каждый пятый подозреваемый не работал, а находился на пенсии, был безработным или получал социальное пособие по состоянию здоровья. Остальные занимались трудовой деятельностью или учились. 42% проживали совместно с партнером и (или) детьми. Эти преступники были значительно старше (в среднем 50 лет) одиноких правонарушителей (в среднем 35 лет). Все подозреваемые были озабочены сокрытием своих занятий от окружающих, но только 60% удалось полностью обособить их от своей повседневной жизни. Что касается остальных, то их противоправное поведение, как правило, обретало навязчивый характер и было в той или иной мере переплетено с их повседневной жизнью и, возможно, не очень хорошо скрыто от окружающих. К этой второй группе, как правило, относились лица низкого социально-экономического статуса и высокого уровня компьютерной грамотности, около 4% преступников имели проблемы с психическим здоровьем.

Схема противоправного поведения. Подозреваемые были вовлечены в преступления в сфере детской порнографии, как правило, в течение

[1] См.: Валдайские записки. 2017. Июнь. № 68.

сравнительно длительного периода времени — в среднем 5 лет при диапазоне от 6 месяцев до 30 лет. Более 60% подозреваемых не только собирали детскую порнографию, но и торговали ею (распространяли ее) через файлообменные сервисы, а 35% использовали в этих целях иную сеть (иные сети) помимо файлообменных. Из них половина была связана между собой вне Интернета, что свидетельствует о том, что лица, выходящие за рамки просмотра детской порнографии, торгуя ею, занимаются этим не только через Интернет, но и офлайн.

Взаимосвязь с преступной деятельностью офлайн. Что касается преступников, работающих онлайн и офлайн, т. е. сетевых преступников, то они чаще всего являются европейцами, безработными и по возрасту незначительно моложе внесетевых преступников. Тем не менее взаимосвязь может иметь место. Согласно результатам одного из исследований ООН (2013) по выборке из свыше 3500 сетевых преступников в сфере детской порнографии каждый шестой был также причастен к сексуальному насилию над детьми офлайн. По данным исследования ВГРГ, 6% ранее подвергались преследованию за сексуальную эксплуатацию детей через сеть Интернет, 18% привлекались к ответственности за развратные действия в отношении детей младше 16 лет, а 15% привлекались к ответственности за преступления несексуального характера. Существовало небольшое частичное совпадение между преступлениями сексуального и несексуального характера, что свидетельствовало в пользу склонности подозреваемых к специализации на преступлениях сексуального характера в отношении детей. Подозреваемые с высокой степенью вовлеченности в сферу детской порнографии в сети Интернет также входили в число лиц, которые были причастны либо являлись причастными на тот момент к сексуальному насилию над детьми.

Другое исследование, «Butner Study», акцентировало внимание на преступниках в сфере детской порнографии и проводилось посредством сравнения групп преступников, участвующих в программах добровольного лечения, на основе наличия дополнительной истории сексуальных преступлений в форме «непосредственного контакта» в отношении по крайней мере одного ребенка. Результаты исследования подчеркивают большое значение того факта, что взаимосвязь между просмотром детской порнографии и сексуальными домогательствами к детям имеет сложную взаимообусловленность. Было установлено, что действующие в сети Интернет преступники были с гораздо большей вероятностью причастны к сексуальному насилию над детьми путем непосредственного контакта, многие (из них) могут быть скрытыми педофилами, и использование ими детской порнографии служит признаком их парафильного расстройства. Если бы не их противоправная деятельность в сети Интернет, эти преступники могли бы так и не попасть в поле зрения правоохранительных органов.

В целом для преступников из выборки ВГРГ был характерен относительно высокий уровень прошлого и параллельного опыта преступлений, связанных с сексуальным насилием над детьми вне сети Интернет. В отношении более чем половины подозреваемых с судимостями за сексуальное насилие над детьми имелись доказательства продолжения ими связанной с этим деятельности.

§ 4. «Группы смерти» в Интернете

Вопрос о суицидальных группах смерти в Интернете остро встал при публичном обсуждении и реагировании правоохранительных органов России на публикацию 15 мая 2016 г. в «Новой газете» статьи Г. Мурсалиевой «Группы смерти». Именно из этой публикации широкая общественность узнала о существовании сообществ в социальной сети «ВКонтакте», которые вовлекают подростков в смертельную игру, последним шагом в которой должно стать самоубийство. Доведение до самоубийства проходило в ходе «квеста», «завербованным» в который давались индивидуальные номера, 50 дней на принятие решения, по истечении которых они должны были совершить «самовыпиливание». Автор статьи приводит элементы культа — изображение китов и бабочек (киты якобы выбрасываются на берег, таким образом спасаясь от неурядиц).

Весь 2016 г. шли дискуссии на данную тему с участием общественных организаций, органов государственной власти и социальных сетей. Роскомнадзор продолжал свою деятельность по блокированию страниц с информацией о способах совершения суицида или призывами к его совершению. Кстати, с 1 ноября 2012 г. к началу 2017 г. им было заблокировано 9357 подобных страниц.

20 февраля 2017 г. Президент России В. В. Путин поручил Правительству РФ принять решения, направленные на совершенствование системы профилактики подросткового суицида. Спустя несколько дней в Государственную Думу РФ был внесен законопроект об уголовной ответственности за склонение детей к самоубийству. Проект был поддержан и Президентом, и Правительством РФ. Законопроект прошел все стадии принятия в ускоренном темпе — фактически за три месяца. Параллельно резко активизировались правоохранительные органы. МВД России и Следственный комитет РФ начали интенсивно заниматься «группами смерти» и их организаторами. Произошел первый арест создателя «группы смерти»[1].

[1] См.: «Группы смерти» стали проверкой для государства и общества в России. URL: https://vz.ru/society/2017/6/9/873862.print.html.

Клубы самоубийц существовали с древнейших времен во многие исторические эпохи: в Древнем Египте при Клеопатре, в Германии 1819 г., в Вене 1824 г., в США начала XX в. Но виртуальные сообщества сторонников суицида отличаются от своих традиционных предшественников многочисленностью, отсутствием географической привязанности и свободным доступом лиц любого возраста. Эта проблема носит общемировой характер — виртуальная культура суицида появилась практически одновременно с развитием Интернета и распространяется по миру одновременно с ним. Исследования показывают, что большинство посетителей форумов и сайтов о самоубийстве моложе 25 лет. Некоторые индивиды состоят сразу в нескольких виртуальных сообществах, посвященных суицидам. Формально это закрытые группы, но для получения допуска к информации в них необходимо просто подписаться на группу или написать о своих переживаниях редактору сайта или создателю группы в социальной сети[1].

Период от возникновения суицидальных мыслей до попытки их реализации называют пресуицид: индивид находится в состоянии угнетающего аффекта, его мрачные мысли усиливаются, неудовлетворенность жизненными условиями растет. Материалы, размещенные на личных страницах в социальных сетях участников виртуальных клубов самоубийц, показывают, что они испытывают депрессию и страдают от одиночества. Такое настроение является благоприятной почвой для внушения и развития угнетающего настроения, характерного для пресуицидального периода.

В Интернете легко найти информацию о способах и местах совершения суицида. Контент виртуальных клубов самоубийств направлен на доведение его участников до суицида. Опасность открытого доступа индивида к подобной информации подчеркивает рекомендация Всемирной организации здравоохранения: нельзя публиковать в СМИ фотографии и предсмертные записки самоубийц, а также сообщать о конкретных способах совершения суицида[2].

[1] См.: *Ключко Е. И.* Воздействие Интернета на суицидальное поведение молодежи // Terra humana. 2014. № 1.

[2] См.: Предотвращение самоубийств (SUPRE) // Всемирная организация здравоохранения. URL: http://www.who.int/mental_health/prevention/suicideprevent/ru/index.html (дата обращения: 25.02.2013).

Детальное исследование данной проблемы проведено Российской академией народного хозяйства и государственной службы при Президенте РФ, Институтом общественных наук, Школой актуальных гуманитарных исследований и Лабораторией теоретической фольклористики (см.: «Группы смерти»: от игры к моральной панике. М., 2017).

§ 5. Сетевые «тролли» и иные группы травли в Интернете

В виртуальном мире кроме сообществ, рассказывающих о преимуществах самоубийства, молодой человек может столкнуться с проблемой травли (троллинга).

Троллинг — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.

Прямую аналогию из обычной жизни для явления троллинга подобрать нелегко. Ближайшие понятия — это искушение, провокация и подстрекательство, т. е. сознательный обман, клевета, возбуждение ссор и раздоров, призыв к неблаговидным действиям[1].

Термин «троллинг» происходит из сленга участников виртуальных сообществ и не имеет прямого отношения к сфере научного дискурса (дословно англ.: trolling — ловля рыбы на блесну). В наиболее общем виде это явление характеризуется как процесс размещения на виртуальных коммуникативных ресурсах провокационных сообщений с целью нагнетания конфликтной обстановки путем нарушения правил этического кодекса интернет-взаимодействия. В качестве таких действий могут выступать волны правок — искажение первичных текстов (постмодерация сообщений, тем, новостей) — флейм (англ.: flame — пламя, огонь) либо бесцельная конфронтация — холивары (англ.: holy war — священная война).

Основными местами осуществления троллинга могут выступать различные тематические форумы, конференции, социальные сети, порталы, чаты и новостные сайты. Тролль представляется типичным пользователем, который разделяет общие интересы и проблемы группы либо сообщества.

В отношении пользователя, осуществляющего троллинг, утвердилось обозначение «тролль». Это слово приобрело популярность из-за другого его значения — существо, упоминаемое в скандинавской ми-

[1] См.: URL: https://ru.m.wikipedia.org/wiki/Троллинг. См. также: *Семенов Д. И., Шушарина Г. А.* Сетевой троллинг как вид коммуникативной деятельности // Международный журнал экспериментального образования. 2011. № 8; *Акулич М. М.* Троллинг в социальных сетях: возникновение и развитие // Вестник РУДН. Серия: Социология. 2012. № 3; *Загидуллина М. В.* Развитие интернет-троллинга и проблемы «Шума» в канале коммуникации // Вестник Челябинского государственного университета. 2013. № 31 (322). Филология. Искусствоведение. Вып. 84; *Строителев Н. М., Сабурова Н. А.* Происхождение и эволюция троллинга: от провокационного речевого поведения до субкультурного феномена // Ученые заметки ТОГУ. Электронное научное издание. 2016. Т. 7. № 3 (2).

фологии. Мифологические существа тролли, особенно в детских рассказах, изображаются в качестве уродливых, неприятных существ, созданных для причинения вреда и сотворения зла.

Оксфордский словарь английского языка впервые упоминает троллинг в связи с Интернетом в 1992 г., называя две версии происхождения: мифологическую и рыболовную.

С начала XXI в. интернет-троллями начали создаваться *собственные сетевые сообщества* и организации для обмена опытом по наиболее эффективному разжиганию конфликтов. Первое упоминание троллинга в академической литературе произошло в 1996 г. и принадлежит Дж. Донат, которая описала троллинг как умышленно вредоносную ложь, отмечая, что тролли способствуют быстрому снижению доверия и терпимости к чужакам, а также способствуют развитию паранойи в онлайн-сообществе.

О том, почему люди занимаются сетевым троллингом, У. Филлипс в книге «Трололо»[1] пишет: помимо самоидентификации как таковой тролли мотивированы тем, что называют лулзами. *Лулзы* — особая разновидность несочувственного, трудно истолковываемого посторонними смеха. Они напоминают немецкое понятие «Schadenfreude», которое можно приблизительно перевести как «радость от несчастий кого-то вам неприятного». Но зубы у лулзов гораздо острее. Лулзы также свидетельствуют о специфической комической и визуальной эстетике.

Утверждение (и очень распространенное в мире троллей), что перед лулзами все равны, опровергается тем фактом, что значительная доля лулзов направлена на небелых (особенно афроамериканцев), женщин, а также на лесбиянок, геев, бисексуалов, трансгендеров и квир-индивидов (ЛГБТК). При этом исторически доминирующие группы также часто являются источником лулзов. «Белые христиане», и республиканцы особенно, наряду с группами белых людей, объединенных общим делом (в первую очередь это экологи и сообщества фанов), вызывают изрядное количество троллинга. Хотя на первый взгляд эти мишени кажутся совершенно разными, тролли выбирают жертв, руководствуясь общим принципом — пригодностью для эксплуатации. Тролли считают, что ничто на свете не следует принимать всерьез, и потому расценивают публичные проявления сентиментальности, политических убеждений и (или) идеологической ограниченности как призыв к троллингу.

Последний признак троллинга — тролли настаивают на анонимности и поднимают ее как знамя. Возможность скрыть свою офлайновую

[1] *Филлипс У.* Трололо. Нельзя просто так взять и выпустить книгу про троллинг. М., 2016.

личность имеет ряд важных поведенческих последствий. Самое очевидное из них — анонимность позволяет троллям совершать поступки, которые они никогда не повторили бы в профессиональной или иной публичной обстановке. И, напротив, успешность троллинга часто зависит от отсутствия анонимности мишени или по крайней мере от ее готовности раскрыть свои привязанности, интересы и уязвимые места в реальной жизни. Для троллей это основание для незамедлительного троллинга, поскольку в понимании троллей Интернет является — хотя бы должен быть — зоной, свободной от привязанностей.

В последнее время троллинг все шире используется как PR-технология в коммерческой, политической и даже внешнеполитической сферах.

По мнению ученых из Оксфордского университета, подготовивших исследование «Войска, тролли и возмутители спокойствия: глобальный обзор организованных манипуляций соцсетями», правительства по всему миру создают «кибервойска», которые занимаются манипулированием в Facebook, Twitter и других соцсетях. Манипуляции в Интернете используются для управления общественным мнением, распространения дезинформации и подрыва позиций критиков. При этом согласно исследованию демократические и авторитарные режимы не слишком сильно различаются в этом отношении.

Авторы изучили ситуацию в 28 странах, где правительства применяют технологии для манипулирования общественным мнением. Речь идет о самых разных способах — как комментировании, целевом индивидуальном подборе получаемой пользователем информации и создании спонсируемых правительством сайтов и страниц, так и о фейковых новостях и подготовке специального контента, размещаемого в соцсетях. Соцсети делают пропагандистские кампании более сильными и потенциально более эффективными, чем в прошлом.

Правительства заимствуют применяемые в Интернете технологии и у оппозиционных активистов, которые распространяли информацию и привлекали сторонников через Интернет. При этом речь идет не только непосредственно о правительственных подразделениях, занимающихся манипулированием общественным мнением, но и о связанных с правительством партиях, организациях и частных лицах[1].

Есть и иные «группы травли» в Интернете, которые занимаются:

— пранком (телефонным хулиганством). Пранкер разыгрывает жертву по телефону, при этом записывая разговор, который и выкладывает в Интернет;

— «навязчивым спамом» — закидыванием жертвы сообщениями различного содержания — рекламным текстом или любым бессмыс-

[1] См.: Коммерсантъ. URL: http://kommersant.ru/Online?date=2017-7-18.

ленным набором слов. Цель — вывести жертву из себя потоком навязчивых сообщений;

— деанонимизацией, т. е. раскрытием имени пользователя в ситуации анонимного интернет-общения, установлением авторства какого-либо текста, рисунка вопреки желанию автора и т. д.;

— созданием групп против травимого в социальных сетях или даже сайтов;

— созданием страниц, аккаунтов от имени травимого в различных социальных сетях, журналах; пишутся (якобы жертвой) разного рода компрометирующие, грубые тексты. Это называют «атакойклонов»;

— взломом учетной записи, аккаунта жертвы и рассылкой с ее страницы различной информации;

— распространением компромата, слухов, сплетен, в том числе выкладыванием различного рода личных документов, фотографий и видеороликов (нередко поддельных) в социальных сетях и т. п.;

— съемками жертвы тайком или принудительно на видео, обычно в унизительном положении, после чего запись выкладывается на YouTube или другом популярном видеохостинге.

§ 6. Деструктивные секты в Интернете

Как известно, *деструктивная секта* — термин, используемый социологами, психологами, криминологами, богословами по отношению к религиозным, неорелигиозным и другим группам и организациям, причинившим (причиняющим) вред обществу или своим членам (материальный, психологический или физический). Часто секты именуют *тоталитарными*, когда они обвиняются в доведении до самоубийства и убийствах людей, торговле людьми, употреблении и распространении наркотиков.

Прецеденты, когда киберпространство содействовало культовому и религиозному насилию, известны с момента появления Интернета. Так, согласно японскому изданию Japanese Newspaper Reports, когда токийская полиция изъяла множество CD-дисков из здания, принадлежащего террористической секте «Аум Синрикё», в них были обнаружены длинные списки электронных адресов, принадлежавших студентам японских колледжей. Силовые структуры убеждены, что секта могла использовать свыше 40 тыс. email-контактов для вербовки новых членов из числа учащейся молодежи[1].

Хронологически первым деструктивным культом, имевшим представительство в Интернете, стала община «Небесные врата». Общест-

[1] См.: *Яковлева М. Г.* Особенности представительства деструктивных сект и экстремистских религиозных организаций в Интернете // Homo cyberus: электронный научно-публицистический журнал. URL: http://homocyberus.ru.

венную огласку секта получила в марте 1997 г. после коллективного самоубийства своих членов на одном из ранчо Калифорнии. Культовый суицид был приурочен к приближению кометы Хейла — Боппа, за которой, как полагали члены общины, летит космический корабль, предназначенный для того, чтобы забрать их души в межгалактическое путешествие. Примечательно, что секта «Небесные врата» имела достаточно эффектный для того времени сайт, делая информацию о жизни общины доступной для всех пользователей Интернета. Веб-страница включала множество ярких графических изображений, но основу контента сайта составляли догматы секты. В дни, непосредственно предшествовавшие массовому самоубийству членов группы, их веб-страница провозглашала: «Красная тревога. Комета Хейла — Боппа приносит конец времен». Эксперты подчеркивают, что секта «Небесные врата» не могла добиться больших успехов в распространении своих идей посредством веб-страницы в 1997 г. по причине того, что Интернет не обладал такой популярностью, как в наши дни. Однако секта во многом опередила свое время, заложив новый вектор развития деструктивной религиозности в современном мире.

Особую опасность деструктивные секты в сети Интернет представляют для несовершеннолетних.

В последние годы в России участились факты, когда подростки под воздействием сектантских сайтов (особенно сатанистских) совершают насильственные преступления.

К насильственным преступлениям, совершаемым несовершеннолетними в ритуальной форме, относятся уголовно наказуемые деяния (убийство, умышленное причинение вреда здоровью различной тяжести, побои, истязание, изнасилование, насильственные действия сексуального характера, вовлечение несовершеннолетнего в совершение преступления и антиобщественные действия, вандализм, жестокое обращение с животными и др.), совершаемые ими в процессе совместного участия в «магических» ритуалах, связанных с их приверженностью к верованиям и оккультным учениям, либо под влиянием таких приверженцев. При этом для насильственных преступлений, совершаемых в ритуальной форме несовершеннолетними, характерны коллективные формы проявления жестокости и агрессивности, порождаемые общим чувством зависимости от сверстников на фоне крушения авторитета взрослых[1].

В зависимости от целей ритуалы, сопровождающие насильственное поведение несовершеннолетних, выражаются в следующем:

— совершение жертвоприношения, в том числе человеческого;

[1] См.: *Семочкина А. А.* Предупреждение насильственных преступлений, совершаемых несовершеннолетними в ритуальной форме: автореф. дис. ... канд. юрид. наук. М., 2016.

— совершение убийства, представляющего собой ритуал мести (может совершаться в том числе и по мотиву религиозной ненависти или вражды);

— совершение насильственного преступления как части обряда посвящения в члены секты;

— совершение насильственного преступления с целью получения органов и тканей живых существ, которые необходимы для последующих ритуальных манипуляций;

— совершение насильственного преступления для «приобретения каких-либо магических способностей»;

— совершение насильственного преступления в целях «вызывания духов и демонов»;

— совершение насильственного преступления в целях гадания (обычно умерщвляется животное);

— совершение акта экзорцизма, т. е. процедуры изгнания бесов и других сверхъестественных сущностей из «одержимого» с помощью молитв, обрядов определенной религии, в результате чего потерпевшему может причиняться физический вред, вплоть до смерти.

Насильственные преступления в ритуальной форме несовершеннолетние в большинстве случаев совершают группой лиц по предварительному сговору, чаще организованной группой. Численный состав может варьироваться от двух человек до 15—20 и больше. Многочисленные группы в основном имеют смешанный возрастной состав и возглавляются совершеннолетними. Каждое третье ритуальное насильственное преступление совершается подростками в отношении лица, заведомо находящегося в беспомощном состоянии, которое обусловлено малолетним возрастом, в силу чего жертва преступления не была способна защитить себя, оказать активное сопротивление виновным, которые осознавали это и рассчитывали воспользоваться этим состоянием жертвы. При этом механизм совершения насильственного преступления несовершеннолетними в ритуальной форме характеризуется тщательной продуманностью действий преступников, их согласованностью, последовательностью и единством[1].

Часто такие насильственные действия снимаются на видео через смартфоны и выкладываются в Сеть.

По статистике, которую ведет Российская ассоциация центров изучения религии и сект, в России сейчас действует более 80 крупных сект и несколько сотен мелких. Это религиозные секты и оккультные. Их членами являются около 1 млн человек. С развитием Интернета вербовка пошла намного интенсивнее, чем раньше, особенно среди де-

[1] См.: *Семочкина А. А.* Указ. соч.

тей — сегодня около 50—60 тыс. детей участвуют в различных оккультных сектах. 80% сект в России вербуют себе сторонников через Интернет[1]. Ежемесячно 50 обращений с просьбой спасти близкого человека из сетей онлайн-секты поступает в Лигу безопасного Интернета[2].

Глава 7. Организованная преступность цифрового мира

§ 1. Особенности современных ОПГ

В 2016—2017 гг. ряд крупнейших мировых форумов выделил в числе 10 наиболее острых международных проблем и рисков мировой экономики организованную преступность. Об этом говорили участники конференции «Двадцатки» в 2016 г. в Ханчжоу (Китай), заседаний Давосского форума 2017 г. и конференции Всемирного банка, посвященной институциональным проблемам и рискам мировой экономики. В ходе этих крупнейших международных форумов их участники выделили одни и те же *10 основных сфер деятельности организованной преступности* в настоящее время и на ближайшие 10 лет:

— финансовые преступления, включая незаконное обогащение, отмыв и преступное перемещение финансовых ресурсов, капиталов и активов;

— производство, хранение, транспортировка и продажа контрафактной продукции;

— хищение и противозаконное использование интеллектуальной собственности;

— преступная деятельность, связанная с производством, хранением, оборотом и сбытом наркотиков;

— незаконная торговля оружием;

— работорговля;

— незаконное изъятие, хранение, транспортировка и использование человеческих органов для трансплантации;

— организованная педофилия;

— незаконный игорный и лотерейный бизнес, включая создание виртуальных казино, противозаконных компьютерных игр, предполагающих безлицензионную монетизацию и т. п.;

— широкий круг преступлений экологического характера, в первую очередь связанных с незаконными операциями с городскими и

[1] См.: *Гросс Ф.* Криминальный RUNET. Темные стороны Интернета. М., 2016. С. 264—282.

[2] См.: URL: http://www.interfax-religion.ru/print.php?act=print_media&id=19203.

промышленными отходами, а также отловом, транспортировкой и сбытом фауны.

Сегодня ОПГ действуют не только в криминальной экономике, но и в легальном секторе, особенно финансовом, принося туда криминальные методы, лежащие за пределами национального и международного законодательств. Имеются многочисленные примеры такого рода симбиоза криминальной и легальной экономик, который становится все более характерным для глобального хозяйства[1]: реализация контрафактных товаров, продажа на легальных рынках интеллектуальной собственности, добытой криминальным путем, использование инсайдерской информации в операциях на фондовых рынках и т. п.

Чем дальше, тем больше симбиоз криминальной и легальной экономик будет формировать ландшафт организованной преступности. Наряду с этим ОПГ сегодня все шире представлены в сферах экономической деятельности, не имеющих однозначного законодательного регулирования. Наличие такого рода серых зон в мировой экономике создает для преступников колоссальные возможности. Наиболее яркими примерами такого рода «серых» зон являются криптовалюты и новые финансовые платформы типа краудфандинга и краудинвестинга. Поскольку в большинстве стран ЕС, а также в Соединенных Штатах криптовалюты рассматриваются не как платежное средство, а как товар, они де-факто легализованы. Легализованы по обе стороны Атлантики краудфандинг и краудинвестинг, а также платформы прямого взаимодействия между потребителями и лицами, оказывающими услуги типа Uber и Airbnb. Подавляющая часть участников этих и подобных платформ являются добропорядочными гражданами и не имеют никакого отношения к преступности. Однако отсутствие детальных нормативных актов и практики правоприменения превращает подобный бизнес в «серую» зону, куда устремляется криминал.

В условиях цифрового мира с всеобщей телекоммуникационной связанностью, вероятно, пора отказаться в определении ОПГ от признака непосредственной связи и личного взаимодействия участников ОПГ. Наряду с компактными ОПГ, о которых и шла речь в определении, данном Конвенцией ООН, все большее распространение получает не только страновая, но и трансграничная сетевая организованная преступность. В строгом понимании сеть и иерархия являются двумя различными типами графов или матриц. В условиях современных телекоммуникаций организованные преступники в целях конспирации часто действуют, не встречаясь лично и даже не зная друг друга в лицо, поддерживая лишь аудио- и текстовую связь.

[1] См.: Доклад Европола «Серьезная и организованная преступность: текущие угрозы. Криминал в век технологий». Февраль 2017 г.

Эксперты Европола отмечают, что ОПГ, действующие в настоящее время в ЕС, весьма разнообразны по своей организационной структуре, функционалу и составу. Они варьируются от крупных традиционных иерархических ОПГ до гибких устойчивых сетевых структур и небольших высокотехнологичных групп, ориентированных на конкретные виды преступности. На начало 2017 г. в ЕС расследовалась деятельность более 5 тыс. ОПГ, работающих на международном уровне. В 2013 г. расследование велось в отношении 3,6 тыс. международных ОПГ в ЕС.

На увеличение численности ОПГ оказывает влияние феномен появления небольших высокотехнологичных преступных групп, работающих на криминальных рынках, сильно зависящих от Интернета. Как правило, в таких группах меньшинство являются профессиональными преступниками, а основной контингент составляют работники IT-компаний, банков и т. п. С известной долей преувеличения такие группы можно обозначить как *ОПГ преступников в свободное от работы время*.

Наибольшую прибыль среди различных криминальных рынков ЕС по-прежнему продолжают приносить наркотрафик, торговля людьми и контрабанда мигрантов, а также финансовая киберпреступность. В то же время наиболее быстрыми темпами растут такие виды преступности, как онлайн-торговля незаконными товарами и услугами, а также онлайн-торговля и туристическая деятельность, связанные с педофилией.

В 2013—2016 гг. преступники из более чем 180 стран были вовлечены в серьезную организованную преступность в ЕС. Большинство ОПГ, действующих на международном уровне в ЕС, состоит из представителей нескольких стран. Большинство подозреваемых, вовлеченных в серьезную организованную преступность в ЕС, — 60% — являются гражданами одного из государств — членов ЕС.

По видам деятельности картина складывается следующим образом. Более одной трети ОПГ, действующих в ЕС, участвуют в производстве, распространении и логистике наркотиков. Более 25% международных ОПГ вовлечены в различного рода контрабанду, в том числе 10% — в контрабанду мигрантов; 15% ОПГ занимаются корыстными финансовыми преступлениями и мошенничествами. В их составе не менее 10% составляет киберкриминал.

В настоящее время 45% ОПГ участвуют более чем в одном виде преступной деятельности. Диверсификация криминала резко возросла по сравнению с 2013 г. Наиболее диверсифицированными крими-

нальными структурами являются ОПГ, задействованные в преступлениях, связанных с контрафактом, а также киберпреступные группы.

Многие ОПГ отличаются высокой мобильностью и пластичностью. Они способны перейти от одной преступной деятельности к другой или быстро расширить свою специализацию. Во многих случаях ОПГ работают по бизнес-модели «по требованию» и становятся активными только после появления новых возможностей получения прибыли или заказа со стороны.

По состоянию на 2016 г. сохранялся явственный барьер между киберкриминалом и традиционными ОПГ. Барьер связан с различным образовательным, культурным и профессиональным уровнем участников этих ОПГ и часто с различиями в этническом и территориальном составе. Однако эксперты Европола полагают, что уже в ближайшие годы киберкриминал и небольшие высокотехнологичные преступные группы, имеющие гораздо более высокие показатели эффективности преступной деятельности и несущие меньшие риски быть пойманными, нежели традиционная преступность, начнут подминать под себя не только традиционные ОПГ, но и уличную преступность.

В течение нескольких последних лет *концепция преступления «по требованию»* стала характерной чертой различных криминальных рынков. При этом все чаще ОПГ рекламируют специальные возможности для преступников-индивидуалов. Им предлагается техническая, юридическая и иная поддержка в обмен на долю от конкретных криминальных проектов.

В своей деятельности ОПГ во всевозрастающей степени используют коррупцию для проникновения в государственные, частные и общественные организации. Основными видами коррупции являются взяточничество, услуги нематериального характера, а также представление собственности и бенефиций через третьих лиц. Максимальный уровень коррупции связан с киберпреступностью в финансовой и торговой сферах. Практически совершение любого крупного киберпреступления в онлайн-банкинге или онлайн-торговле поддерживается преступными инсайдерами изнутри компании.

§ 2. ОПГ, контрмеры и цифровые средства общения

За последние годы существенно возросло внимание ОПГ к проведению контрмер. Контрмеры — это действия отдельных преступников и ОПГ по пресечению или предотвращению деятельности правоохранительных органов против них. Данную деятельность ОПГ осуществляют как самостоятельно, в основном через коррупционные методы и проникновение внутрь рядов правоохранителей, так и пользуясь услугами кибергруппировок. На территориях стран ЕС действуют несколько кибергруппировок, которые специализируются на распознавании работников правоохранительных органов, включая агентов под прикрытием, по общедоступному фотоконтенту в социальных сетях, а также анализу потокового видео. Кроме того, подобные криминальные формирования предоставляют ОПГ данные о составе семей полицейских, их местоположении, школах, где учатся дети работников правоохранительных органов, и т. п.

В контексте контрмер ОПГ активно применяют информационные технологии. Большинство ОПГ на территории ЕС используют шифрованную почту, в основном со швейцарской юрисдикцией, шифрованные мессенджеры, иностранные и предоплаченные сим-карты. Большой популярностью среди преступников пользуются спутниковые телефоны.

Согласно исследованию «Flashpoint», проведенному в начале 2017 г., Skype является наиболее предпочтительным вариантом общения среди киберпреступников по всему миру. В этом плане продукт Microsoft обгоняет WhatsApp, Telegram и ICQ.

Исследовательская компания использовала «упоминания социальных платформ в подпольных сообществах», чтобы проанализировать текущее состояние дел в онлайн-коммуникации, связанной с преступностью. В список сообществ вошли многочисленные форумы, связанные с мошеннической деятельностью в Интернете.

В целом Skype возглавил список, но мошенники прибегают к использованию различных мессенджеров в зависимости от местоположения и языка, на котором они говорят. Киберпреступники при выборе платформы для общения учитывают такие факторы, как простота использования, безопасность и анонимность.

Skype доминирует среди русско- и англоговорящих интернет-мошенников — приложение Microsoft упомянули 38 и 64% из них соответственно. Согласно исследованию в 2012 г. испанские и арабские киберпреступники также чаще полагались на Skype, но большинство из них к 2016 г. перешли, соответственно, на WhatsApp и ICQ.

Примечательно, что ICQ попал в пятерку самых популярных мессенджеров среди мошенников, которые говорят на русском, испанском, французском, арабском и английском языках.

Еще одним популярным средством общения киберпреступников является программа Jabber. С ее помощью хакеры совершают сделки, делятся данными и предлагают техническую поддержку для своих шпионских программ. Завоевав уважение российских хакеров, Jabber одновременно набирает популярность среди киберпреступников всего мира.

Jabber (известен также как XMPP или Extensible Messaging and Presence Protocol) — это открытый интегрируемый интернет-мессенджер с тысячами независимых серверов и приблизительно 10 млн пользователей по всеми миру. На основе этой технологии созданы такие известные продукты, как частная коммуникационная платформа HipChat и приложения для общения в видеоиграх Electronic Arts Origin и приставки Sony Play Station. Приложение WhatsApp, у которого более 1 млрд пользователей, также работает на варианте XMPP.

Все, из-за чего многим компаниям удобно использовать Jabber, делает его идеальным вариантом для преступников. Технология поддерживает надежное шифрование и несколько видов защиты, которые вкупе с открытостью резко увеличили популярность программы в «постсноуденовскую» эпоху.

Jabber был создан в 1999 г. и через 10 лет набрал миллионы пользователей. Начиная с 2013 г. популярность мессенджера пошла вверх, так как в Сети участились взломы и активизировалась разведка. В России пользователи прекратили общение через мессенджер ICQ 1996 г., который оставался самым популярным средством связи на протяжении практически двух десятилетий, в пользу предложенной Jabber безопасности. В России обычно загружают и безопасно используют мессенджер с OTR-протоколом.

Хакеры интегрируют Jabber в Skype.

По правилам сообщества Jabber любой пользователь может открыть сервер и делать все, что захочет. Это очень привлекательно для преступников, которые обеспокоены тесным сотрудничеством компаний и правительства, особенно в США. И некоторые серверы Jabber созданы специально для преступников.

Во избежание физического надзора ОПГ все чаще отказываются от наличия собственного транспортного парка и используют наемные авто- и авиатранспорт. Также ОПГ проявляют особый интерес к внедрению своих кротов в службы видеоконтроля крупных европейских городов, а также торговых центров и т. п.

При тесном взаимодействии и переплетении традиционных и вновь образованных высокотехнологичных ОПГ они существенно различаются по методам и организации преступной деятельности. Современные ОПГ в основном отказываются от традиционных иерархических структур времен дона Карлеоне и Тони Сопрано, а представляют собой подвижные сетевые структуры. Они активно используют аутсорсинг, коллективное предпринимательство, платформенные решения и т. п. Одним словом, если преступники до середины XX в. плелись в хвосте технических, организационных и финансовых технологий, то сегодня они, несомненно, находятся в авангарде.

Киберпреступность, безусловно, требует более высокого технического уровня, сметливости и дисциплины, чем традиционный промысел «ножа и отмычки», но обладает и множеством преимуществ, решающими из которых являются два: во-первых, добыча одного среднего киберпреступника, по данным нью-йоркской киберполиции, в семь раз превышает добычу уличного преступника; во-вторых, в Нью-Йорке, например, раскрываемость обычных преступлений составляет в разные годы от 40 до 60%, а киберпреступлений — 4%. Иными словами, киберпреступность — это высокодоходная и малорискованная криминальная деятельность. Не случайно согласно опросу в Бухарестской математической школе (2016) более 70% десятиклассников сказали, что с удовольствием стали бы хакерами в криминальных группировках.

Если первый тренд связан с появлением новых групп, то второй тренд — это взрыв уровня организованности киберпреступников. По данным ФБР, в настоящее время не менее 40% киберпреступников старше 35 лет. Миф о том, что хакеры — это подростки, — не более чем недоразумение.

Новые национальные киберпреступные синдикаты — это *программно-финансово-организационные структуры* нового поколения. Эти структуры имеют возможность отбирать лучших студентов в лучших учебных заведениях, создавать собственные мощные центры исследований и разработок, нанимать лучших адвокатов. Еще пять — семь лет назад 80% хакеров были одиночками, своего рода неорганизованными фрилансерами.

В настоящее время согласно исследованию RAND Corporation 80% хакеров входят в состав регулярных (постоянных) ОПГ. В том, что преступники используют технологии, нет ничего нового. Однако есть некая принципиальная разница между вчерашним днем и днем сегодняшним. Раньше преступники использовали военные или гражданские технологии, приспосабливая их для своих нужд. Нынешние преступные группы сами разрабатывают технологии, используют их как отдельный побочный бизнес и реализуют через свои легальные предприятия в гражданской и военной сферах.

Кроме того, особенностью современной организованной преступности является упор на исследования и разработки. Если раньше она использовала технологии либо те или иные устройства по прямому назначению, то теперь старается выжать из технологий все возможное.

Например, принятое сегодня повсеместное использование мобильных телефонов для сбора больших данных впервые было осуществлено мексиканскими преступными синдикатами. В международном аэропорту Мехико существует обширная вип-зона, где прилетающие

высокопоставленные гости коротают время, пока разгружается багаж. Одновременно, будучи занятыми людьми, которым необходимо все время находиться на связи со своими офисами, они сразу же переключают роуминг. Мексиканские преступники вмонтировали в стойку бара вип-зала международного аэропорта сложную аппаратуру, которая перехватывала сигналы роуминга и сигнализировала о прибытии того или иного гостя. Соответственно, преступники, наблюдая, с одной стороны, за гостем, с другой стороны, контролируя разгрузку багажа, имели 15—20 минут на то, чтобы в зоне разгрузки багажа не украсть багаж, как делают в Европе и Америке, а открыть его, взять дорогую вещь и вернуть багаж на место. В итоге, когда спустя некоторое время жертва ограбления обнаруживала пропажу, она подозревала кого угодно, но не этих преступников. Промысел процветал полтора года и принес несколько десятков миллионов долларов. Он закончился не из-за провала в аэропорту, а из-за неосторожной попытки сбыть на нью-йоркском аукционе уникальную золотую статуэтку.

Современные преступники быстро адаптируются к техническим новациям и сами создают и продвигают технологии. Варианты адаптации могут быть различные. Например, известна преступная группа, которая, внимательно проанализировав известный сервис Uber, создала аналог для преступников. Суть сервиса состоит в том, что любой преступник может разместить в приложении место, где он располагается, размер вознаграждения и точку, которую ему надо достичь на ирландской границе. Приложение пользуется большой популярностью в преступном мире, а полиции пока не удалось отследить разработчиков приложения. Еще более удивительным является факт, что приложение отличает полицейского под прикрытием от обычного водителя. По крайней мере за полтора года действия приложения полиции ни разу не удалось направить своего водителя, который подвез бы преступника. На предложения лжеводителей, размещенных в приложении, ни один преступник не откликнулся. Это заставило британских журналистов думать, что создателями приложения являются британские полицейские, связанные с ОПГ.

§ 3. Структурные изменения ОПГ в эпоху технологических трансформаций

Начиная с 2000 г. организационные формы серьезной криминальной деятельности претерпели значительные изменения. Сегодня они являются наиболее разнообразными и пластичными за весь период существования европейского организованного криминала.

До начала XXI в. существовало два основных типа структур организованной преступности.

Первый тип — это *жестко структурированные иерархические ОПГ*. Для этих групп характерен постоянный состав руководителей и значимых членов при достаточно высокой текучести рядовых участников групп. Как правило, в таких ОПГ вопросы решаются коллегиально, а преступный лидер выполняет не столько функции безусловного руководителя, сколько арбитра и последней инстанции при отсутствии единодушия среди руководящего состава группировки. Подобные ОПГ формировались по принципам местничества (происхождения из одной местности, города, района, пребывания в одной тюрьме и т. п.) или этнического состава (для национальных меньшинств). Если ранее такие группировки, как правило, занимались одним-двумя видами преступной деятельности, то чем дальше, тем больше они диверсифицируют свою деятельность.

Наибольшие успехи в борьбе с организованной преступностью начала XXI в. как на уровне отдельных государств ЕС, так и сообщества в целом связаны с операциями правоохранительных органов именно против этого типа ОПГ. Они наиболее распознаваемы и уязвимы. Как правило, участники этих ОПГ ни раньше, ни теперь не вовлечены в легальную экономическую деятельность и являются либо безработными, либо лицами без определенных занятий, либо скрываются от правоохранительных органов. С появлением информационного общества с новыми средствами наблюдения и контроля распознавать тип активности населения стало гораздо проще, чем ранее.

Об эффективности противодействия традиционным формам организованной преступности свидетельствуют следующие цифры. Если в 2002 г. на этот вид ОПГ приходилось 25—27% лиц, вовлеченных в серьезную организованную преступность в странах, входивших тогда в ЕС, и на их долю приходилось соответственно 62—65% криминальных доходов, то в 2015—2016 гг., согласно данным правоохранительных органов государств ЕС и исследованиям по заказу Интерпола, доля лиц, вовлеченных в подобные ОПГ, сократилась до 10% от общего количества серьезных организованных преступников, а доходы теперь составляют всего 15% от общей добычи криминала на территории ЕС.

Основным видом организационных структур преступности в странах ЕС в конце XX и в начале XXI в. были *ОПГ временного характера и состава*. Эти группы, в отличие от традиционной иерархической организованной преступности, создавались и создаются для проведения конкретных преступных операций либо реализации определенных, относительно кратковременных — от трех месяцев до полутора-двух лет — криминальных проектов.

Подобные группы, по образному выражению М. Поттера, аналитика ФБР, являются *реализацией продюсерской экономики в преступ-*

ном мире. Как правило, такие группы формируются вокруг преступного лидера, имеющего высокий авторитет в криминальных кругах, проектировщика или разработчика криминальной операции (проекта) и небольшого числа высококвалифицированных опытных преступников различной функциональной специализации.

Постепенно ядро обрастает либо исполнителями подсобных работ, либо принимающими на себя основные риски возможных боевых столкновений с правоохранителями. Временные ОПГ формируются не по местническому или этническому признаку. Их состав в решающей степени зависит от личных знакомств лидера и членов функционального ядра ОПГ.

В начале XXI в. в подобного рода ОПГ состояли 70—73% организованных преступников. Их добыча составляла примерно 23—25% общего убытка европейской экономики и домохозяйств от организованной преступности. В 2015—2016 гг. доля в общей численности снизилась до 25%, а в совокупной криминальной добыче — до 10%.

На рубеже XX—XXI вв. с приходом в Интернет не только университетов и продвинутых пользователей, но и бизнеса, и среднего класса появились первые киберпреступные ОПГ. В основе их организации лежал и лежит сетевой принцип. В отличие от традиционной организованной преступности участников ОПГ не обязательно связывают длительные личные отношения и даже просто очные знакомства. Во многих кибергруппировках такого рода личные пересечения не поощряются. При этом практически обязательным условием вхождения в состав подобных ОПГ является длительный бэкграунд в различных подпольных форумах, чатах. Кроме того, широко распространен *институт рекомендателей*. Для вхождения в состав сетевой ОПГ требуется, чтобы кто-то, лично знающий руководителей ОПГ, порекомендовал потенциального кандидата, с которым встречался на различных хакерских конференциях, неформальных встречах и т. п.

В начале XXI в. численность таких ОПГ не превышала 1% общей численности организованных преступников, а доходы составляли примерно 3% криминальной добычи. К началу 2017 г. доля численности сетевых киберпреступных группировок возросла до 5%, а добыча — до 20%.

В 2013—2016 гг. наиболее преуспевающие традиционные ОПГ изменили свою организационную структуру с иерархической на *блочно-сетевую*. Наибольший толчок структурным изменениям дал мигрантский кризис 2014—2016 гг., а также повышение эффективности деятельности правоохранительных органов.

Принципиальное отличие блочно-сетевой структуры организованной преступности от традиционных ОПГ состоит в том, что в стабильном, устойчивом ядре аккумулируются руководство, наиболее

опытные искусные преступники, а также люди, выполняющие сервисные функции, связанные с отмыванием денег, защитой в судах, коррупционными связями с государственными структурами и т. п. Все остальные, в том числе профильные, функции подобных ОПГ выполняют специализированные по территориальному или функциональному признакам *контрактные ОПГ*, работающие по модели *«преступление как сервис»*. Переход от иерархической к блочно-сетевой структуре усложнил работу правоохранительных органов по выявлению и пресечению деятельности руководителей преступных образований. При блочно-сетевой модели основной удар принимают на себя преступники-контрактники. При пресечении деятельности ОПГ, работающих на подряде, или при малейшем подозрении на раскрытие их деятельности правоохранительными органами блочное ядро прекращает любые контакты и заключает новый контракт с другой группой.

Наибольшие опасения у Европола вызывает появление на территории ЕС так называемых *мебиус-преступных групп*. Отличительными особенностями этих групп являются небольшая численность, легальный характер занятий участников групп, высокий уровень их профессиональной, в том числе высокотехнологической, расследовательской и военной компетенций.

Такого рода группы выполняют заказы крупных бизнес-структур, а иногда государственных органов нескорых стран за пределами ЕС. Также они подряжаются для выполнения контрактов с террористическими группами и сетями. Наконец, по данным исследовательского центра Европола, такого рода группы самостоятельно разрабатывают, готовят и осуществляют технически и организационно сложные преступления.

Развитие информационных и иных высоких технологий постоянно увеличивает деструктивный и летальный потенциал небольших групп. В 2013—2017 гг. у небольших групп впервые появились возможности наносить ущерб не на уровне отдельного бизнеса или локальной общины, а в масштабах мегаполисов и крупнейших корпораций.

На состоявшейся в январе 2017 г. конференции по криптовалютам в Катаре впервые был поставлен вопрос о малых высокотехнологичных группах, которых в США называют «организациями-оборотнями», а французские правоохранители — «мебиус-преступниками». Некоторые ошибочно полагают, что такого рода группы по роду своих занятий относятся исключительно к киберкриминалу.

Однако это не соответствует эмпирическим данным, накопленным Европолом при участии правоохранителей Германии, Франции, Нидерландов и Италии. Наряду с киберпреступностью такие группы

разрабатывают и проводят преступные операции по корпоративному и личному шантажу, краже людей, в том числе детей, хищению уникальных произведений искусства и особенно масштабные финансовые преступления, требующие сочетания внешних кибератак с внутренним саботажем, и т. п.

§ 4. Движущие силы современных ОПГ в цифровом мире и технологические новации как ускорители деятельности ОПГ

Важнейшим направлением развития деятельности ОПГ являются их усилия по *повышению результативности отмывания преступных доходов, их трансферту в законную экономику*. Криминальные сети и группы постоянно стремятся использовать новейшие технические разработки, такие как криптовалюты и анонимные способы оплаты. Быстрая обработка транзакций и распространение эффективных инструментов анонимизации затрудняют деятельность правоохранительных органов по доказательной идентификации реальных бенефициаров доходов от преступной деятельности.

Все возрастающее количество онлайн-платформ и приложений предлагают новые способы перевода денег. Они не регулируются в той же степени, что и традиционные поставщики финансовых услуг, что облегчает жизнь преступников. Кроме того, по данным Европола, есть вероятность, что некоторые широко распространенные платежные системы на основе блокчейна через компании-«прокладки» могут контролироваться международным криминалом.

Онлайн-банкинг также облегчает жизнь преступникам. По данным Европола, на «черном» рынке, ориентированном на ОПГ, активно продаются специальные программы, позволяющие обойти ныне все более широко применяемую биометрическую идентификацию собственников счетов физических и юридических лиц.

Важнейшими факторами перемен в направлениях деятельности, структуры и методов организованной преступности в Европе являются *технологические инновации*. Европейские преступники демонстрируют высокую степень приспособленности и креативности в использовании новых технологий. Интернет и возрастающие возможности его подключения ко всем компонентам физической среды оказывают все большее влияние на виды серьезной организованной преступности. Инновации в инструментарии и методах, коммуникациях и логистике криминала все в большей степени позволяют ОПГ совершать преступления анонимно, в любом месте, в любое время, без физического присутствия.

«Интернет вещей» постоянно расширяется. Возможность подключения всех типов устройств становится реальностью для домашних

хозяйств и предприятий в странах ЕС. В отличие от традиционных компьютеров и планшетов смартфоны и подключенные к Интернету вещи остаются крайне уязвимыми для вторжения. В городах-миллионниках в странах ЕС до 90% общедоступных узлов Wi-Fi не защищены шифрованием. Соответственно, киберпреступники могут подключиться к любому из миллионов абонентов, ежедневно использующих эти узлы. По мнению Европола, крупнейшую угрозу в области организованной преступности в ближайшие три — пять лет будут представлять отнюдь не искусственный интеллект или большие данные, а превращение крайне уязвимых к внешнему злонамеренному вторжению смартфонов в домашние бухгалтерии, кошельки и точки доступа к многочисленным сервисам и программам, требующим персональных данных.

Другим ключевым фактором, определяющим изменения криминального ландшафта ЕС, является *динамика геополитической ситуации* в Европе и вокруг нее. ОПГ уже извлекли сотни миллионов долларов преступных доходов от конфликтов на периферии ЕС, прежде всего в Ливии, Сирии, Ираке, Афганистане, Йемене. Вооруженные конфликты и бедность в этих регионах обусловливают долгосрочный характер нарастания миграционных потоков.

Еще одним направлением развития ОПГ является *установление все более тесных связей между преступностью и корпоративным сектором* в некоторых странах ЕС. Данное взаимодействие строится по трем направлениям.

Во-первых, бизнес-структуры, иногда даже крупнейшие корпорации, не гнушаются заказывать у преступников определенные мероприятия. В наибольшей степени это имеет отношение к киберпреступности и связано с кражей интеллектуальной собственности и компрометирующей конкурентов документации.

Во-вторых, ОПГ стараются в гораздо бóльших размерах, чем ранее, инвестировать преступные прибыли не в криминальный, а в легальный бизнес. Особым интересом у ОПГ пользуются такие отрасли, как строительство, уборка городского мусора и экология в целом. Также криминал инвестирует в IT-индустрию, особенно в финансовые технологии, изготовление видеоигр и различного рода приложений, предусматривающих получение от клиентов персональных данных.

Наконец, в-третьих, это шантаж со стороны ОПГ среднего, крупного и особенно крупнейшего бизнеса. Шантаж основан на практике уклонения европейского бизнеса от налогообложения с отправлением денег в офшорные юрисдикции. По данным Европола, некоторая часть адвокатских, консультативных и регистрационных бюро, связанных с налоговым планированием и трансфертом средств в офшор-

ные зоны, которыми пользуется легальный бизнес, находится под контролем международных ОПГ.

Новой чертой последних лет стало пристальное *внимание ОПГ к крупнейшим европейским транспортным хабам*, используемым для глобального распределения товарных потоков.

В настоящее время наибольшие темпы динамики преступности приходятся на локации, характеризующиеся несколькими факторами, включая наличие эффективной транспортной инфраструктуры, близость или связь со странами — источниками товаров, услуг или мигрантов, доступ к деловым или инвестиционным возможностям, а также спрос на незаконные товары и услуги.

Раздел IV
ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В ЦИФРОВОМ МИРЕ

Глава 8. Предупреждение киберпреступлений

§ 1. Доктринальные и стратегические требования по защите граждан, общества и государства от киберпреступлений в Российской Федерации

На наш взгляд, в широком смысле слова криминологическая защита от киберпреступлений во многом идентична обеспечению информационной безопасности в сфере государственной, общественной и экономической безопасности.

Доктрина информационной безопасности определяет ее как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие, оборона и безопасность государства.

Обеспечение информационной безопасности — осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных

систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые участвуют в решении задач по обеспечению информационной безопасности.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

— противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности России;

— пресечение деятельности, наносящей ущерб национальной безопасности РФ, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

— повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

— повышение безопасности функционирования объектов информационной инфраструктуры, в том числе обеспечение устойчивого взаимодействия государственных органов, недопущение иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи РФ, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории РФ;

— повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

— обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

— совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности.

Для криминологической защиты от киберпреступлений большое значение имеет использование положений международно-правовых и национальных правовых актов в этой сфере.

Например, весьма интересен терминологический аппарат, используемый в Великобритании при разработке новой Стратегии цифровой безопасности (2017).

Под *цифровой безопасностью* там понимают безопасность использования ИКТ во всех аспектах человеческой деятельности на уровне государств, международного сообщества, организованностей негосударственного характера, социальных сообществ, групп и отдельных людей. Цифровая безопасность — это безопасность использования ИКТ в обществе, включая все его аспекты, и прежде всего в сфере политики, экономики и культуры в ее широком понимании, вплоть до повседневной жизнедеятельности граждан.

Цифровая безопасность включает три главных аспекта: информационную безопасность, кибербезопасность и поведенческую безопасность.

Информационная безопасность — это безопасность программно-аппаратных комплексов и сетей, а также размещенных в сетях виртуальных платформ поиска, распознавания, передачи, обработки и хранения сигналов и данных. Информационная безопасность предполагает исключение помех, нарушений или разрушения программно-аппаратных средств, сетей и виртуальных платформ в результате использования различного рода вредоносного и разрушительного программного кода, а также кражу или нарушение целостности баз данных, сведений и знаний.

Кибербезопасность в рамках разработки Стратегии цифровой безопасности отличается от понимания кибербезопасности в рамках разработки указанной Стратегии.

В рамках цифровой безопасности *кибербезопасность* — это поддержание целостности и обеспечение бесперебойного функционирования телекоммуникационных сетей и программно-аппаратных средств или модулей управления физическими объектами любого типа, включая машины, механизмы, оборудование, инфраструктурные сети, робототехнику, системы вооружения, а также человека как биологическое существо. Кибербезопасность в буквальном ее понимании означает безопасность управления. В цифровом мире управление осуществляется при помощи телекоммуникационных сетей и программно-аппаратных комплексов.

Поведенческая безопасность — это безопасность использования ИКТ для укрепления присущих конкретному обществу ценностей, стандартов поведения, повышения качества жизни, развития способностей и творческого потенциала граждан во всем разнообразии их групповых и индивидуальных особенностей. Одновременно поведенческая безопасность предполагает недопущение использования ИКТ для внешнего управления поведением групп любого размера и отдельных граждан.

Наиболее известными типами поведенческих технологий, использующихся в настоящее время как в позитивных, так и в деструктивных целях, являются надж, психопрограммирование, социальное программирование, вычислительная пропаганда, нейромаркетинг и т. п. При этом указанные технологии не исчерпывают всего разнообразия поведенческих технологий. Например, высокоуровневой киберагрессии практически всегда сопутствует использование социального инжиниринга. Социальный инжиниринг является деструктивной поведенческой технологией.

§ 2. Предупреждение виктимизации, связанной с киберпреступностью

Для практики обеспечения кибербезопасности в целях предупреждения виктимизации, связанной с киберпреступностью, большое значение имеют Руководящие принципы ОЭСР в отношении безопасности информационных систем и сетей (2002). Руководящие принципы ОЭСР нашли отражение в Резолюции Генеральной Ассамблеи ООН, посвященной созданию глобальной культуры кибербезопасности (от 31 января 2001 г.), а также в региональных документах. Руководящие принципы ОЭСР строятся на трех категориях принципов кибербезопасности: 1) базовые принципы; 2) социальные принципы; 3) принципы жизненного цикла безопасности. Эти принципы служат организационной основой для классификации подходов к предупреждению киберпреступности, которые применяются организациями частного сектора.

Базовые принципы кибербезопасности включают осознание значимости организационных рисков, отчетность за действия с учетом такого осознания, а также процессы координации и изучения для реагирования на инциденты.

Практически все обследования организаций частного сектора решают проблему осознания рисков за счет обучения персонала в сочетании с политикой и контролем за доступом работников, клиентов и третьих сторон к данным и их использованием. Такие меры традиционно разрабатываются компаниями своими силами, а затраты на их внедрение варьируются в зависимости от размера организации. К ним относятся такие элементы, как распространение информации о самых последних угрозах и ограниченности технических решений.

Как правило, сотрудники специально созданных подразделений по кибербезопасности занимаются вопросами сохранения данных, являющихся доказательствами, и продвинутыми формами расследований в Интернете, а также в некоторой степени — вопросами отслеживания формирующихся угроз и тенденций в области киберпреступности, сотрудничества с правоохранительными органами и изучения способов обеспечения безопасности компьютерных систем. Подготовка таких кадров в основном осуществляется силами самих компаний, некоторую помощь в этом оказывают организации частного сектора, научные учреждения и неправительственные организации.

К двум ключевым технологическим изменениям последнего времени, которые влияют на риски в сфере информационной безопасности, относятся быстрый рост использования услуг «облачных» вычислений и использование работниками их собственных цифровых устройств (особенно смартфонов и планшетов) для доступа к корпоративным системам.

Определенная ОЭСР категория *социальных принципов* включает этические и демократические принципы поведения членов информационного общества. Сюда относятся осознание влияния нарушения безопасности на другие стороны, соответствующее законодательство и регулирование, а также соответствие поведения работников ценностям компании. Это также связано с совместимостью практик в области безопасности с социальными ценностями, такими как свобода выражения мнений, право на частную жизнь, открытость и прозрачность.

Респонденты из числа организаций частного сектора в значительной степени сосредоточили внимание на сформулированных ОЭСР *принципах жизненного цикла безопасности*, которые носят скорее оперативный характер. К этим принципам относятся оценка рисков, разработка систем смягчения последствий выявленных рисков, разработка политики, процессов и процедур управления такими системами и регулярный их пересмотр по мере развития технологий.

Большинство респондентов из числа организаций частного сектора сообщили об использовании технических решений для предупреждения киберпреступлений, например брандмауэров, сохранения цифровых доказательств и ограничения подключения к определенным IP-адресам. Многие из них также задействуют способы идентификации определенных видов контента, меры предупреждения нарушения

товарных знаков/авторских прав, расшифровку зашифрованных материалов и меры, направленные против неправомерного использования компьютеров. К основополагающим элементам таких решений относятся анализ и контроль за работой системы, выявление случаев вмешательства в систему и антивирусные программы. Респонденты сообщали о том, что большинство систем разработаны частным сектором, причем некоторые из них — силами самих компаний, а ежегодные затраты на их реализацию являются значительными, особенно в случае транснациональных компаний-респондентов.

Помимо работы с собственными проблемами в части своей кибербезопасности некоторые международные технологические компании заняли активную внешнюю позицию, расследуя и прекращая кибератаки, которые ставят под угрозу доверие клиентов к их системам. Такие инициативы в случае их реализации в полном соответствии с профильными законами могут дополнить действия правоохранительных органов, а также обеспечить положительную рекламу и хороший морально-психологический климат для персонала.

Ряд компаний, занимающихся вопросами интернет-безопасности, собирают детальные данные о распространении вредоносных программ и бот-сетей, публикуют их в регулярных отчетах и предоставляют партнерам из корпоративного сектора и правоохранительных органов. Ряд компаний публикуют ежеквартальные отчеты об угрозах, в которых содержатся данные об уровне заражения устройств (включая мобильные устройства), взломах баз данных, атаках (например, фишинге) и специфических киберпреступлениях, таких как требования выкупа и преступные программы, данные о группах и отдельных лицах, связанных с киберпреступлениями в регионе, отчеты по результатам сопоставительного анализа профилей киберпреступников. Многие телекоммуникационные компании делятся данными о структуре трафика и атаках, наблюдаемых в их сетях.

Ряд организаций частного сектора помогают компаниям составлять профили правонарушителей и причин их атак. Эта информация позволяет повысить качество технической защиты и судебных исков, использовать прием размещения ложной информации в собственных сетях компаний для обмана правонарушителей и сделать атаки более ресурсоемкими мероприятиями. Некоторые компании рассматривают возможности «обратных хакерских атак», направленных против хакеров, но пока не ясно, насколько это будет законно или технически возможно.

В целом картина предупреждения киберпреступности носит смешанный характер. Более крупные компании, особенно в секторе финансовых услуг, придерживаются более сложных стратегий предупреждения киберпреступности, в том числе используют специальные

технологии в области безопасности, такие как аппаратные ключи безопасности для авторизации пользователей. Компании, занимающиеся вопросами безопасности, осуществляют активный мониторинг и регулярно публикуют отчеты о формировании новых угроз, а ряд крупных технологических компаний активно обращается в суды с исками о ликвидации бот-сетей, преследовании спамеров и мошенников. Тем не менее более мелкие компании не столь хорошо защищены, причем некоторые из них не предпринимают даже базовые меры предосторожности или не имеют реалистичного представления о рисках, связанных с вопросами безопасности.

Предупреждение киберпреступности со стороны поставщиков услуг Интернета и хостинга. Поставщики услуг Интернета занимают уникальное положение в рамках интернет-инфраструктуры. Они приобретают в собственность или арендуют емкие оптоволоконные каналы и другие ключевые элементы интернет-инфраструктуры, такие как серверы, сетевые коммутаторы и маршрутизаторы, а также (в случае операторов мобильных сетей) радиосоты, что позволяет размещать и доставлять контент, подключать к Интернету настольные и карманные устройства. С одной стороны, очевидно, что поставщики услуг должны играть некоторую роль в предупреждении киберпреступности, но с другой — с этим связано много нюансов и сложностей, включая проблемы обязанностей и ответственности поставщиков услуг за интернет-контент.

Поставщики услуг Интернета обеспечивают подключение пользователей к Интернету и передачу данных между пользователями и устройствами, такими как глобальная сеть, электронная почта и серверы для передачи речи по IP-протоколу (VoIP). Поставщики услуг Интернета потенциально могут анализировать некоторую часть этого трафика, если пользователь не шифрует данные с использованием виртуальной частной сети, прокси-сервера или функций, встроенных в используемое для информационного обмена программное обеспечение. К данным абонента, которые могут быть доступны поставщикам услуг Интернета, относятся содержание информационного обмена, т. е. незашифрованные тексты и изображения на веб-сайтах и в электронной почте, и контекстуальные данные, например, какие серверы абонент посещает, источник и назначение сообщений электронной почты, время и продолжительность использования различных услуг абонентом, причем эта информация доступна поставщику услуг даже при условии использования шифрования. В целом содержание может быть доступно только в момент отправки данных, а затем только при условии конкретного мониторинга подключений пользователя и сохранения данных с применением специального оборудования. Примечательным исключением являются случаи, когда поставщик услуг

Интернета управляет таким сервисом, как сервер электронной почты, на котором сообщения хранятся более длительное время.

Одно лицо нередко обслуживается несколькими поставщиками услуг Интернета, поскольку доступ осуществляется из разных мест. Часто услуги Интернета для дома предоставляет один поставщик, а услуги Интернета для мобильных устройств — другой. Для доступа в Интернет на рабочем месте может использоваться третий провайдер, а при подключении к беспроводной сети в местном кафе задействуется еще один поставщик услуг Интернета, обеспечивающий такое подключение. Поэтому информацией об активности одного лица могут владеть разные поставщики услуг.

Поставщики интернет-хостинга контролируют системы, которые используются для работы веб-сайтов и других сервисов. Как и в случае отношений между поставщиками услуг Интернета и их абонентами, компании — поставщики услуг хостинга имеют уникальную возможность наблюдать весь входящий и исходящий трафик сервисов их клиентов. Поэтому у них имеются технические возможности отключить или заблокировать незаконное использование таких сервисов. В своих соглашениях об обслуживании компании, предоставляющие хостинг, как правило, устанавливают ограничения на характер сервисов, которые могут размещаться на их серверах, обычно охватывая широко известные виды ненадлежащего поведения, такие как рассылка большого количества спама или оскорбительных почтовых сообщений, размещение незаконного контента или нарушение авторских прав.

Поставщики услуг могут играть определенную роль в предупреждении киберпреступности в рамках двух основных направлений: а) хранение данных пользователей, к которым впоследствии могут получить доступ правоохранительные органы, чтобы использовать эти данные в расследовании киберпреступлений; б) активная «фильтрация» информационного обмена в Интернете или содержания данных, прежде всего в целях предупреждения киберпреступлений. Далее анализируются технические и нормативные аспекты этих направлений.

Мониторинг данных. Учитывая объем трафика, проходящего через сети поставщиков услуг Интернета, они не в состоянии вести полный учет всего трафика. Некоторые страны внедрили сложные системы наблюдения за Интернетом, однако в связи с технологическими ограничениями могут возникать сложности со сбором и анализом огромных объемов данных. Регистрация менее детальной информации (такой, как IP-адреса, присваиваемые отдельным пользователям в определенные моменты) может охватывать длительные периоды времени. Поставщики услуг Интернета, как правило, в состоянии осуществлять адресный мониторинг данных в режиме реального времени, а правила «законного перехвата» многих стран предполагают, что поставщики услуг Интернета должны иметь возможность осуществлять целевой мониторинг подключений лица или помещения в режиме реального времени.

Защита данных. Хранение и обработка данных поставщиками услуг Интернета во многих странах регулируются законодательством о защите данных, которое устанавливает требования в области защиты и использования данных личного характера. В 1990 г. Генеральная Ассамблея ООН приняла Руководящие принципы регламентации компьютеризированных карточек, содержащих данные личного характера. В них зафиксировано 10 принципов, включая принцип законности, точности и принцип цели, которые должны применяться ко всем государственным и частным компьютеризированным картотекам. Принцип безопасности гласит, что картотеки должны быть защищены от связанных с деятельностью человека рисков, таких как несанкционированный доступ, противозаконное использование данных или заражение компьютерным вирусом.

Некоторые региональные системы защиты данных, такие как нормативно-правовая база ЕС, содержат определенные правила защиты данных в секторе электронных средств связи. В рамках этой нормативно-правовой базы предусмотрено, что провайдеры общедоступных услуг электронной связи должны предпринять необходимые технические и организационные меры для обеспечения безопасности предоставляемых услуг, при необходимости совместно с провайдером — сети связи общего доступа, если это касается вопроса безопасности сети. Данные трафика, касающиеся абонентов, могут обрабатываться только для определенных целей и должны быть уничтожены или сделаны анонимными, если в них нет дальнейшей необходимости, хотя есть случаи, когда данные сохраняются (см. ниже). Государства — члены ЕС могут ограничивать некоторые из этих прав для достижения определенных целей, включая общественную безопасность, предупреждение, расследование, выявление и судебное преследование уголовных преступлений или несанкционированное использование системы электронных средств связи.

В большинстве стран имеются конституционные и законодательные положения по защите конфиденциальности данных личного характера. Среди характерных примеров целей, обозначенных в законодательстве о защите данных, можно назвать регулирование сбора, использования и раскрытия информации личного характера при одновременном признании права лица на частную жизнь и потребностей организации в информации. Что касается вклада поставщиков услуг Интернета в дело предупреждения киберпреступности, то зако-

нодательство о защите данных может играть определенную роль. Ограничения на обработку данных в целом не должны (по крайней мере при наличии достаточных исключений, зафиксированных в законодательстве) препятствовать законному доступу правоохранительных органов к клиентским данным поставщиков услуг Интернета для целей расследования. Характерный пример исключений: организация, не относящаяся к правоохранительным органам (в том числе компания), которая хранит информацию личного характера, может раскрывать эту информацию правоохранительным органам в случае, когда это обоснованно необходимо для обеспечения применения уголовного законодательства.

Сохранение данных. Учитывая требования положений законодательства о защите данных в сочетании с финансовыми последствиями хранения больших объемов данных, поставщики услуг Интернета не хранят данные неограниченно долго. В целях оказания помощи правоохранительным органам в проведении расследований некоторые страны сделали исключения к положениям законодательства о защите данных, в соответствии с которыми поставщики услуг Интернета обязаны хранить определенные виды данных об онлайновой активности абонентов на протяжении некоторого периода времени (например, одного года), в течение которого следственные органы могут получить доступ к этим данным при наличии разрешения судебных или административных органов.

Если обратиться к законодательству такого рода, то наиболее широкое применение нашла Директива ЕС о хранении данных (2006). Государства — члены ЕС должны требовать, чтобы поставщики услуг Интернета хранили генерируемые ими данные, которые необходимы для отслеживания и определения источника информационного обмена, определения назначения, вида и времени информационного обмена, а также для определения устройств связи, использованных абонентами. Эти данные должны храниться от шести месяцев до двух лет.

Уведомление о повреждении систем безопасности данных. Наконец, требования об обязательном уведомлении о повреждении систем безопасности данных также могут оказывать влияние на хранение данных абонентов поставщиками услуг Интернета. Обязательное уведомление пострадавших сторон и регулирующих органов о повреждении систем безопасности данных, особенно в случае раскрытия данных личного характера, нашло широкую поддержку в ряде стран. Уведомление призвано дать стороне, пострадавшей от такого повреждения, возможность предпринять меры по снижению последствий инцидента с точки зрения безопасности (например, посредством смены паролей или персонального кода пользователя или обращения

за перевыпуском платежных карточек), усилить конкурентное давление на компании, чтобы они совершенствовали свои системы безопасности, и поддержать усилия регулирующих органов, отвечающих за вопросы защиты данных и жизненно важной инфраструктуры.

Фильтрация интернет-контента. Помимо содействия предупреждению преступности за счет возможностей, связанных с хранением данных, поставщики услуг Интернета также могут принимать участие в деле предупреждения киберпреступности за счет активного анализа информационного обмена в Интернете и передаваемых при этом данных. В связи с этим одной из основополагающих концепций является фильтрация интернет-контента поставщиками услуг Интернета.

Фильтрация интернет-соединений имеет место на определенном уровне практически в любой сети. Базовый уровень фильтрации, используемый для повышения эффективности работы и безопасности сети, состоит в блокировании неверных или иным образом поврежденных данных. Поставщики услуг Интернета также могут иметь технические возможности для фильтрации данных на предмет определенного вредоносного или незаконного контента. Например, многие поставщики услуг Интернета могут применять базовые спам-фильтры для фильтрации сообщений в электронной почте их абонентов и обеспечивать защиту от хорошо известного вредоносного трафика, связанного с вирусами или хакерскими атаками, отказываясь передавать далее трафик, отнесенный к этой категории.

Спам и бот-сети. Фильтрация спама является серьезной проблемой всех поставщиков услуг электронной почты, учитывая большие объемы содержащих спам сообщений, которые отправляются и поступают ежедневно. Средства фильтрации спама разнообразны и сложны. К ним относятся анализ отправителя почтовых сообщений для определения известных источников спама, а также анализ текстов для выявления стандартных фраз и структуры содержания в сообщениях. Сообщения, которые классифицируются как спам, иногда полностью блокируются или доставляются в «папку спама» пользователя. Помимо фильтрации спама поставщики услуг Интернета также могут играть определенную роль в борьбе с вредоносным содержанием, например с содержанием, генерируемым бот-сетями.

Когда поставщики услуг Интернета получают уведомление или определяют, исходя из структуры интернет-трафика, что устройство в их сети, по-видимому, стало частью бот-сети или иным образом заражено вредоносными программами, один из возможных вариантов действий включает в себя блокирование части или всего трафика, идущего с этого адреса, при одновременном уведомлении абонента о шагах, которые он может предпринять для удаления вредоносных программ. Такие уведомления могут поступать от отвечающих за

безопасность компаний, которые осуществляют мониторинг в целях выявления бот-сетей с использованием таких приемов, как устройства-«ловушки», которые преднамеренно привлекают вредоносные программы. Поставщики услуг Интернета также могут предпринимать шаги по активному выявлению взломанных устройств, осуществляя мониторинг трафика на предмет известных сигнатур, однако для эффективности таких действий необходима определенная степень адресности. Анализ, проведенный Европейским агентством по сетевой и информационной безопасности, позволил сделать следующий вывод: выявление трафика, связанного с бот-сетями, в потоке безопасного стандартного трафика можно сравнить с поиском иголки в 100 млн стогов сена.

Фильтрация содержания данных. Что касается ответственности поставщиков услуг Интернета, то в законодательстве некоторых стран содержится требование, чтобы поставщики услуг Интернета блокировали доступ к незаконному контенту, такому как детская порнография. Существуют различные способы, с помощью которых поставщики услуг Интернета могут это делать, причем разные методы предполагают разные варианты компромиссного выбора с точки зрения сочетания скорости, стоимости, действенности и точности. Применение *фильтров DNS* позволяет поставщикам услуг Интернета контролировать ответы, которые DNS-серверы направляют их абонентам, и ограничивать доступ к домену, такому как Google.com, но не к конкретной странице или набору результатов поиска. Такие ограничения легко обойти, поскольку пользователи могут просто использовать альтернативные серверы DNS, которые дадут подлинные результаты. *Фильтрация по заголовкам IP* может использоваться для блокирования отдельных компьютеров в зависимости от их адресов или даже для частичного блокирования определенных сервисов, таких как Интернет или электронная почта. На одном интернет-сервере может размещаться большое количество веб-сайтов, что может повлиять на не связанные с проблемой веб-сайты, причем иногда их число может быть очень велико. *Углубленная проверка пакетов* может применяться для анализа основного содержания интернет-трафика. Это позволяет очень гибко подходить к фильтрации, но требует дорогостоящего оборудования, которое приходится устанавливать на высокоскоростных каналах ISP и которое может замедлять соединения всех абонентов.

На практике многие режимы фильтрации предполагают некое сочетание этих подходов с образованием гибридного фильтра. Более простые фильтры, например на основе DNS, часто используются для выявления трафика, который следует направить для проверки более сложными фильтрами. Такой гибридный подход обеспечивает сложную фильтрацию при значительном сокращении необходимых ресурсов.

Поставщики услуг Интернета также могут реагировать на незаконный контент с помощью замедления трафика, а не полной его блокировки. Данный подход может применяться для того, чтобы сервис стал достаточно неудобным и абоненты избегали его. К таким примерам относятся замедление зашифрованных соединений с Интернетом, чтобы вынудить абонентов пользоваться незашифрованными и, следовательно, открытыми для проверки версиями веб-сайтов, а также регулирование поставщиками услуг Интернета пропускной способности такого файлообменного трафика, как BitTorrent.

Ответственность посредников. Фильтрация интернет-контента неразрывно связана с возможностью установить ответственность поставщиков услуг за содержание данных. Поставщики услуг Интернета, как правило, несут ограниченную ответственность как каналы «просто передачи» данных. Однако, как показано ниже, особенно в условиях интернет-хостинга модификация передаваемого контента, а также фактическая или презюмируемая осведомленность о незаконной деятельности может вести к усилению ответственности в рамках некоторых правовых систем. А своевременные действия после уведомления, как правило, предполагают снижение ответственности.

Многие правовые системы включают понятие субсидиарной ответственности, когда одна сторона содействовала неправомерным действиям другой стороны и может нести ответственность за причиненный в результате ущерб. При повсеместном распространении Интернета в середине 1990-х гг. возникла озабоченность в связи с влиянием неопределенности в части ответственности поставщиков услуг Интернета и услуг хостинга контента в Сети на формирующуюся цифровую экономику. В связи с этим ряд стран приняли «горизонтальное» законодательство, ограничивающее такую ответственность в рамках различных сфер права. Соответствующие положения обычно снимают с посредников ответственность за передачу или размещение контента третьих сторон, если выполняется ряд условий, особенно удаление определенного контента при получении уведомления.

В ряде государств также принято «вертикальное» законодательство, регулирующее вопрос субсидиарной ответственности в определенных сферах, таких как защита детей, защита данных личного характера, подлог, диффамация, мошеннические платежные схемы, имена доменов и азартные игры в режиме онлайн.

В специальных режимах ответственности, связанных с доменами, больше всего внимания уделяется *авторским правам*. Как правило, требуются система уведомлений и удаления контента, политика закрытия учетных записей пользователей, неоднократно нарушающих

требования, и применение основанных на стандартах технических мер контроля доступа к произведениям. Правообладатели могут подавать иски для получения предписаний суда о блокировании доступа к материалам, нарушающим авторские права, закрытии учетной записи подписчика или других сравнительно действенных для этих целей мерах, которые наименее обременительны для поставщика услуг.

Кроме того, на международном уровне ведется широкая дискуссия по вопросу обязанностей посредников предпринимать действия против *детской порнографии*. Интерпол ведет перечень адресов веб-сайтов со всего мира, на которых содержатся материалы «жесткого характера», которые поставщики услуг Интернета в некоторых странах обязаны блокировать в соответствии с законодательством о связи.

В целом, учитывая, что поставщики услуг Интернета и хостинга обеспечивают подключение отдельных лиц и организаций к Интернету, они могут играть ключевую роль в предупреждении киберпреступности. Так, они могут вести журналы, используемые при расследовании уголовных преступлений, помогать клиентам выявлять взломанные компьютеры, блокировать некоторые виды незаконного контента, такого как спам, и оказывать общую помощь в создании безопасной среды информационного общения для своих клиентов.

§ 3. Деятельность правоохранительных органов по предупреждению киберпреступности

Как отмечено в докладе Европола «Оценка угроз организованной киберпреступности (IOCTA)» (2016), поддержание правопорядка требует активизации работы по идентификации, локализации и профилизации преступных индивидов и групп, являющихся составными элементами европейского криминального киберсообщества. Это предполагает создание постоянно пополняемых страновых и международных баз данных по киберпреступности.

Ключевое значение для успешной борьбы правоохранительных органов с киберпреступностью имеют выделение достаточных ресурсов для исследования вредоносного программного обеспечения и новых бизнес-моделей киберкриминала, а также проведение стресс-тестов и аудита безопасности государственных органов и населения.

Правоохранительные органы должны иметь инструменты, методы и опыт для борьбы с преступным злоупотреблением шифрованием и анонимностью.

Поскольку DDoS-атаки в комбинации с сетевыми стали общим бичом для многих стран, необходимы скоординированные усилия правоохранительных органов различных государств в борьбе с этим видом киберкриминала.

В рамках эффективной деятельности в DarkNet правоохранительным органам важно избежать дублирования усилий и обеспечить межстрановое взаимодействие активных операций в DarkNet, используя общие программно-аппаратные возможности и единые базы данных.

Приоритетом номер один для правоохранительных органов во всех странах должно стать обеспечение перелома в борьбе с сексуальной эксплуатацией и насилием в отношении детей. Правоохранительные органы должны получить самые широкие полномочия в борьбе с этим абсолютным злом.

Для того чтобы справиться с преступным использованием шифрования и анонимизации, правоохранительные органы должны провести *сплошную переподготовку кадров*, причем не только работников подразделений, занятых киберпреступностью, а также получить в свое распоряжение необходимые программно-аппаратные комплексы. Кроме того, правоохранители нуждаются в получении программного инструментария, позволяющего проводить цифровые расследования и использовать киберсредства для расследования не только особо сложных, но и любых преступлений в цифровом мире.

Правоохранительные органы должны продолжать развивать систему профессиональной переподготовки и вкладывать в нее средства. Наряду с офлайн- и онлайн-курсами компьютерной грамотности для рядовых работников правоохранительных органов необходимо создать распределенную сеть центров по переподготовке кадров по узкоспециальным проблемам. Примерами таких проблем являются узкоспециальные и особо сложные кибератаки, секторальная (например, финансовая) киберпреступность, использование киберпространства для извлечения доходов от проституции, продажи порнографического контента, а также услуг, связанных с педофилией. Необходимо разработать общими усилиями методические учебные материалы, учебники и курсы лекций по цифровому следствию и криминалистике для различных уровней, начиная с оперативных работников низового уровня и вплоть до руководителей правоохранительных органов.

С учетом быстроменяющегося характера киберпреступности и скорости развития технологий существует потребность в *более адаптивном и гибком подходе к исследованиям и разработкам*. В этом плане заслуживает внимания опыт ряда стран, отказавшихся от закрытых конкурсов на разработку программного обеспечения.

По мере того как преступное использование виртуальных валют продолжает набирать обороты, для исполнения законов все более важными становятся гарантии того, что работники правоохранительных органов имеют соответствующую подготовку в сфере новейших финансовых технологий.

Правоохранительные органы должны *вывести на новый уровень координацию взаимодействия с иными странами*, где скрываются и откуда действуют киберпреступники, а также странами, где осуществляется обналичивание скомпрометированных карт.

DarkNet является киберсредой, где организованная киберпреступность чувствует себя особенно вольготно[1]. DarkNet, как и его компоненты — сети Tor и иные P2P-сети, не является незаконной средой. Настало время с учетом законности, но предрасположенности среды к криминальным действиям предусмотреть для нее специальный правовой режим. Целесообразно изучить вопрос, как бороться с киберпреступностью не методами запрета, а путем расширения возможностей и полномочий правоохранительных органов.

Когда дело доходит до практических мер по снижению объема киберпреступности, инвестирование средств в профилактические мероприятия может оказаться гораздо более эффективным направлением, нежели поиск, идентификация и наказание киберпреступников — виновников в конкретных правонарушениях. В дополнение к информированности по вопросам предупреждения преступности целесообразно изучить, каким образом облегчить и упростить возможности граждан информировать правоохранительные органы об имеющихся у них сведениях о готовящихся или замышляемых преступлениях в киберсреде.

В настоящее время профилактические кампании в области киберпреступности обращены в основном к гражданам и бизнесу, т. е. потенциальным жертвам киберпреступности. Не ослабляя внимания к этой работе, необходимо резко *активизировать профилактическую работу с потенциальными киберпреступниками, прежде всего подростками и молодежью*, обладающими программными навыками, а также работниками в сфере IT. Упор в таких кампаниях должен быть сделан на разъяснении последствий противоправной деятельности для самих преступников.

Во взаимосвязанном мире национальные профилактические кампании должны быть скоординированы с международными организациями, а также общественными наднациональными движениями.

В рамках профилактической деятельности необходимо *особое внимание уделить мобильным гаджетам* как источникам наибольшей опасности для своих обладателей и проникновения преступников в частные и корпоративные сети.

Правоохранительные органы наряду с некоммерческими организациями и частным сектором должны принимать активное участие в информационно-просветительских кампаниях среди населения. Участие в этих кампаниях должно носить не разовый характер, а предусматриваться как статья финансовых расходов и временны́х затрат правоохранителей.

[1] См.: *Бартлетт Дж.* Подпольный интернет. Темная сторона мировой паутины. М., 2017.

Задачей номер один в области профилактики должно стать повышение информированности родителей, опекунов и воспитателей относительно деятельности киберпреступников в сфере педофилии и жестокого обращения с детьми.

Правоохранительные органы должны *поддерживать атмосферу сотрудничества и рабочие отношения с научными кругами и частным сектором*. Можно рекомендовать странам в условиях сокращения государственных расходов, свойственного большинству стран, обеспечить увеличение расходов на федеральном и муниципальном уровнях на правоохранительные НИОКР и поисковые исследования, связанные с разработкой «софта». При этом нельзя допускать формирования круга одних и тех же разработчиков различных видов «софта».

Дополнительные усилия требуются для улучшения взаимодействия правоохранительных органов и финансовых институтов для пресечения тенденций наращивания финансовой киберпреступности. Наиболее эффективной и опробованной формой такого взаимодействия являются государственно-частные партнерства, соединяющие правовые и информационные возможности правоохранительных органов с ресурсами, инновациями и кадрами частного бизнеса.

Особым сектором партнерства является борьба с высокотехнологичными трансграничными киберпреступными группировками. Успех этой работы может быть обеспечен только на основе двух- и многостороннего межстранового сотрудничества.

По мере того как преступное использование виртуальных валют продолжает набирать обороты, для правоохранительных органов становятся все более важными горизонтальная и вертикальная интеграция и взаимодействие в проведении профилактических и расследовательских операций в этой сфере, включая пресечение обмена виртуальных валют на законодательно признанные.

Всеобъемлющей целью правоохранительных органов является борьба против поставщиков ключевых криминальных услуг и инструментов, которые поддерживают другие виды кибер- и привычной преступности. Ключевые услуги и инструменты являются своего рода ядром программных, аппаратных и кадровых структур европейской киберпреступности. Разрушение этого ядра окажет значительное влияние на снижение киберпреступности. К числу такого рода специализированных инструментов относятся:

— вредоносные программы, включая программы-вымогатели паролей, программы-шпионы и банковские трояны, а также, соответственно, их разработчики, поставщики и покупатели;

— провайдеры, организаторы и исполнители DDoS-атак как услуг;

— программы преодоления антивирусных решений, включая продвинутые решения для личной и корпоративной безопасности, а также их разработчики, продавцы и покупатели;

— производители ботнетов, особенно тех их модификаций, которые используются для распространения других вредоносных программ;

— осуществление DDoS-атак, а также злонамеренных манипуляций путем искажения поисковой выдачи и «зашумления» информационного пространства.

Приоритетные направления, на которых целесообразно сосредоточить профилактические усилия правоохранительных органов:

1) платежные мошенничества:

— вредоносные программы, нарушающие целостность ATM POS-систем, разработчики, поставщики «софта», затрудняющего работу банковских терминалов;

— «софт», применяемый для получения наличных средств или конфиденциальных данных при пользовании кредитными картами, бесконтактными картами и банковскими терминалами;

— «софт», используемый для кражи данных граждан, находящихся в распоряжении финансовых институтов;

— «софт», используемый для кражи средств и мошенничества в сфере электронной коммерции и прежде всего на транспорте, в розничных сетях и туристическом бизнесе;

— «софт», связанный с компрометацией всех видов финансовых данных;

— «софт», преодолевающий криптозащиту транзакций и обеспечивающий незаконное списание со счетов банков и иных платежных систем;

2) сексуальная эксплуатация детей онлайн:

— борьба с каналами потокового видео, связанного с сексуальным насилием в отношении детей;

— искоренение групп, специализирующихся на изготовлении преступного контента, связанного с педофилией и его распространением в сетях DarkNet;

— выявление с помощью цифровых средств конкретных жертв сексуального насилия и эксплуатации и проведение операций по их спасению;

— резкое усиление борьбы со всеми видами присутствия завуалированной рекламы и тем более контента, связанного с педофилией, на законных онлайн-платформах;

3) сквозная преступность:

— вендоры, покупатели и администраторы нелегальных торговых сайтов в DarkNet;

— криминальные провайдеры услуг по незаконной анонимизации и неопознаваемому хостингу;

— «денежные мулы» и «денежные прачечные» не только на территории стран ЕС, но и обслуживающие граждан ЕС;

— эксперты, разработчики и программисты, способствующие использованию биткойна и других виртуальных валют для криминальных обменных операций, отмывания денег и платежных операций, сопряженных с любыми видами преступности.

Подавляющая часть криминальных инструментов и услуг может быть использована в самых различных сферах преступной деятельности. Соответственно, приоритетное разрушение преступных сетей, занимающихся изготовлением программных инструментов и предоставляющих услуги по использованию этих инструментов в интересах иных криминальных групп, позволит разрушить ядро киберпреступности. В связи с этим именно данная деятельность является приоритетом при разработке, реализации планов и проведении оперативных мероприятий.

Оперативные цели, предложенные выше, должны рассматриваться в контексте конкретной информации, полученной в результате работы разведывательных подразделений и аналитических структур правоохранительных органов. Они должны быть встроены в долгосрочные стратегии деятельности и обеспечены инфраструктурной, кадровой и финансовой поддержкой.

§ 4. Предупреждение киберпреступлений в финансовом секторе

Основополагающим документом здесь являются рекомендации G7 «Фундаментальные элементы кибербезопасности для финансового сектора» (от 11 октября 2016 г.).

В указанных рекомендациях обращено внимание на следующие элементы.

1. *Стратегия кибербезопасности и программные средства.* Национальные и корпоративные стратегии безопасности, предусматривающие снижение рисков и опережающее отражение угроз в киберсреде, должны базироваться на международных, национальных и отраслевых стандартах, а также соответствующих руководящих принципах.

Стратегия кибербезопасности и программная среда ее разработки и реализации должны основываться на комплексной и всеобъемлющей идентификации рисков и угроз в киберсреде. Целью стратегии кибербезопасности является снижение рисков и элиминация на

этой основе угроз в киберсреде финансовой инфраструктуры. Субъекты в финансовом секторе должны разрабатывать стратегию кибербезопасности и осуществлять выбор программных средств с учетом характера, масштабов и сложности рисков и угроз в киберсреде. В рамках национальной политики финансовой кибербезопасности целесообразно особое внимание уделить разработке стандартов, процедур и функционального разделения деятельности и взаимодействия между частными институтами и государственными органами в финансовой сфере.

2. *Государственное и корпоративное управление.* Первостепенным условием для обеспечения эффективного управления в сфере кибербезопасности являются разработка, принятие и доведение до персонала стандартов и нормативов. Они призваны определять функции, права, обязанности и ответственность органов и институтов, а также их персонала, вплоть до конкретного работника. Как показывает международный опыт, наиболее эффективно кибербезопасность в финансовом секторе обеспечивается там, где эта работа интегрирована в системы отчетности, организационного планирования и управления, а также материального и социального поощрения. Также первостепенное значение для разработки стратегии и осуществления практической работы в сфере финансовой кибербезопасности имеет возложение персональной ответственности за эту работу (с наделением соответствующими правами и обязанностями) на влиятельных членов советов директоров и топ-менеджеров первого ряда финансовых институтов, а также старших должностных лиц в органах государственной власти.

Эффективная структура управления кибербезопасностью может действовать только в условиях строгой подотчетности и наличия доведенных до уровня стратегических карт и KPI-обязанностей (Key Performance Indicator), перечня главных работ и программ поощрений и взысканий. Эффективное управление в сфере кибербезопасности должно не только обеспечивать установление кооперационных связей между IT, аналитическими и собственно финансовыми подразделениями частных институтов и государственных органов, но и быть способным согласовывать конкурирующие цели. Конкурирующие цели в сфере финансовой кибербезопасности обусловлены сложным, нестабильным и динамичным состоянием киберсреды, а также множественностью рисков и разнообразием угроз. В соответствии с миссиями и стратегиями советы директоров финансовых институтов, а также высшие органы управления государственными учреждениями должны организовать работу по проведению стресс-тестов в сфере кибербезопасности для своих институтов и учреждений. Результаты

тестирования должны стать основой для разработки и внедрения эффективных программ финансовой кибербезопасности.

3. *Оценка рисков и контроль.* Стратегия кибербезопасности может быть эффективно реализована только в случае перевода ее на уровень организационных технологий. Организационные технологии предполагают установление нормативов и операций, регламентирующих деятельность, взаимосвязи, зависимости и контакты как внутри института или органа, так и вне — со стейкхолдерами[1]. Наряду с организационными технологиями по каждому направлению и, более того, каждой операции в рамках программы кибербезопасности необходимо определить исчерпывающий перечень программно-аппаратных средств, а также программных платформ и продуктов, обеспечивающих безусловное выполнение задач, сформулированных в рамках стратегии.

В идеале в рамках программы управления рисками института и органа должны быть указаны люди, выполняющие каждую функцию, процессы, аппаратные и программные средства, а также предоставляемые данные, позволяющие в совокупности обеспечивать безусловное выполнение функций, связанных с реализацией целей стратегии финансовой кибербезопасности. При определении инструментария важно не замыкаться на программных и аппаратных средствах, а в полной мере учитывать риски социального инжиниринга и способы их устранения. Кроме того, при разработке программ необходимо учитывать, что отдельный, даже самый мощный, финансовый институт не может полностью элиминировать угрозы в сфере кибербезопасности. Соответственно, программы каждого конкретного финансового института должны быть составлены таким образом, чтобы наряду с выполнением внутренних задач они являлись фрагментом общестрановой и шире — международной — системы кибербезопасности финансового сектора. Ключевым направлением при разработке стратегии финансовой кибербезопасности должно быть обеспечение надежной защиты проведения транзакций и хранения данных в киберсреде по основным финансовым операциям. В их число входят хранение депозитов, кредитование, работа платежных систем, клиринговые и факторинговые операции, а также расчетно-кассовое обслуживание и финансовая поддержка инвестиционных операций.

4. *Мониторинг.* Первостепенной задачей является создание для одних и развитие для других финансовых учреждений и органов государственной власти систем всеобъемлющего мониторинга собственной программно-аппаратной инфраструктуры и киберсреды, откуда

[1] Стейкхолдеры — все заинтересованные в деятельности юридического лица сторонние субъекты, включая миноритарных акционеров, потребителей, контрагентов, профессиональные ассоциации, общественные группы давления и т. п.

исходят угрозы. Системы мониторинга должны включать в себя сетевой мониторинг в режиме 7/24, активное тестирование, стресс-тесты, проверки и системы взаимодействия корпоративных систем кибербезопасности с системами финансовой кибербезопасности на государственном и международном уровнях и т. п.

Эффективный мониторинг позволяет субъектам финансовой сферы не превышать допустимый уровень рисков, своевременно устранять недостатки в системе институциональной кибербезопасности, а также развивать контуры, обеспечивающие превентивное реагирование на угрозы. В этом большую помощь может оказать создание специализированных внутрикорпоративных, а также общегосударственных и частных организаций, занимающихся аудитом кибербезопасности. В зависимости от характера института, киберпрофиля рисков и угроз функции тестирования и аудита должны быть отделены от функций обеспечения киербезопасности на программном, организационном и, несомненно, кадровом уровнях. Наиболее эффективной формой организаций, специализирующихся на аудите кибербезопасности, подготовке и повышении квалификации кадров в этой сфере и т. п., являются частно-государственные партнерства. Именно партнерства не только позволяют наладить эффективную систему аудита и переподготовки кадров, но и дают возможность понять общесекторальные киберриски, уязвимости и угрозы и на кооперационной основе организовать разработку программных средств, их снижающих.

5. *Последовательность.* Работа в сфере финансовой кибербезопасности носит процессный характер. На стадии практического функционирования системы финансовой кибербезопасности ее работу можно представить в виде последовательных операций:

а) оценка характера, масштабов и последствий того или иного кибер-инцидента;

б) осуществление срочных мер по уменьшению последствий кибер-инцидента;

в) уведомление внутрикорпоративных и внешних, например правоохранительных, регулирующих и других государственных органов, а также стейкхолдеров организации о характере, последствиях, ущербе и принятых мерах по исчерпанию киберинцидента;

г) координация совместных усилий и мер в случаях, когда это будет признано необходимым, по устранению в будущем возможностей аналогичных киберинцидентов.

В рамках установления рисков и проведения контрольных оценок организация должна эффективно реагировать на инциденты. Помимо прочего необходимо устанавливать ответственность подразделений и лиц за киберинциденты. Должны быть прописаны процедуры принятия решений по устранению киберинцидентов, а также процедуры

взаимодействия с внутренними и внешними заинтересованными сторонами. Разработка и осуществление протоколов взаимодействий, как показывает опыт, заметно повышает эффективность мер в сфере кибербезопасности.

6. *Восстановление.* Существует четкая последовательность операций по реабилитации системы кибербезопасности после инцидента. Она включает:

а) устранение вредных последствий киберинцидента для сохранности данных и функционирования программных средств;

б) полное восстановление систем и данных, включая приведение их в нормальное состояние и прохождение стресс-тестов;

в) анализ результатов стресс-тестов, выявление и устранение всех уязвимостей, которые были обнаружены в ходе стресс-теста;

г) системный анализ киберинцидента не как отдельного события, а как фрагмента разнообразной совокупности кибератак на финансовые институты;

д) коммуницирование при необходимости с государственными органами и стейкхолдерами с информированием их о принятых практических мерах по ликвидации последствия инцидента и повышению эффективности кибербезопасности.

После того как будет восстановлена операционная стабильность и целостность данных и программно-аппаратных средств, дальнейшая работа должна основываться на приоритетности обеспечения бесперебойного функционирования финансовой организации. Доверие в финансовом секторе значительно повысится, если финансовые институты и государственные органы будут взаимно помогать друг другу не только на концептуальном, стратегическом и организационном уровнях, но и в повседневном преодолении последствий кибератак. В связи с этим важно наличие в инфраструктуре финансовой кибербезопасности специализированных аудиторских компаний. Они должны организовывать стресс-тесты и осуществлять подведение их итогов, а также выступать инициаторами игр и маневров по взаимодействию финансовых институтов и государственных органов в оперативном противодействии киберугрозам и ликвидации последствий киберинцидентов.

7. *Обмен информацией.* Первостепенное значение для обеспечения кибербезопасности в финансовом секторе имеет своевременный обмен достоверной, полезной информацией об угрозах, уязвимостях, инцидентах между финансовыми институтами и государственными органами. На государственном уровне хорошо себя зарекомендовали институционализированные и неформальные сети кибербезопасности, включающие финансовые институты, государственные, в том числе правоохранительные, банковские и финансовые органы, а так-

же аудиторские компании и организации, специализирующиеся на кибербезопасности.

Обмен технической информацией, включая индикаторы угроз, сведения о том, как были использованы уязвимости в корпоративных системах безопасности и т. п., позволяет финансовым институтам и государственным органам своевременно узнавать о новых методах, технологиях и программных продуктах, используемых злоумышленниками. Взаимопонимание между финансовыми субъектами, между финансовыми субъектами и государственными органами, а также между органами государственной власти обеспечивает эмерджентное знание, а соответственно, и возможность противостоять злоумышленникам, использующим общесекторальные уязвимости. Именно такого рода уязвимости потенциально могут не только привести к нарушению в работе отдельных финансовых институтов, но и поставить под угрозу государственную и международную финансовую стабильность и целостность. С учетом первостепенной важности такой работы государственные органы должны постоянно выявлять и оперативно устранять любые препятствия внутристрановому и международному обмену информацией в сфере финансовой кибербезопасности. Только на этой основе может быть обеспечено глобальное государственно-корпоративное противодействие международной организованной финансовой киберпреступности.

8. *Непрерывное обучение*. В рамках финансовых институтов, государственных органов, аудиторских организаций и компаний в сфере кибербезопасности должно быть организовано внутри- и межинституциональное обучение по вопросам кибербезопасности, включая концептуальное стратегирование, управление кибербезопасностью, оценку рисков, контроль, мониторинг, программно-аппаратное опережающее реагирование на киберугрозы и инциденты, противодействие социальному инжинирингу, восстановление корпоративных и государственных программных и аппаратных инфраструктур после киберинцидентов и т. п.

Киберугрозы развиваются ошеломительными темпами. Киберпреступники и кибертеррористы постоянно берут на вооружение все новые практики, программные решения и технологические новации. Все это происходит на фоне революции в финансовом секторе, связанной с проникновением в финансовые технологии новых способов шифрования, транзакций и т. п. В этих условиях стратегии кибербезопасности и соответствующие им нормативы, процедуры и программные средства, а также системы стресс-тестирования и подготовки кадров требуют периодического пересмотра и обновления. Только при постоянном изменении программные, аппаратные, организационные, управленческие и кадровые решения в сфере кибербезопасности будут опережающим образом адаптированы к множащимся рискам, возрастающим угрозам и стремительному изменению киберсреды. При этом сам по себе финансовый сектор не изолирован от других секторов экономики. Более того, он является их сердцевиной. Проблемы в иных, нефинансовых секторах экономики, и особенно в энергетике и телекоммуникациях, могут оказать заметное позитивное или негативное влияние на ситуацию с кибербезопасностью в финансовом секторе. Поэтому руководители и акционеры финансовых институтов, первые лица государственных органов должны рассматривать вопросы кибербезопасности как ключевые вопросы не просто развития, а выживания общества, бизнеса и государства. Вопросы кибербезопасности должны найти свое место в рамках любых управленческих процессов в сфере бизнеса, национальной безопасности и государственной службы.

Глава 9. Предупреждение кибертерроризма и киберэкстремизма

§ 1. Общие подходы к предупреждению кибертерроризма и киберэкстремизма

В Рекомендациях ОБСЕ по предупреждению кибертерроризма (2013) отмечено, что усилия по борьбе с использованием Интернета террористами должны носить превентивный характер и поддерживать открытость Интернета. Любые необходимые принудительные действия должны иметь узкую направленность. Невозможно контролировать весь онлайн-контент террористического и криминального характера, лучше направить усилия на поддержание открытого Интернета, чем просто закрывать веб-сайты. Однако иногда необходимо принимать принудительные меры, особенно если соответствующие действия переходят определенные границы, например в случае подстрекательства к насилию или возникновения непосредственной угрозы. Такие меры, включающие блокирование веб-сайтов или удаление материалов, должны приниматься в соответствии с четко сформулированными национальными законами и международными обязательствами и принципами. Важно создать эффективную систему надзора, при которой пострадавшая сторона будет иметь возможность подать жалобу в случае неправомерного применения санкции.

Несмотря на то что технологии могут помочь сбору данных, именно сведения, получаемые в результате объединения информации, поступающей из многочисленных источников, включая государственные и прочие службы, позволяют составить наиболее полную карти-

ну. С помощью таких исследований необходимо выявлять основные враждебные группы и постоянно изучать и отслеживать их деятельность.

Эффективные шаги по борьбе с использованием террористами Интернета требуют создания сильных и взаимовыгодных *государственно-частных партнерств* (ГЧП). Государства не меньше бизнеса заинтересованы в безопасном киберпространстве как элементе защиты их финансовых интересов и репутации. Необходимо запрашивать и систематически использовать опыт и технические знания, которыми владеет частный сектор, в том числе путем формулирования четких, понятных законов, регулирующих сотрудничество с учетом роли и обязанностей каждой из сторон. Такое сотрудничество также может основываться на рекомендациях по сотрудничеству, вырабатываемых совместно и реализуемых всеми заинтересованными сторонами, выразившими однозначную готовность к долгосрочной работе. В рамках эффективного сотрудничества обе стороны должны определить контактных лиц, наделенных правами и возможностями выступать от имени своей стороны. В этом отношении сотрудничество с частным сектором может быть также усилено, например, путем создания организационной структуры, позволяющей частному сектору выступать от одного лица. Необходимо продолжить обсуждение вопроса об ответственности компаний или самого пользователя в связи с неадекватными мерами кибербезопасности или безопасности информационно-коммуникационных технологий. Существующие ГЧП или вклады частного сектора необходимо поддерживать, например, механизмами маркировки и передачи информации либо с помощью передовой практики сотрудничества.

В июне 2017 г. ведущие интернет-компании мира — Facebook, Microsoft, Twitter и YouTube объявили о создании Глобального интернет-форума по противодействию терроризму. В рамках форума компании договорились о совместной работе по созданию и совершенствованию технических средств по выявлению пропаганды терроризма и экстремизма в Интернете, оказании технического содействия в этом другим интернет-компаниям и своевременном информировании властей разных стран о том, как можно эффективно бороться с распространением террористических идей в Интернете.

В совместном заявлении крупнейших интернет-компаний говорится, что «распространение терроризма и экстремизма является насущной проблемой глобального характера и вызовом для всех нас». Каждая из этих компаний уже принимает меры по противодействию пропаганде терроризма на своих ресурсах.

Интернет-компании отметили, что в рамках нового форума они намерены обмениваться друг с другом технологическим опытом по

отслеживанию и удалению из Интернета информации экстремистского характера, сотрудничать с общественными организациями и научным сообществом для усовершенствования этой работы.

Работа будет сосредоточена на трех основных направлениях: технологические решения, исследовательская работа, обмен информацией.

Координация действий должна осуществляться не только между участниками форума, но и с Управлением ООН по противодействию экстремизму и терроризму. Еврокомиссия выделила на работу форума 10 млн евро.

Кроме того, участники форума готовы предоставить результаты своих исследований более мелким интернет-компаниям и по мере возможностей оказать им техническое содействие в противодействии пропаганды терроризма в Интернете. Компании также договорились о проведении мастер-классов и конференций для всех участников интернет-индустрии, заинтересованных в борьбе против экстремизма в Интернете.

Контртеррористический форум стал результатом объединения интернет-форума Евросоюза (ЕС) и совместной информационной базы хеширования. Интернет-форум ЕС появился в 2015 г. и является ГЧП, созданным для поиска наилучших путей для выявления и устранения террористической пропаганды и разжигания ненависти в Интернете. База хеширования представляет собой общую базу данных цифровых отпечатков из «самых экстремальных и вопиющих» террористических изображений и видео, вследствие чего материал, помеченный и удаленный с одной платформы, автоматически удаляется и на других. Эти инициативы были ответом на давление со стороны европейских правительств, обвинявших IT-компании в разжигании ненависти в Интернете.

В результате некоторые компании усилили борьбу с экстремистским контентом. Корпорация Google ужесточила борьбу с распространением видеозаписей экстремистского содержания на платформе YouTube. Google планирует расширить сотрудничество с общественными организациями, борющимися с распространением экстремистских материалов в Интернете. С их помощью компания сможет обнаруживать на YouTube контент, который предназначается для вербовки потенциальных экстремистов. Также корпорация собирается связываться с лицами, заинтересовавшимися подобными видеозаписями, и отправлять им ссылки на записи антиэкстремистского содержания.

Facebook также представила новые технологии по борьбе с терроризмом. Сотрудники компании сообщили, что тестируют программное обеспечение, которое будет выявлять в социальной сети вербов-

щиков и экстремистов. Основная роль в процессе отводится искусственному интеллекту[1].

Интернет-пользователи являются важной частью борьбы с использованием террористами Интернета. На индивидуальном уровне существует потребность в *повышении осведомленности конечного пользователя* об ответственном использовании Интернета и о возможных последствиях неосторожного раскрытия личных данных. Повышение осведомленности и обучение отдельных интернет-пользователей тому, как сохранять безопасность, должно начинаться со школьного образования, например путем включения в него экзамена по кибербезопасности и безопасности информационно-коммуникационных систем, и продолжаться в течение всей рабочей карьеры и пенсионного возраста человека. На групповом уровне для интернет-пользователей необходимо создать механизмы и системы, с помощью которых они смогут контролировать друг друга. Сюда необходимо включить соответствующие механизмы передачи информации и маркировки со стороны частного и (или) государственного сектора и знания о том, какую информацию необходимо направлять. Организации гражданского общества играют особую роль в этом отношении как в плане борьбы с идеями террористов, так и в плане информирования о таких преступлениях конечного пользователя и сообщения о террористическом контенте в соответствующие органы. Необходимо продолжить обсуждение ответственности пользователя, а также вопроса о том, как привлекать интернет-пользователей к оказанию помощи при возникновении чрезвычайных ситуаций.

Требуется объединение усилий, направленных на борьбу с различными формами (насильственного) экстремизма в Интернете. Несмотря на то что важно признавать преступления на почве нетерпимости и другие формы правого экстремизма в качестве отдельного вопроса и разбираться с ними на этом основании, особенно с точки зрения образования, повышения осведомленности, реагирования органов правопорядка и судебных органов, все же возникает вопрос возможного дублирования усилий по предотвращению таких выражений насилия и терроризма. Например, требуется более подробное исследование переломных моментов, когда экстремистские взгляды принимают насильственную форму. Это означает, что необходимо опубликовать базовую информацию, которая может использоваться для борьбы со всеми формами экстремизма. Такая информация должна включать все факторы, в том числе мотивацию, обеспечивая лучшую подготовку к возможным новым формам насильственного экстремизма в будущем. В этом отношении также важно активизировать усилия по сопоставлению методов и выявлению общих черт между разными формами контрмер для борьбы с разными формами экстремизма, например, для борьбы с идеями и с ксенофобскими высказываниями.

[1] См.: URL: https://www.kommersant.ru/doc/3337096.

Направления предупреждения кибертерроризма

1. *Баланс между потребностями охраны правопорядка и основными свободами.* Большие объемы коммуникационных данных указывают на то, что меры правоохранительных органов, направленные на противодействие использованию террористами Интернета как тактического средства, должны быть скорее упреждающими, чем ответными. Они не должны применяться за счет нарушения прав человека и основных свобод.

Для предотвращения использования террористами Интернета как тактического средства одновременно перед правоохранительными и антитеррористическими органами ставятся сложные задачи. Нарушители могут использовать анонимные коммуникационные технологии или публичные точки доступа к Интернету (например, интернет-кафе), чтобы скрыть свою личность. Кроме того, они могут использовать криптографические технологии для того, чтобы помешать доступу к контенту сообщения, а также к хранящимся данным. В связи с этой анонимностью некоторые страны ввели инструменты интенсивного расследования, которые обязывают подозреваемого предоставить пароли к зашифрованному материалу. Разные юрисдикции пришли к разным выводам в отношении того, как это повлияло на основные права человека, особенно в отношении запрета свидетельствования против самого себя. Кроме того, законы, обязывающие подозреваемых выдавать ключи к зашифрованному материалу, часто не учитывают такие новые технологии, как TrueCrypt, которые позволяют скрывать контент даже при выдаче паролей.

Несмотря на то что контролировать весь сетевой контент террористического и криминального характера невозможно, эксперты подчеркивают, что лучше сохранить открытый Интернет и собирать свидетельства для преследования нарушителей, чем закрывать сайты. Иногда принудительные меры неизбежны, особенно если действия пользователей выходят за определенные границы, например, в случае подстрекательства к насилию или возникновения непосредственной угрозы. Однако такие меры, включающие блокирование веб-сайтов или удаление материалов, которые часто вызывают противоречивое отношение общественности, должны приниматься в соответствии с четко сформулированными национальными законами и принципами, следует соблюдать основные права и устанавливать, какими угро-

зами оправдываются конкретные меры. Кроме того, важно создать эффективную систему надзора, при которой пострадавшая сторона будет иметь возможность подать жалобу в случае применения к ней неправомерных санкций. В разработку политики, связанной с принудительными мерами, необходимо вовлекать общественность и гражданское общество и обращаться к ним за содействием. Это важно для того, чтобы объяснить, чего пытаются добиться власти, и избежать отрицательной реакции общественности, которая, в свою очередь, создает возможности для развития терроризма. Аналогичным образом власти должны принимать во внимание то, как такие усилия повлияют на международное сотрудничество.

2. *Освобождение разведывательной информации от излишней детализации.* В периоды бюджетных ограничений специально обученный персонал, способный анализировать постоянно растущие объемы передаваемых данных, должен работать максимально эффективно.

При сборе разведывательных данных в рамках противодействия киберугрозам необходимо учитывать человеческий фактор. Несмотря на то что власти способны собирать огромные объемы данных, возникают проблемы с большим количеством информации, поскольку технические возможности целенаправленной тщательной проверки таких данных развиваются не столь быстрыми темпами. Специально обученные кадры, таким образом, становятся важнейшим фактором, особенно в чрезвычайных ситуациях, поскольку: 1) для работы с несистематическими разведывательными киберданными требуется высокий уровень профессионализма, технических знаний и аналитических навыков и 2) после анализа разведывательных данных необходимо действовать на их основании, в том числе в сотрудничестве с партнерскими органами и странами. Поэтому так важно обеспечить обучение и укрепление потенциала разведывательных кадров в этих областях. Кроме того, эксперты должны быть обучены тому, как наилучшим образом использовать *разведку по открытым источникам*, в том числе с применением таких средств, как триангуляция и фальсификация «плохой» информации.

Преимущества ГЧП пока еще недостаточно используются в связи со сбором и совместным использованием разведывательных данных. Для более эффективного использования всего богатства знаний, которыми обладает частный сектор, властям необходимо установить четкую политику, законодательство, механизмы и процедуры сотрудничества. Также для обеих сторон важно создать координационные центры, действующие в качестве единых контактных точек в рамках обеспечения своевременного сотрудничества.

Уже существуют международные сообщества, позволяющие осуществлять совместное использование разведывательных данных и информации, связанной с киберпреступлениями и использованием Интернета террористами. И все же некоторые эксперты придерживаются мнения, что, хотя такие механизмы являются устойчивыми платформами для сотрудничества, их эффективность порой ограничена из-за того, что они связаны с определенными международными правовыми инструментами, в которых участвуют не все государства. Более того, сама природа разведывательных данных и связанных с ними средств защиты иногда препятствует тому, чтобы распространять такие данные в международных масштабах.

3. *Роль интернет-пользователей.* Именно частные интернет-пользователи часто бывают самым слабым звеном с точки зрения борьбы с использованием террористами Интернета как тактического средства, например из-за небрежного обращения со своей личной информацией. Отдельный интернет-пользователь также является ключом к предотвращению онлайн-деятельности террориста, которая может привести к потенциальным атакам.

Прежде чем рассматривать пользователя в качестве ключевого участника работы по предотвращению использования террористами Интернета как тактического средства, необходимо разъяснить нынешнюю роль и статус пользователей и степень наделения их правами и возможностями. Например, можно возразить, что неразумно ожидать от обычных интернет-пользователей умелого обращения со сложным набором технологических инструментов и программных решений, доступных в настоящее время, управления ими или принятия информированных решений в отношении этих инструментов. В самом деле, многие пользователи полагаются на знания, навыки, профессионализм, правовые и нормативные структуры, технологические ноу-хау и инженерное мастерство широкого спектра посредников, чтобы те разработали четкие однозначные руководства, надежную аппаратуру и программные решения на основании демократических принципов, производящих надежные, заслуживающие доверия и уважаемые продукты, которыми могут пользоваться обычные потребители. Но можно возразить, что именно пользователь умело манипулирует технологическими достижениями эры Интернета нечестными способами, например планирует и осуществляет террористические атаки. Это отражает поведение пользователей, а не сами технологии. Пользователи, таким образом, могут принять на себя обязательства больше узнать о принадлежащих им инструментах, чтобы понять, что может случиться, и предпринимать разумные меры для защиты своих систем от атак и предотвращать их захват для последующих атак против других людей.

Предупреждение использования террористами и экстремистами социальных сетей

1. *Совершенствование работы правоохранительных органов.* Учитывая бюджетные ограничения, специально обученные кадры, способные анализировать и реагировать на использование террористами инструментов социальных сетей, должны работать максимально эффективно.

Форумы для общения и социальные сети все больше демонстрируют и свои преимущества, и свои недостатки. В то время как террористы используют их потенциал для коммуникации, налаживания отношений, подстрекательства, восхваления терроризма и операционного планирования, правоохранительные органы также могут привлекать эти инструменты для получения более глубокого представления о деятельности террористов, собирая при этом свидетельства для преследования виновников преступной деятельности. Принимаемые ответные меры в первую очередь должны учитывать соответствующие правовые процедуры, защиту данных, исключение дискриминации, неприкосновенность частной жизни и вопросы, связанные с профилированием, в сочетании с обеспечением гарантии свободы мнений и их выражения и права на свободу собраний.

Ввиду ценности информации, размещаемой на сайтах социальных сетей, аналитики правоохранительных органов по всему миру уже изучают информацию, размещаемую в Twitter и Facebook, для сбора разведывательных данных в рамках борьбы с использованием террористами сайтов социальных сетей, что является очень трудоемкой работой. Поскольку им приходится иметь дело с огромными объемами данных, некоторые правоохранительные органы вкладывают средства в развитие цифровых инструментов, способных сканировать весь спектр социальных сетей, что позволяет получать больше данных. Такие технологии крайне важны, если учесть соотношение количества сотрудников правоохранительных органов и киберпреступников, включая террористов.

Однако существуют и сомнения в пользе таких инструментов: многие эксперты отметили, что основная трудность заключается в том, чтобы научить компьютеры читать. Например, как программа может определить разницу между ценной информацией и тонкими различиями смысла, с одной стороны, и шуткой — с другой? Кроме того, возникает проблема с аутентичностью, когда речь идет о компьютерных программах, известных как спам-боты, которые уже не дают покоя таким сервисам, как Twitter, своими «мусорными» сообщениями, аналогичными спаму в электронной почте. Многие эксперты полагают, что возможности создавать спам-боты только увеличатся со

временем, и потенциально они смогут обманывать аналитиков и их программы, которые будут думать, что имеют дело с деятельностью реального человека, в то время как это будет искусственно создано с целью вводить в заблуждение. Кроме того, применение технологии отслеживания без определения узкой и направленной правоохранительной цели также вызывает вопросы с точки зрения прав человека и основных свобод, даже если информация общедоступна, а действия не направлены на конкретные группы или определенных лиц. В итоге все равно потребуются обученные специалисты, которые будут отсеивать данные, собранные программами или внешними источниками, и принимать соответствующие меры.

2. *Наделение интернет-пользователей и гражданского общества правами и возможностями.* Социальные сети играют важную роль в предотвращении использования террористами инструментов социальных сетей и борьбе с терроризмом.

Концепции «последней линии обороны» и «службы экстренного реагирования» представляют собой подходящие отправные точки для рассмотрения роли и прав конечных пользователей в борьбе с использованием террористами инструментов социальных сетей. Можно утверждать, что конечные пользователи сами заинтересованы в безопасных и защищенных социальных сетях. В качестве службы экстренного реагирования пользователи должны быть в состоянии распознавать случаи злонамеренного использования социальных сетей террористами и иметь стимулы для сообщения о таких случаях операторам социальных сетей, компетентным государственным органам и (или) организациям гражданского общества. В качестве «последней линии обороны» отдельные пользователи должны быть обучены ответственному сетевому поведению, разбираться в вопросах конфиденциальности и рисках, связанных с раскрытием личных данных и иной потенциально секретной информации через социальные сети. Индивидуальные пользователи также должны быть устойчивы к распространяемым через социальные сети сообщениям и контенту, имеющим насильственный характер или потенциально являющимся сигналом к насильственному отношению.

Особая роль принадлежит организациям гражданского общества, которые играют крайне важную роль в укреплении устойчивости конечных пользователей к насильственному контенту. Важно, что организации гражданского общества основывают свою деятельность на допустимости, надежности и свободе действий, которых может не быть у государственных властей, особенно при борьбе с ненасильственным экстремизмом. Их следует стимулировать к использованию социальных сетей для формулирования и распространения позитив-

ных обращений и контрмер, противостоящих террористической пропаганде и разжиганию вражды.

Социальные сети дают организациям гражданского общества уникальные инструменты защиты: получение возможности выразить свое несогласие, инновационные способы оформления и целенаправленное обращение к конкретной аудитории. Например, инструменты социальных сетей можно использовать для объединения конечных пользователей и других заинтересованных лиц, таких как бывшие экстремисты и пострадавшие, в рамках создания интерактивных сообществ на основе позитивных ценностей. Аналогичным образом организации гражданского общества могут быть задействованы в мониторинге и механизмах предоставления рекомендаций для выявления и рассмотрения подозрительных материалов или действий, включая организацию «сетевого превентивного вмешательства» для взаимодействия с конечными пользователями, подвергающимися риску.

Некоторые операторы социальных сетей предлагают механизмы, которые могли бы применять пользователи для маркировки контента, нарушающего правила сообщества или условия обслуживания. Однако пока не ясно, насколько часто такие возможности фактически используются и сколько людей занимается отсевом такого контента. Также не ясно, в какой степени компании информируют пользователей о таких возможностях и стимулируют людей к их использованию. Фактически поощрение использования таких механизмов может быть контрпродуктивным и дорогостоящим для операторов и представлять собой репутационный риск. В будущем подобные дебаты необходимо сосредоточить, во-первых, на том, как стимулировать пользователей к применению таких возможностей, а во-вторых, на том, какие стимулы можно было бы создать, чтобы операторы активно продвигали такие системы.

Особую сложность при обучении интернет-пользователей безопасному использованию инструментов социальных сетей представляет динамичная среда самого Интернета. Например, Facebook существует с 2004 г., а Twitter — с 2006 г. Другая сложность заключается в стимулировании пользователей к фактическому применению их знаний о кибербезопасности. В связи с этим киберобразованию необходимо сосредоточиться как на практических мерах, так и на изменении поведения, т. е. поощрять пользователей к безопасному поведению в течение длительного периода времени. В этом отношении стимулы крайне важны для периодического поощрения хорошего поведения.

3. *Роль частного сектора*. Поскольку большинство инструментов социальных сетей принадлежит частным компаниям, прозрачные, институционализированные и взаимовыгодные ГЧП исключительно

важны для предотвращения злоупотребления террористами инструментами социальных сетей.

Предотвращение использования террористами инструментов социальных сетей и борьба с этим явлением преимущественно являются обязанностью органов государственной власти. В связи с этим представляются необоснованными потенциальные обязательства, налагаемые на операторов социальных сетей, по мониторингу социальных сетей. Однако и у частного сектора есть коммерческий интерес во внесении своего вклада в эту работу и в поиске взаимоприемлемых решений о сотрудничестве.

Для того чтобы получить широкомасштабную поддержку частного сектора, было предложено обратиться к корпоративной социальной ответственности операторов социальных сетей и к их интересу к защите собственного имиджа и репутации. Однако при рассмотрении репутационных вопросов власти должны быть осторожны в связи с тем, что владельцы и операторы социальных сетей могут опасаться того, чтобы не выглядеть в глазах пользователей и клиентов агентами или представителями правительства.

Многие провайдеры уже приняли разного рода меры по защите своих сетей от террористических материалов, например путем изъятия видеоматериалов с террористической пропагандой. Однако такие ответные меры были несистематическими, и разными владельцами применялись разные правила. Одна из идей заключалась в том, чтобы разработать добровольные руководящие принципы, которые можно было бы применять повсеместно и которые давали бы определенную степень устойчивости. В этом отношении важно подумать о стимулах для поощрения долгосрочного соблюдения требований (т. е. позитивное закрепление), включая потенциальные (коммерческие) выгоды, например улучшение репутации, снижение административных затрат или привилегированный доступ к дополнительным ресурсам.

§ 2. Превентивное устранение угроз кибертерроризма

В наиболее сконцентрированном виде это направление борьбы с кибертерроризмом выражено в британских Стратегии национальной кибербезопасности 2016—2021 гг. и Стратегии цифровой безопасности. Суть такого подхода заключается в переходе от концепта отражения угрозы к *превентивному блокированию угроз*.

Активная киберзащита — это принцип опережающего реагирования на возможные риски и угрозы целостности и надежному функционированию телекоммуникационных сетей, баз данных, хранилищ информации и информационных систем.

В коммерческом контексте под активной кибербезопасностью обычно понимаются опережающая диагностика и аналитика характера рисков и угроз, распознавания инструментов и почерка кибератак и определение на этой основе акторов деструктивных действий в киберпространстве с последующим осуществлением мер по активному противодействию их угрозам.

В рамках Стратегии цифровой безопасности Великобритании правительство впервые приняло решение использовать принцип *активной кибероборо*ны на государственном уровне. Для этого будут использоваться имеющиеся у правительства уникальные разведывательно-аналитические возможности, программно-аппаратный потенциал и компетенции государственных служащих, включая сотрудников разведки правоохранительных органов и военнослужащих.

Для превентивного отражения кибератак следует:

— силами служб, комитетов и подразделений по борьбе с кибератаками своевременно выявлять появление у кибертеррористов программно-аппаратных и кадровых возможностей проведения разрушительных сетевых операций;

— в полной мере использовать программные и агентурные возможности внедрения в кибертеррористические сети и группировки с целью их разгрома еще на стадии подготовки кибертеррористических актов.

Правительство Великобритании будет оценивать успехи в борьбе против терроризма на основании степени достижения:

— количества и ущерба от кибератак, осуществленных террористическими группировками самостоятельно либо одиночными террористами, приверженцами джихадизма, а также хакерскими группировками, действующими по заказу террористов в рамках модели «киберпреступление как услуга»;

— создания эффективной программно-аппаратной и агентурной сети мониторинга и внедрения в террористические организации, практикующие либо собирающиеся взять на вооружение кибертерроризм;

— масштабов выявления лиц и групп, вступивших в контакт с террористами, по тематике использования программно-аппаратных средств и социального инжиниринга как для непосредственного проведения киберагрессивных актов, так и для создания IT-инфраструктуры осуществления традиционных террористических атак.

Правительство Великобритании осуществит меры по улучшению ресурсного, программно-аппаратного и кадрового потенциала Национальной группы по борьбе с киберпреступностью, находящейся в распоряжении Национального агентства по борьбе с преступностью.

Указанная группа постепенно будет переориентирована с координационных функций на проведение активных мероприятий в рамках политики сдерживания и на расследование наиболее серьезных киберпреступлений. Для этого группа сможет шире привлекать к своим операциям службы, занимающиеся киберпреступностью, полицию, а также разведывательные структуры, а в случае принятия соответствующего закона — частные компании цифровой безопасности. Группа развертывает сеть подразделений по борьбе с киберпреступностью на региональном уровне. В этих целях группе будут переданы подразделения и отдельные сотрудники правоохранительных органов, занимающиеся борьбой с киберпреступностью на низовом уровне, вплоть до городов и поселений.

Для снижения ущерба от высокоуровневой киберпреступности предусматриваются следующие меры:

— сплошная переподготовка работников правоохранительных органов, начиная от оперативных сотрудников до руководства по вопросам кибербезопасности и борьбы с киберкриминалом. Кроме того, в рамках учебы необходимо резко повысить уровень осведомленности работников правоохранительных органов о потенциале цифровых инструментов и методов расследования киберпреступлений. Также каждый работник правоохранительных органов в ходе учебы должен получить комплекс необходимых знаний и навыков по собственной кибергигиене и сдать экзамен;

— насыщение киберсреды программно-аппаратными средствами раннего распознавания и фиксации киберугроз.

При всей важности совершенствования программно-аппаратного оснащения правоохранительных органов и насыщении киберсреды средствами распознавания и идентификации правительство Великобритании будет поддерживать усилия правоохранительных органов по наращиванию и повышению эффективности страновой и международной сети агентов-осведомителей и сотрудников под прикрытием среди национальной и международной организованной киберпреступности. Никогда программно-аппаратные средства не заменят деятельность работников под прикрытием, осведомителей-агентов в борьбе с киберпреступностью и кибертерроризмом.

Планируется рассмотреть возможность введения обязательной цифровой идентификации граждан, имеющих профессию и навыки, связанные с разработкой и использованием высоких технологий, особенно в киберцифровом пространстве и сфере поведенческих и биотехнологий; внести на обсуждение вопрос об обязательной идентификации подобного рода пользователей при любом подключении к Интернету и одноранговым сетям.

Поставлена задача переориентировать взаимодействие с бизнесом со взаимопомощи при ликвидации киберинцидентов и расследовании киберпреступлений на опережающее распознавание и сдерживание деструктивных акторов в киберсреде. В этих рамках предусмотрено начать предоставление разведывательных сведений бизнесу и университетам при неукоснительном соблюдении безопасности информации и государственных секретов.

Превентивная парадигма Стратегии цифровой безопасности, делающая акцент на раннем распознавании и сдерживании деструктивных акторов, базируется на трех основных принципах:

а) в условиях реального перехода общества, бизнеса и государства в мир «Интернета всего» невозможно гарантировать распознавание, сдерживание и превентивное устранение угроз во всех случаях. Это цель, к которой необходимо стремиться, но обеспечить стопроцентную ее реализацию невозможно;

б) стратегия сдерживания и превентивного устранения угроз может быть осуществлена только в условиях наличия четкой иерархии опасности угроз для Великобритании, ее обороноспособности, для бизнеса и жизнедеятельности гражданского общества. Представляется необходимым создать систему национальной кибербезопасности, которая исключит или почти исключит возможность успешной атаки деструктивных акторов на сети и объекты критической инфраструктуры;

в) в мире, где все пользуются компьютерами, гаджетами, вещами, подключенными к Интернету, Стратегия цифровой безопасности не может быть реализована исключительно на уровне правительства и только за счет государства. Национальная кампания за обеспечение каждым британцем требований кибергигиены является важнейшим компонентом Стратегии. Бизнес должен в полной мере осознать угрозы, исходящие из киберсреды, и не жалеть ресурсов на создание эффективных систем киберзащиты, особенно в финансовой, высокотехнологической и медицинской сферах.

В настоящее время в Великобритании создана эффективная защита доменной зоны «uk» и платформ, сайтов, блогов и иных ресурсов в этой зоне. Однако до сих пор должным образом не защищены другие сегменты информационной среды, включая мессенджеры, социальные сети, гаджеты, платформы социальных медиа. Главными критериями прогресса в части защиты информационной среды Великобритании будут:

— сокращение, в том числе количественное, успешных кибератак, связанных с взломом платформ социальных медиа, сетей, мессенджеров с размещением там противозаконных сообщений, а также резкое снижение уровня зараженности гаджетов;

— разработка процедур и проведение обучения государственных служащих, наемных работников и граждан методам противодействия социальной инженерии — неотъемлемой части цифровых нападений;

— увеличение доли превентивной блокировки вредоносных программ и технических артефактов, используемых киберпреступниками и кибертеррористами для активных мероприятий и эксплуатации уязвимостей;

— количественная оценка изменений в масштабах экономического ущерба от кибератак на телекоммуникационный трафик Великобритании и инфраструктуру национальных и региональных провайдеров;

— оценка возможностей интегрированных действий Центра правительственной связи, вооруженных сил Великобритании и Национального криминального агентства по превентивному реагированию на серьезные киберугрозы.

Прогресс информационных и поведенческих технологий позволяет встраивать их в интернет-платформы, онлайн-продукты и услуги, делающие их «безопасными по умолчанию». Это предполагает, что программное обеспечение безопасности ресурсов в доменной зоне Великобритании, телекоммуникационных протоколах, а также программно-аппаратных компонентах «Интернета вещей», а в последующем «Итернета всего» будет обеспечивать *безопасность по умолчанию* в отношении подавляющего числа кибератак и кибернападений. В этих условиях пользователи в правительстве, бизнесе и гражданском обществе по умолчанию и бесплатно будут иметь максимальную безопасность, если только они сами не захотят добровольно снизить ее уровень, отключив соответствующие компоненты.

Великобритания в рамках реализации Стратегии цифровой безопасности будет последовательно переходить от парадигмы «моя безопасность — мое дело» к парадигме «безопасность каждого — дело всех». К настоящему времени уже имеются необходимые программно-аппаратные, организационные и юридические предпосылки для реализации новой парадигмы. Создается финансовая бизнес-модель, которая сделает парадигму жизнеспособной в условиях бюджетных ограничений.

Поскольку Великобритания является лидирующей финансовой державой, а Лондон — мировой инвестиционный центр, до 2021 г. будут предприняты все необходимые меры для того, чтобы сделать максимально безопасными любые электронные финансовые транзакции.

В рамках перехода к виртуальному банкингу, всемирному распространению финансовых инноваций на основе телекоммуникационных протоколов, финансовых технологий, финансовых и платежных систем на основе блокчейна британское правительство совместно с

банками и инновационным сектором разрабатывает ресурсно обеспеченную частными и государственными инвестициями, увязанную по срокам, исполнителям и мероприятиям программу «Безопасные цифровые финансы и инвестиции» со сроком реализации до 2020 г. и дальнейшей пролонгацией.

К началу 2019 г. будет создана и начнет работу Национальная система цифровой безопасности «Fintech». Эта система обеспечит кибер- и цифровую безопасность для инновационной британской финансовой аистемы. Она включает краудфандинговые и краудинвестинговые платформы, кредитование «P2P», небанковские платежные системы и финансовые инновации на основе блокчейна.

Британское правительство видит значительные риски в широком распространении услуг по использованию сложного биотехнологического оборудования по модели «оборудование как сервис». Особенно резко возрастают риски в рамках развития синтетической биологии, интегрирующей достижения информационных и биологических наук. Британское правительство уже подготовило и внесет на рассмотрение партнеров в странах ЕС, Соединенных Штатах, странах британского Содружества предложения по заключению международного договора об обязательной сертификации биотехнологических лабораторий, предоставляющих оборудование и выполняющих работы для сторонних заказчиков. Предусматривается, что эта сертификация будет включать в себя распространение в международном масштабе на биотехнологическую отрасль и сектор синтетической биологии правил и норм, применяемых в настоящее время для финансового сектора, включая правила «знай своего клиента» и получения клиентами специальных разрешительных сертификатов от международных или страновых регулирующих органов на право размещения заказов или аренды оборудования.

§ 3. Защита от терроризма критической информационной инфраструктуры

Основополагающим документом, регламентирующим эти вопросы в данной сфере в России, является Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Данный Закон регулирует отношения в области обеспечения безопасности критической информационной инфраструкруры (далее — КИИ) России в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак.

При этом под *компьютерной атакой* в целом понимается целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Компьютерный инцидент согласно Закону — это факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Сама *КИИ* — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. В объекты КИИ входят информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Субъектами КИИ являются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Под информационными ресурсами РФ в Законе понимаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории РФ, в дипломатических представительствах и (или) консульских учреждениях РФ.

К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся:

— подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ;

— организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, для обеспечения координации деятельности субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

— подразделения и должностные лица субъектов КИИ, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

Средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, являются технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

В государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ осуществляются сбор, накопление, систематизация и анализ информации, которая поступает в данную систему через средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, информации, которая представляется субъектами КИИ и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, в соответствии с перечнем информации и в порядке, определяемыми федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, а также информации, котограя может представляться иными не являющимися субъектами

КИИ органами и организациями, в том числе иностранными и международными.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, организует в установленном им порядке обмен информацией о компьютерных инцидентах между субъектами КИИ, а также между субъектами КИИ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

Категорирование объекта КИИ представляет собой установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Категорирование осуществляется:

— исходя из социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимального времени отсутствия доступа к государственной услуге для получателей такой услуги;

— политической значимости, выражающейся в оценке возможного причинения ущерба интересам России в вопросах внутренней и внешней политики;

— экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам КИИ и (или) бюджетам РФ;

— экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

— значимости объекта КИИ для обеспечения обороны страны, безопасности государства и правопорядка.

Устанавливаются три категории значимости объектов КИИ — первая, вторая и третья.

Субъекты КИИ в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам КИИ. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих

критериев и их значениям, ему не присваивается ни одна из таких категорий.

Сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий субъекты КИИ в письменном виде в 10-дневный срок со дня принятия ими соответствующего решения направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, по утвержденной им форме.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, в 30-дневный срок со дня получения таких сведений проверяет соблюдение порядка осуществления категорирования и правильность присвоения объекту КИИ одной из категорий значимости либо неприсвоения ему ни одной из таких категорий.

В случае, если субъектом КИИ соблюден порядок осуществления категорирования и принадлежащему ему на праве собственности, аренды или ином законном основании объекту КИИ правильно присвоена одна из категорий значимости, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, вносит сведения о таком объекте КИИ в реестр значимых объектов КИИ, о чем в 10-дневный срок уведомляется субъект КИИ.

В случае, если федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, выявлены нарушения порядка осуществления категорирования и (или) объекту КИИ, принадлежащему на праве собственности, аренды или ином законном основании субъекту КИИ неправильно присвоена одна из категорий значимости и (или) необоснованно не присвоена ни одна из таких категорий и (или) субъектом КИИ представлены неполные и (или) недостоверные сведения о результатах присвоения такому объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, в 10-дневный срок со дня поступления представленных сведений возвращает их в письменном виде субъекту КИИ с мотивированным обоснованием причин возврата.

Субъект КИИ после получения мотивированного обоснования причин возврата сведений, указанных в законе, не более чем в 10-дневный срок устраняет отмеченные недостатки и повторно направляет такие сведения в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ.

Сведения об отсутствии необходимости присвоения объекту КИИ одной из категорий значимости после их проверки направляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, о чем в 10-дневный срок уведомляется субъект КИИ.

В случае непредставления субъектом КИИ сведений, указанных в законе, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, направляет в адрес указанного субъекта требование о необходимости соблюдения положений закона.

Категория значимости, к которой отнесен значимый объект КИИ, может быть изменена в порядке, предусмотренном для категорирования, в следующих случаях:

— по мотивированному решению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ РФ, принятому по результатам проверки, проведенной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ;

— в случае изменения значимого объекта КИИ, в результате чего такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости;

— в связи с ликвидацией, реорганизацией субъекта КИИ и (или) изменением его организационно-правовой формы, в результате чего были изменены либо утрачены признаки субъекта КИИ.

В целях учета значимых объектов КИИ федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, *ведет реестр значимых объектов КИИ* в установленном им порядке. В данный реестр вносятся следующие сведения:

— наименование значимого объекта КИИ;

— наименование субъекта КИИ;

— сведения о взаимодействии значимого объекта КИИ и сетей электросвязи;

— сведения о лице, эксплуатирующем значимый объект КИИ;

— категория значимости, которая присвоена значимому объекту КИИ;

— сведения о программных и программно-аппаратных средствах, используемых на значимом объекте КИИ;

— меры, применяемые для обеспечения безопасности значимого объекта КИИ.

Сведения из реестра значимых объектов КИИ направляются в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

В случае утраты значимым объектом КИИ категории значимости он исключается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, из реестра значимых объектов КИИ.

Субъекты КИИ имеют право:

— получать от федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ РФ, информацию, необходимую для обеспечения безопасности значимых объектов КИИ, принадлежащих им на праве собственности, аренды или ином законном основании, в том числе об угрозах безопасности обрабатываемой такими объектами информации и уязвимости программного обеспечения, оборудования и технологий, используемых на таких объектах;

— в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;

— при наличии согласия федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

— разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта КИИ.

Субъекты КИИ обязаны:

— незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидакции последствий компьютерных атак на информационные ресурсы РФ, а также Центральный банк РФ (в случае, если субъект КИИ осуществляет деятельность в банковской сфере и в иных сферах финансового рынка) в установленном федеральным органом исполнительной власти порядке (в банковской сфере и в иных сферах финансового рынка указанный порядок устанавливается по согласованию с Центральным банком РФ);

— оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

— в случае установки на объектах КИИ средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

Субъекты КИИ, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, также обязаны:

— соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ;

— выполнять предписания должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ РФ, об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ, выданные этими лицами в соответствии со своей компетенцией;

— реагировать на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ;

— обеспечивать беспрепятственный доступ должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ РФ, к значимым объектам КИИ при реализации этими лицами полномочий, предусмотренных законом.

В целях обеспечения безопасности значимого объекта КИИ субъект КИИ в соответствии с требованиями к созданию систем безопас-

ности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, создает систему безопасности такого объекта и обеспечивает ее функционирование.

Основными задачами системы безопасности значимого объекта КИИ являются:

— предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом КИИ, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

— недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта КИИ;

— восстановление функционирования значимого объекта КИИ, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

— непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

Требования по обеспечению безопасности значимых объектов КИИ, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, дифференцируются в зависимости от категории значимости объектов КИИ. Этими требованиями предусматриваются:

— планирование, разработка, совершенствование и осуществление внедрения мпероприятий по обеспечению безопасности значимых объектов КИИ;

— принятие организационных и технических мер для обеспечения безопасности значимых объектов КИИ;

— установление параметров и характеристик программых и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов КИИ.

Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, могут устанавливать дополнительные требования по обеспечению безопасности значимых объектов КИИ, содержащие особенности функционирования таких объектов в установленной сфере деятельности.

Оценка безопасности КИИ осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, в целях прогнозирования возникновения возможных угроз безопасности КИИ и выработки мер по повышению устойчивости ее функционирования при проведении в отношении нее компьютерных атак.

При осуществлении оценки безопасности КИИ проводится анализ:

— данных, получаемых при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов КИИ, признаков компьютерных атак;

— информации, представляемой субъектами КИИ и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, в соответствии с перечнем информации и в порядке, определяемыми федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, а также иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными;

— сведений, представляемых в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов КИИ, о нарушении требований по обеспечению безопасности значимых объектов КИИ, в результате которого создаются предпосылки возникновения компьютерных инцидентов;

— иной информации, получаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, организует установку в сетях электросвязи, используемых для организации взаимодействия

объектов КИИ, средств, предназначенных для поиска признаков компьютерных атак в таких сетях электросвязи.

В целях разработки мер по совершенствованию безопасности КИИ федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, результаты осуществления оценки безопасности КИИ.

Основанием для осуществления плановой проверки объектов КИИ является истечение трех лет со дня:

— внесения сведений об объекте КИИ в реестр значимых объектов КИИ;

— окончания осуществления последней плановой проверки в отношении значимого объекта КИИ.

Основанием для осуществления внеплановой проверки являются:

— истечение срока выполнения субъектом КИИ выданного федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, предписания об устранении выявленного нарушения требований по обеспечению безопасности значимых объектов КИИ;

— возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте КИИ;

— приказ (распоряжение) руководителя федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры РФ, изданный в соответствии с поручением Президента РФ или Правительства РФ либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

По итогам плановой или внеплановой проверки федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, составляется акт проверки по утвержденной указанным органом форме.

На основании акта проверки в случае выявления нарушения требований вышеназванного Закона и принятых в соответствии с ним нормативных правовых актов по обеспечению безопасности значимых объектов КИИ федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, выдает субъекту КИИ предписание об устранении выявленного нарушения с указанием сроков его устранения.

Глава 10. Использование новейших технологий цифрового мира в предупреждении преступлений

§ 1. Стратегический подход в использовании новейших технологий цифрового мира в предупреждении преступлений

Понимание и использование новейших технологий цифрового мира в контексте преступности имеет двойственный характер. С одной стороны, данные и технологии используются преступниками для совершения криминальных действий. В этом плане новые технологии входят в число драйверов преступности и подробно рассмотрены выше. С другой стороны, технологии являются инструментом, позволяющим успешно не только бороться, но и профилактировать криминал.

В наиболее развернутом виде данный вопрос освещен в Современной стратегии предупреждения преступности (март 2016 г., Великобритания). В частности, в этом документе отмечено, что эффективные протоколы обмена информацией и координации действий между центральными и региональными полицейскими структурами, бизнесом и гражданским обществом являются ключом к повышению эффективности борьбы с криминалом. Данные и информационно-коммуникационные технологии являются важнейшим фактором создания систем эффективного обмена сведениями и результативного взаимодействия. Если еще несколько лет назад главные усилия правоохранительных органов были направлены на создание текстовых баз данных об организованной и уличной преступности, то в настоящее время ситуация в корне изменилась.

Уже сейчас не менее 70% хранилищ данных о криминале занимают видео- и фотофайлы. С переходом городов Великобритании с населением свыше 100 тыс. человек и всех транспортных коммуникаций страны на 100%-ный охват видеонаблюдением (не позднее 2018 г.) именно видеофайлы станут основным элементом данных и материалом для профилактики преступности и проведения расследований. В настоящее время перед системой криминальной юстиции и обеспечения правопорядка в Великобритании стоит задача не только технически ответить на этот вызов, но и оснаститься средствами и инструментами, позволяющими максимально полно использовать видеоинформацию совместно с текстовой и аудиоинформацией.

Британская полиция использует большие данные и технологии, причем не только программные, но и физические технологии (типа БПЛА). В отличие от ряда других стран британский криминал уступа-

ет полиции по своей оснащенности. Это дает определенные преимущества в ведении правоохранительной деятельности.

Чтобы наилучшим образом использовать данные и технологии, британская полиция предполагает не только осуществить до 2020 г. аппаратное и программное переоснащение, но самое главное — провести сплошное повышение квалификации полицейских, и в первую очередь на низовом уровне, изменить культуру полицейских расследований.

В ближайшее время не останется невысокотехнологичной преступности вообще. Даже уличные преступники будут использовать те или иные плоды высоких технологий.

Британский бизнес, особенно ключевая отрасль хозяйства — финансовая, требует от полиции качественного повышения уровня противодействия высокотехнологичной преступности. Для этого планируется продолжить работу по формированию специализированных подразделений по киберпреступности, в том числе в рамках ГЧП. Вместе с тем все британские полицейские должны иметь доступ к базам данных и современным инструментам, обеспечивающим эффективные коммуникации, профилактику и расследование преступлений с использованием информационных технологий. Наступило время, когда все британские полицейские, независимо от возраста, должны пройти ускоренные курсы подготовки в области использования информационно-коммуникационных технологий.

Анализ больших данных. Электронные устройства генерируют новые данные с невероятной скоростью. Значительная часть данных может быть использована для профилактики преступности. Если раньше общественность интересовали прежде всего процедуры доступа к персональным и корпоративным данным, то в ближайшие годы необходимо, не дожидаясь кризиса общественного мнения, четко регламентировать доступ правоохранительных структур к потоковым видеоданным, протоколам платежных систем и конечно же протоколам «Интернета вещей». Уже сегодня данные, в том числе геолокация, получаемые со смартфонов, позволяют раскрыть и предотвратить многие серьезные преступления. Потенциал данных, извлекаемых из «Интернета вещей», гораздо выше эффекта от данных геолокации со смартфона, хотя это и сложно представить.

Сегодня одной из наиболее высокооплачиваемых и развивающихся профессий являются специалист по данным и аналитик данных. Это люди, которые проектируют базы и хранилища данных, а также обеспечивают пользователям возможность воспринимать данные при помощи визуальных и дружественных интерфейсов. В Великобритании подобных специалистов не хватает даже для бизнеса, поэтому

британские компании и банки ищут их по всему миру. В британской полиции в настоящее время нет ни одной должностной позиции аналитика и специалиста по данным. Это положение планируется в кратчайшее время исправить.

Если совместить три компонента: создание мощных, доступных вплоть до низового уровня, баз и хранилищ данных; укомплектованность полиции аналитиками данных и специалистами по данным; повышение уровня компьютерной грамотности полицейских, вплоть до низового уровня, британская полиция может осуществить революцию данных. Эта революция позволит:

— все шире и с лучшими результатами переходить от предотвращения к профилактике преступлений. В Соединенных Штатах уже появился соответствующий термин — «предикативная полицейская деятельность»;

— использовать информацию не только из полицейских баз, но и из других государственных и частных баз, которые позволяют опережающим образом выявлять лиц и группы, уязвимые для преступников;

— заранее распознавать подозрительные модели деятельности и следы как готовящихся, так и уже совершенных преступлений. Наибольший эффект здесь может дать совмещение аналитики электронных платежей с видеоаналитикой и аналитикой совершаемых покупок;

— перевести дискуссии относительно уровня криминализации и уязвимости различных сфер деятельности, видов торговли и сегментов рынка с общетеоретического, экспертного анализа на язык документированной статистики. Выяснение тенденций, куда криминал направляет свои основные усилия, позволит британской полиции с опережением реагировать на изменение обстановки;

— наряду с повышением уровня раскрываемости преступлений и все бóльшим переносом работы с расследования на профилактику и предупреждение криминальных действий усилить контроль общества над полицией. В последние годы в Парламенте Великобритании неоднократно поднимался вопрос о том, что полиция отказывается открывать уголовные дела, связанные с высокими технологиями гораздо чаще, чем в отношении других видов преступлений. Использование данных и цифровых доказательств позволит и эту тему перевести из разряда экспертных дискуссий на уровень количественного анализа. Со временем контролирующие органы как внутри полиции, так и вне ее смогут в автоматизированном режиме выявлять все случаи необоснованного отказа в возбуждении уголовных дел, связанных с использованием высоких технологий.

Лондонская, манчестерская, ливерпульская полиция, полицейские силы Глазго, Эдинбурга и Белфаста уже начали применять пробные формы предикативной полицейской деятельности. В ситуации, когда в самой полиции нет специалистов необходимого уровня по направлению аналитики данных, выход был найден в тесном сотрудничестве с лучшими британскими университетами. Во взаимодействии с университетскими исследовательскими группами полиции этих городов сумели выйти на достаточно высокий уровень прогнозирования риска традиционных преступлений, например таких, как кража со взломом, по отдельным районам городов, вплоть до кварталов, а иногда и домов. После того, как на основе данных предикативного анализа полицейские городские структуры изменили графики и распределение патрульных экипажей, удалось в течение 2015—2016 гг. добиться снижения преступности, эквивалентного снижению традиционной преступности, связанной с кражами со взломом суммарно за предыдущие семь лет. Эти результаты произвели огромное впечатление как на полицейские силы, так и на население и бизнес. Полицейские перестали бояться высоких технологий, а бизнес стал охотнее жертвовать средства на повышение технического уровня полиции.

Это только первые шаги. Планируется сделать гораздо больше, чтобы в полной мере реализовать потенциал данных и аналитику данных в борьбе и профилактике преступности. При наличии надлежащих гарантий в отношении личной информации необходимо помочь полицейским силам использовать данные так же легко, как сегодня британские интернет-магазины используют данные покупателей для таргетированной работы с клиентами. Вот почему руководство британской полицией:

— неуклонно выполняет Национальную программу развития баз данных правоохранительных органов. В рамках программы создается единая платформа, позволяющая одновременно централизовать данные, получаемые из национальной базы данных полиции, национальной базы компьютерной безопасности, национальной базы распознавания номеров и иных национальных и региональных баз с возможностью обращения к этой базе всех полицейских подразделений и команд вплоть до патрульных экипажей. Когда платформа заработает на полную мощность, все британские полицейские смогут получать необходимую информацию в полном объеме в режиме онлайн в удобном и доступном для практического использования виде. Это не будет базой данных на уровне центрального аппарата министерства, это не будет базой данных лондонской полиции, это будет база данных каждого полицейского Великобритании;

— работает с Национальным советом начальников полицейских подразделений. Эта работа имеет своей главной целью обеспечить защиту населения и бизнеса от преступников, использующих высокие технологии не только для осуществления коммуникаций, но и для совершения преступных актов. В этих рамках станут более открытыми тендеры и конкурсы на поставку полиции самых эффективных решений;

— укрепляет связи с британскими и международными компаниями в сфере информационных технологий, ориентированными на удовлетворение нужд полиции. В этих рамках завершается работа по созданию единого стандарта технических и программных требований к информационно-коммуникационным компонентам, используемым полицией. Создание подобного стандарта позволит британской полиции в рамках политики единой платформы расширить круг поставщиков и обеспечить большую эффективность при меньших затратах;

— уделяет особое внимание опережающему созданию базы и аналитики данных, связанных с миграцией и предоставлением убежища. В настоящее время основной упор в этой работе делается на обеспечение эффективной оперативной связи с пограничными службами и миграционными бюро. В Великобритании создается единая база лиц, пересекающих границы Великобритании. Соответственно, эта база будет включать профили различного информационного объема в зависимости от продолжительности и целей пребывания иностранцев в Великобритании. Специальный раздел этой базы, создаваемый в первую очередь, касается нелегальных мигрантов. По каждому выявленному случаю будет собираться и храниться в базе максимально возможная информация. Есть основания полагать, что это позволит достаточно быстро выявить конкретные преступные группы, обеспечивающие нелегальную миграцию в Великобританию, и пресечь их деятельность. Именно это является наиболее эффективным подходом борьбы с нелегальной миграцией.

Использование существующих технологий и сканирование перспективных технологий, способствующих предотвращению преступлений. МВД Великобритании активно сотрудничает с правоохранительными органами и бизнесом в целях наиболее эффективного использования существующих технологий для предупреждения и борьбы с преступностью. Основными направлениями работы являются:

— технологии цифровой разведки для предотвращения преступлений. Цифровые источники играют все более важную роль в любом полицейском расследовании. Особо большие возможности предоставляет полицейским разведка по открытым источникам, в первую очередь по социальным сетям и приложениям. В условиях снижения возраста преступности, в том числе повседневной, уличной, практи-

чески весь криминал активно пользуется техническими устройствами. Извлечение данных из захваченных в ходе расследований ноутбуков или смартфонов позволяет получить результаты, на которые раньше, в доцифровом мире, у полицейских уходили недели упорной работы. Начиная с 2017 г. Министерство внутренних дел приступает к реализации программы «Цифровые расследования и разведка». Эта программа наряду с усилиями по созданию единой платформы поощряет овладение полицейскими методами разведки по открытым источникам и оснащения их простым, но эффективным «софтом»;

— мобильные технологии. Министерство создает в сотрудничестве с британским бизнесом единую систему связи для аварийных служб, включая полицию, пожарно-спасательную службу и скорую медицинскую помощь. Также эта система будет подключена к отдельным бизнес-структурам и общественным организациям. В 2018 г. в Великобритании будет создана единая сеть аварийных служб. Она обеспечит надежные услуги голосовой, текстовой и широкополосной видеосвязи, включая передачу данных. Система, располагающая мощнейшими центрами обработки данных, будет выведена на смартфоны, а также специальные устройства, прикрепленные к амуниции работников аварийных служб. Работники аварийных служб, находящиеся на переднем крае, в какой бы критической ситуации они ни оказались, смогут не только поддерживать связь, но и оперативно получать необходимую помощь;

— технологии цифрового видео. Британская полиция видит три основных направления использования цифрового видео в своей деятельности: во-первых, это видеоматериалы с места преступления; во-вторых, это канал взаимодействия с общественностью; в-третьих, это гигантский, пополняемый в онлайн-режиме видеоархив с камер наблюдения в британских городах и на транспортных магистралях. Впервые в истории у британской полиции есть в распоряжении программно-аппаратные средства, позволяющие в онлайн-режиме работать с потоковым многоканальным видео. По сути, речь идет о том, что впервые у полиции появляется возможность предикативно анализировать намерения потенциальных преступников.

Перспективные направления. В МВД Великобритании создан Центр перспективных прикладных наук и технологий (CAST). Его задачей является работа с бизнесом и наукой по выявлению новых технологий и при необходимости их финансовая и иная поддержка. Особое внимание Центр уделяет не международным и ведущим британским компаниям — поставщикам МВД, а исследовательским командам в британских университетах, стартапам и т. п. Центр не только внимательно изучает их разработки, но и облегчает доступ

лучшим из них на тендеры, проводимые Министерством внутренних дел.

В рамках работы Центра наряду с традиционными направлениями особое внимание уделяется таким перспективным технологиям, как:

— *3D- и 4D-печать*. Трехмерная печать позволяет создавать объекты при помощи послойного нанесения материала в определенной форме. 4D-печать представляет собой 3D-печать, чья форма программируемо изменяется с течением времени. Первое оборудование для 4D-печати уже создано в британских университетах. Данная технология интересна для Центра с позиций возможности использования 3D- и 4D-печати преступниками. Если пластиковые пушки в настоящее время ненадежны и представляют большую угрозу для стрелка, чем для жертвы, то стремительно развивающаяся 3D-металлическая печать позволяет преступникам оснащать себя стрелковым оружием дома с низкими затратами и высокими качеством. Благодаря тому, что удалось своевременно распознать эту угрозу, в настоящее время в Великобритании компании, производящие 3D-принтеры для металлической печати получают специальную разрешительную лицензию, которая предусматривает не только предоставление МВД сведений обо всех покупателях подобных устройств, но и установку внутрь устройств вшитых распознавателей локации. Также удалось выявить такие угрозы, как использование 3D-печати для производства различных устройств, используемых для контрабанды наркотиков, произведений искусства и т. п.;

— *дроны*. Нынешние разработки в области робототехники позволяют массово производить летающие роботы, несущие полезную нагрузку до 25 кг со временем полета более двух часов и скоростью до 400 км/ч по цене 200—300 ф. ст. Очевидно, что подобные дроны, используемые в настоящее время в основном государственными службами, в ближайшие год-два станут оснащением преступников. Центром совместно с лабораториями в Саутгемптонском и Бристольском университетах удалось создать устройство, которое позволяет распознавать на высоте до 1,5 км характер груза, размещенного на дроне. Устройство позволят идентифицировать основные виды взрывчатки, наркотиков и химических реагентов. Эта революционная разработка позволит сбивать или сажать путем перехвата управления подобные преступные дроны;

— *биткойн и блокчейн-технологии*. Британское МВД четко разделяет анонимные виртуальные криптовалюты, использование которых запрещено, с технологиями блокчейна. Если анонимные виртуальные валюты являются все более важным платежным средством для различного рода незаконных транзакций (от оплаты убийств, наркотиков и т. п. до вывода за рубеж коррупционных и прочих нелегальных

денег), то технологии блокчейна осуществляют революцию в финансах. Великобритания вместе с США является лидером использования блокчейн-технологий в финансовом секторе. Для того чтобы разобраться во всех аспектах блокчейн-технологий, Министерство внутренних дел ассигновало Центру совместно с Институтом Алана Тьюринга по 10 млн ф. ст. ежегодно вплоть до 2020 г. на блокчейн-исследования;

— *всеобщая взаимосвязь*. В настоящее время мир движется к сплошной связанной среде и инфраструктуре. К 2020 г. в мире будет около 20 млрд связанных между собой сетевых устройств. Британское МВД понимает, что глобальный связанный мир полностью меняет требования к работе правоохранительных органов. В полностью связанном мире криминал, не ограниченный законодательством, будет действовать глобально, поверх государственных границ. В то же время правоохранительные органы в своих действиях ограничены государственной юрисдикцией. Если эта проблема до 2020 г. не будет разрешена, то преступники получат огромное, а возможно, решающее преимущество. Несмотря на надежды руководителей отдельных крупных государств на эффективное закрытие собственного информационного пространства, это технически невозможно на программно-аппаратном уровне. Кроме того, любые подобные попытки приведут к отрыву государств от мировой экономики и глобальной технологической гонки и приведут их к стремительной деградации;

— *цифровое шифрование*. Цифровое шифрование амбивалентно. С одной стороны, оно создает возможности для общественности, граждан и бизнеса защитить свою информацию не только от преступников, но и от несанкционированного доступа к ней правительственных структур. С другой стороны, широкое распространение шифрования создает большие трудности для полицейских органов. Начиная с 2013 г. многие британские граждане стали использовать шифрованную электронную почту, мессенджеры и т. п. Это создает значительные затруднения правоохранительным органам. Поэтому предполагается регламентировать возможности шифрования гражданами, а также специально предусмотреть обязанность для производителей шифрованных коммуникаторов предоставлять соответствующие ключи правоохранительным органам.

§ 2. Искусственный интеллект и большие данные для предупреждения преступлений

Лидером внедрения искусственного интеллекта в процесс борьбы с преступностью является ФБР США. Основные работы в этом направлении ведутся в Информационном центре ФБР (NCIC). Это ме-

табаза, включающая на начало 2017 г. 21 базу данных, содержащих досье на 12 млн активных индивидуальных преступников и членов преступных организаций. В среднем NCIC отвечает на 14 млн запросов в день. Помимо ФБР NCIC обслуживает более 90 тыс. точек доступа в органах уголовного правосудия, а также судах, прокуратуре, системе исправительных учреждений и т. п.

Информационный центр ФБР находится в разгаре модернизации, известной как проект N3G. В рамках проекта в систему включаются принципиально новые блоки обработки и анализа информации, базирующиеся на интеллектуальном анализе больших данных. В 2017 г. началось сооружение и оснащение здания нового Центра данных и вычислений взамен действующего.

Новый Центр будет запущен в рамках проекта N4G. По площади он будет в 12 раз превосходить действующий в настоящее время Центр в Бриджпорте (штат Коннектикут) и иметь более чем в 50 раз бóльшую емкость и мощность хранения и обработки данных. Предусматривается, что Центр будет подключен к национальной сети суперкомпьютеров АНБ и Министерства энергетики. Программно-аппаратная архитектура Центра проектируется вокруг программно-аппаратных комплексов искусственного интеллекта.

Работы ведутся совместно с Лабораторией искусственного интеллекта корпорации Google. Выработано инженерное определение искусственного интеллекта. Именно оно будет положено в разработку концепции архитектуры и перечня программных решений для N4G.

Особое внимание ФБР уделяет скачкообразному увеличению *быстродействия компьютеров*. Так, выигрыш компьютера у человека в го (логическая игра) был осуществлен не просто компьютером Google, а программно-аппаратным комплексом, где за программу отвечали алгоритмисты Google, а «железо» сделала канадская компания, недавно купленная Google — Google DeepMind. DeepMind — это единственная сегодня компания в мире, которой удалось создать действующий квазиквантовый компьютер (квази — потому что значительная часть вычислений осуществляется в рамках традиционного кремниевого электромеханического компьютера, и лишь некоторые выполняет квантовый компонент). Но даже в таком виде обеспечивается на порядки более высокая скорость, чем у современных кремниевых суперкомпьютеров. Чем выше скорость, тем проще осуществлять глубокое обучение методом проб и ошибок.

Основные направления применения искусственного интеллекта в структуре ФБР и полиции США в 2017—2020 гг. Двусторонние и многосторонние встречи, открытые конференции и совещания за закрытыми дверями позволили определить основные направления использования искусственного интеллекта и его элементов в работе ФБР и

полиции штатов. Эти направления нашли отражение в концепции N4G. В число основных направлений включаются следующие.

1. Использование в аналитико-ситуационных центрах в офисах ФБР на местах и аналогичных офисах полиции штатов программно-аппаратной среды с единой интегральной обработкой файлов различной размерности и формой представления, включая текстовые, табличные, аудио-, видеофайлы, сигналы от датчиков, банковские транзакции, показания локации и т. п.

В 2017 г. в пяти полицейских управлениях на уровне штатов и в двух отделах ФБР запущены подобные пилотные ситуационные центры.

С 2015 г. Центр ФБР совместно с MTI и Google ведет работу по созданию *рекуррентной базы данных*. Принципиально от ныне существующих баз данных ее отличают три обстоятельства. Не человек, а машина будет принимать решение о появлении того или иного профиля в базе данных. Проще говоря, предусматривается система, в корне отличающаяся от ныне принятого порядка. Сейчас соответствующие руководители полиции, агенты ФБР принимают решения о заведении файлов на того или иного человека. Как показывает практика, эти решения часто бывают ошибочны и субъективны. В новой системе предполагается обеспечивать нефильтрованными потоками информации. Фильтровать, а соответственно, определять необходимость заведения профилей будет сама система. В систему встраивается модуль глубокообучаемых нейронных сетей. Данный модуль будет отвечать за своевременное исключение профилей и параметров лиц, которые по критериям базы попали в нее, но в течение определенного времени не вызвали интереса со стороны ФБР или полиции штатов. Наконец, данная система в отличие от ныне применяемых будет способна взаимодействовать с конечными пользователями на естественном языке и с использованием визуальных средств.

2. Как уже отмечалось, одним из наиболее подверженных угрозам с точки зрения динамики организованной преступности секторов экономической жизни являются небанковские платежные системы. По согласованию с наиболее динамичными платежными системами Stripe и Wise ФБР организовало ГЧП по созданию и эксплуатации платформы по обнаружению мошенничеств и взломов платежных систем. Данная система будет открыта для всех лицензированных платежных систем. Предусматривается, что они будут выделять на содержание системы ежегодный взнос в зависимости от объема транзакций и уровня сертификата информационной защиты, присвоенного платежной системе. Производителем системы в результате тендера выбрана компания Palantir.

3. С использованием платформы контекстного интеллекта Nigel предусматривается создать безбумажный офис агента ФБР или полицейского участка. Система Nigel в отличие от других способна не только к семантическому анализу (распознаванию объектов по онтологиям; онтологии могут быть различны — свойства, отношения, функции, человек, юридическое лицо, предмет и т. п.), но и к контекстному распознаванию ситуации. Ситуации могут быть одинаковы по онтологиям, но различными по смыслу. Например, в двух ситуациях участвуют одни и те же персонажи — женщина, мужчина и ребенок. Контексты ситуаций могут быть различны. В одном случае это может быть счастливая семья; в другом — бывшие супруги, делящие ребенка. Сейчас ни одна система, кроме Nigel, не способна распознавать ситуацию. В результате система будет давать экспертные оветы правоохранителям, привязанные к уникальной конкретной обстановке.

4. Начиная с 2017 г. ФБР совместно с компанией ForAllSecure и Университетом штата Пенсильвания преступило к разработке системы искусственного интеллекта Mayhem — первой в мире системы искусственного интеллекта, основными функциями которой являются распознавание индивидуального почерка хакеров и хакерских группировок, а также обнаружение атак и активного тестирования и преследование хакеров вплоть до установления их локации.

ФБР и исследователям Пенсильванского университета удалось установить, что методы комбинаторики позволяют системам искусственного интеллекта распознавать в доли секунды некоторые особенности вредоносного «софта», а также архитектуры атак, которые укрываются из-за недостатка времени от высококвалифицированного персонала служб информационной безопасности.

Большие данные против криминала. Огромные массивы разнообразной информации, например, информация с форумов и социальных сетей, видеозаписи, текстовые документы, лог-файлы (англ.: log file — файл регистрации) или, например, данные о трафике и соединениях абонентов, содержатся в различных источниках, нередко за пределами организации. В результате правоохранительные структуры могут иметь доступ к огромному объему данных из внутренних и внешних источников и не иметь необходимых инструментов, чтобы осуществить их совместную обработку, выявив определенные взаимосвязи и сделать на их основе значимые выводы. Технологии больших данных позволяют решить эту проблему, связав воедино разнородные данные.

Кроме того, обрабатываемая с использованием указанной технологии информация обновляется быстро (потоковые данные), напри-

мер пассажиропоток в аэропортах и на вокзалах, при этом необходимо принимать решения на основании их оперативного анализа.

Опыт сотрудничества компании IBM с правоохранительными органами свидетельствует о том, что требуются: во-первых, консолидация разрозненных источников информации в единое хранилище данных; во-вторых, применение специального программного обеспечения, позволяющего выявлять полезную информацию из разрозненных и неполных документированных данных, а также из несвязанных событий; в-третьих, использование специализированных, программно-аппаратных решений, максимально ускоряющих работу и принятие решений при обработке огромных объемов данных структурированной и неструктурированной информации.

С этой целью в Нью-Йорке в 2007 г. было принято решение о создании централизованного операционного центра общественной безопасности. Было интегрировано более 100 разрозненных источников данных. Все потоки информации от патрульных машин, тысяч камер видеонаблюдения, звонки от свидетелей в виде неструктурированных данных поступают на корпоративную шину данных и преобразуются в универсальный формат. Затем аналитические инструменты ассоциируют информацию, помещая ее в определенный контекст, и распределяют ее согласно запросам пользователей. Аналитическая система ассоциирования распознает не только структуру, но и значение информации, включая взаимоотношения между различными частями. Создание единого хранилища позволило снизить преступность в городе на 27%.

Был реализован также сервис поиска полезных данных из плохо документированной информации: жалоб граждан, отчетов полиции, записей на номер 911, протоколов арестов и др. Все эти данные изобилуют неточностями, сокращениями, аббревиатурами, специальными терминами и т. п., и выявление нужных сведений и взаимосвязей при помощи традиционного контекстного поиска в них крайне затруднено.

В результате удалось достичь общего повышения эффективности работы. Применение инструментария поиска и анализа позволило сформировать описание событий, классифицировать их (при этом поиск осуществляется по неструктурированной информации, содержащей порой неточные описания).

В целом это позволяет создать простые, унифицированные представления для каждого аспекта работы полиции, включая планирование, отчетность и совместную работу.

Ключевыми элементами работы операционного центра полиции Нью-Йорка являются пространственно-временная модель города и

поведенческие модели, которые используются для связывания наиболее вероятных сценариев преступного поведения. Центр по раскрытию преступлений реального времени (RTCC) использует ситуативный подход к большим данным, который требует особых навыков для составления запросов и интерпретации извлекаемых знаний. В результате каждое обращение к большим данным является уникальным поиском, в отличие от стандартных систем анализа информации в транзакционных и других системах управления реляционными базами данных с их фиксированными запросами и типовыми задачами.

Свою эффективность доказала система Blue CRUSH (англ.: Crime Reduction Utilizing Statistical History — снижение преступности на основе статистических данных), разработанная компанией IBM, которая поставляет полицейским подготовленные на основе имеющейся статистики совершения преступлений сведения о зонах потенциальной угрозы совершения преступления с указанием места (в пределах нескольких кварталов) и времени (в пределах нескольких часов конкретного дня недели). Подобного рода профилактическое прогнозирование привело к снижению уровня преступности в Мемфисе (штат Теннесси) на 31%, из которых 15% приходится на тяжкие преступления.

Благодаря расширенному использованию информационных технологий в борьбе с преступностью и с чрезвычайными обстоятельствами, стало возможным:

— реализовать автоматический анализ видеоинформации для предотвращения преступлений;

— ускорить расследование преступлений в 10—30 раз;

— использовать автоматизированные предсказания, поиск ассоциативных связей и техники кластеризации данных для ускорения принятия решений;

— автоматизировать процесс построения регламентов ответа на чрезвычайные ситуации;

— обеспечить сопровождение событий и отображение местонахождения сил и средств в реальном времени.

В 2001 г. IBM приобрела британскую компанию i2 Group, которая разрабатывала аналитические средства для правоохранительных органов, спецслужб, военной разведки и специалистов по борьбе с «фродом» (англ.: fraud — мошенничество в сфере IT).

Один из продуктов, основанных на i2, разработан специально для полиции. Он позволяет быстро получить доступ к информации, накопленной правоохранительными органами, и проявить в ней скрытые связи между людьми, местами, автомобилями, мобильными телефонами и тому подобными объектами.

В канадском Ванкувере полиция внедрила систему анализа данных, основанную на разработках IBM и географической информационной системе компании ESRI. Система не только выявляла тенденции, но и предсказывала вероятное время и место совершения преступлений. С 2007 до 2011 г. количество преступлений, связанных с собственностью, сократилось на 24%, а насильственная преступность — на 9%.

Похожие результаты сообщают полицейские департаменты Лас-Вегаса, Мемфиса и других городов, где экспериментируют с программами для анализа данных.

В полиции Лос-Анджелеса компьютерный алгоритм занимается тем, что обычно называют проактивной правоохраной. Используя отчеты о преступлениях за годы и десятилетия, алгоритм определяет районы, где вероятность совершения правонарушений является наибольшей. Он отмечает такие участки на карте города небольшими красными квадратами, и эти данные тут же передаются в патрульные машины.

Система прогнозирования преступлений (разработана в лос-анджелесском кампусе Калифорнийского университета (UCLA)) теперь стоит на балансе десятков полицейских подразделений.

В 2014 г. программное обеспечение PredPol применялось в семи территориальных подразделениях полиции Лос-Анджелеса. Их патрули оснащены электронными картами с десятками мигающих красных квадратов, которые указывают места возможной противоправной деятельности. Полиция Лос-Анджелеса сосредоточила силы на предупреждении краж имущества из домов и машин, а также угонов — видах преступлений, составляющих более половины всех преступлений, регистрируемых в городе.

Десятки других населенных пунктов по всем США и за их пределами используют программное обеспечение PredPol для прогнозирования других преступлений, включая активность ОПГ, наркоторговлю и незаконное применение огнестрельного оружия. Полиция Атланты применяет PredPol для прогнозирования грабежей и разбоев. В Сиэтле он используется для прогнозирования вооруженного насилия. В Кенте (Англия) PredPol применялся для предсказания наркопреступлений и грабежей. Полиция Кента была еще более изобретательной: не только отправляла своих сотрудников патрулировать опасные районы, но также прибегала к помощи местных волонтеров-дружинников и работников реабилитационных клиник для наркоманов.

Система прогнозирования в режиме реального времени анализирует новые отчеты о преступлениях в этих городах, и красный квадрат, предсказывающий место совершения правонарушения, может сдвинуться в любой момент. Хотя патрульные из подразделений, использующих PredPol, обязаны находиться определенное количество времени в каждом из тех красных квадратов, они не просто слепо следуют командам системы. Патрульный вправе принимать решения самостоятельно, исходя из обстановки, а не только подчиняться алгоритмам.

Использование больших объемов данных и обработка с помощью математических моделей значительно превосходят по конечному результату банальное определение горячих точек на карте в ручном или даже автоматизированном режиме. Специальные испытания, проводившиеся почти два года в трех территориальных подразделениях лос-анджелесской полиции, установили, что PredPol верно предугадывает в два раза больше мест преступлений, чем позволяют лучшее из существующих методик.

Специальное программное обеспечение применяется полицией Чикаго. Оно с высокой вероятностью предсказывает не только имена будущих убийц, но и тех, кто станет жертвами, — в американской преступной среде эти категории людей плотно пересекаются.

Программа, разработанная при участии ученых из Иллинойского технологического университета (США) (разработчик — профессор М. Веркик), позволила полиции Чикаго определить список лиц, находящихся в группе риска совершения убийств. Узнав их имена, полицейские ведут с ними профилактическую работу, предположительно позволяющую снизить вероятность посягательств на жизнь других людей.

В основе работы программы лежит отбор по десяти основным признакам. Среди них есть ряд цифр по истории приводов того или иного лица в полицию. Среди прочего алгоритм учитывает, были ли у человека аресты за незаконное ношение огнестрельного оружия или за участие в структурах организованной преступности. Алгоритм ищет людей, которые соответствуют всем или хотя бы нескольким критериям отбора. Те, кто набирает больше всего пересечений по списку критериев, вносятся в группу максимального риска.

По заявлениям полиции, новый алгоритм является довольно эффективным. Из 2,7 млн жителей Чикаго он отобрал лишь 1400 человек, имеющих чрезвычайно высокую вероятность убить или быть убитым.

Более 70% членов данного списка были застрелены в течение 2016 г. Каждый четвертый стрелок также входил в список Департамента полиции Чикаго. Согласно данным правоохранителей 117 из 140 человек, арестованных во время общегородского рейда против

банд, также присутствовали в вышеупомянутом перечне и составляли «группу риска».

Полицейские применяют новый метод не только для своевременного совершения арестов. Власти города видят в алгоритме эффективное средство «персональных уведомлений», в которых работники социальной сферы и общественные лидеры агитируют членов — лидеров «Списка стратегических субъектов» изменить образ жизни и навсегда покинуть криминальный мир.

Полиция города Дарема на севере Англии запустила в 2017 г. компьютерную программу, которая при помощи алгоритма искусственного интеллекта должна помочь полицейским определить, кого следует содержать под стражей, а кого можно отпустить. Алгоритм классифицирует задержанных по степени риска — с какой вероятностью они могут вновь совершить преступление.

Программа Harm Assessment Risk Tool (Hart) «изучала» данные полиции Дарема об арестах за пять лет, между 2008 и 2012 гг. Затем система была протестирована даремской полицией в 2013 г., после чего в течение двух лет изучались результаты этого тестирования — полицейские отслеживали, вернулись ли освобожденные к преступной жизни или нет. Как выяснилось, алгоритм мог предсказать, что задержанный не представляет опасности, в 98% случаев. А находящихся в группе «высокого риска» компьютер правильно выявлял в 88% случаев.

Это отражает настройки алгоритма искусственного интеллекта — он запрограммирован «осторожничать» и классифицировать задержанных людей чаще в группы среднего или высокого риска, чтобы не выпускать на свободу тех, кто может снова совершить преступление.

В ходе испытаний программы полицейские следили за выводами программы Hart, но вердикт алгоритма не влиял на принятие решения об аресте.

Подозреваемые, ранее не совершавшие преступлений, с меньшей вероятностью будут записаны алгоритмом искусственного интеллекта в категорию высокого риска. Однако если они арестованы по подозрению в серьезном преступлении, как, например, убийство, то это отразится на оценке программы.

Программа может быть хорошим помощником во многих случаях: когда полиции следует решить, держать ли задержанного еще несколько часов; следует ли отпустить его под залог до того, как ему будут предъявлены официальные обвинения, и стоит ли держать его под арестом после предъявления обвинений.

В ходе нового эксперимента полицейские будут использовать систему при рассмотрении лишь ряда дел, выбранных случайным путем.

Любой вывод алгоритма носит лишь рекомендательный характер и ни в коем случае не отбирает у полиции прерогативу принимать окончательное решение о судьбе задержанного. Алгоритм должен сохранять все данные о том, как программа пришла к определенному выводу.

Кроме того, британская полиция с 2014 г. проверяет компьютерную систему, которая может собрать воедино то, что могло произойти на месте преступления. Идея состоит в том, что система, называемая VALCRI (Visual Analytics for Sense-making in Criminal Intelligence Analysis), сможет в течение нескольких секунд выполнять кропотливую работу аналитика, освобождая время для того, чтобы сосредоточиться на деле, а также провоцируя новые направления расследования и возможные упущенные детали.

Основная работа VALCRI заключается в том, чтобы помочь генерировать правдоподобные идеи о том, как, когда и почему было совершено преступление, а также кто сделал это. Система сканирует миллионы полицейских записей, интервью, фотографий, видеороликов и многое другое, чтобы определить связи, которые имеют отношение к делу. Все это затем представлено на двух больших сенсорных экранах для взаимодействия с аналитиком.

Мидлсекский университет является одним из нескольких высших учебных заведений, которые в данный момент задействованы в разработке системы VALCRI.

VALCRI исследует личные дела преступников и разделяет паттерны их поведения на отдельные категории. По почерку преступника система практически мгновенно предложит следователям несколько наиболее подходящих кандидатур, которые были способны совершить данное преступление. Причем информация будет предлагаться сотрудникам полиции в интуитивно понятном и очень удобном графическом интерфейсе.

Вместо того чтобы разделять преступников по категориям преступлений, таким как квартирные кражи или взлом автомобилей, VALCRI запоминает и анализирует паттерны поведения преступника, в данном случае — склонность к кражам. Таким образом, VALCRI решает проблему слабого сотрудничества между полицейскими подразделениями, а также учит полицейских обращать внимание на ключевые детали преступления.

В ряде штатов США использование полицией методов и алгоритмов кластеризации и классификации технологии Text Mining (интеллектуальный анализ текста) для выделения криминально значимой информации совместно с технологией Visual Mining (визуальный анализ) в режиме реального времени обеспечивает возможность выполнения аналитической работы по профилактике и расследованию пре-

ступлений в автоматизированном режиме на качественно новом уровне. Эта возможность реализована в интеллектуальной системе криминального анализа в реальном времени RICAS (Real-time Intelligence Crime Analytics System), которая позволяет связать географическое пространство, время, лица и события в одном визуальном пространстве отображения.

В основу построения системы положены такие факторы:

— любая криминально значимая информация содержит данные о месте совершения преступного деяния, которые могут быть отражены либо в текстовом формате в виде адреса либо в географических координатах и времени совершения;

— любой субъект или объект преступления имеет привязку к географическим координатам в текстовом формате (адрес прописки, проживания, регистрация предприятия, места работы, регистрация транспортного средства, оружия и т. д.);

— криминальные события, субъекты и объекты могут иметь взаимосвязи, которые легче обнаружить путем анализа визуального отображения в едином пространстве представления (на одной карте). Например, если в месте совершения разбойного нападения проживают лица, ранее привлекавшиеся за аналогичные преступления, то существует большая вероятность совершения ими данного деяния;

— отображение в едином пространстве событий, растянутых во времени (происходящих в разное время), позволяет обнаружить скрытые закономерности визуально.

С учетом этих факторов в представляемой системе программно реализованы адаптированные алгоритмы технологий Data Mining, Text Mining и Visual Mining, Link Analyzes, которые обеспечивают выполнение следующих операций с потоками входных данных:

— кластеризация объектов по одному или нескольким признакам, имеющим общие пространственно-временные характеристики;

— создание временной ленты событий для определенного географического места (ретроспективный анализ криминальных событий, произошедших в заданный период времени в районе места исследуемого происшествия);

— группировка объектов и субъектов вокруг события;

— анализ связей лиц, объектов, событий.

RICAS — это интеллектуальная система криминального анализа данных, которая объединила в едином пространстве отображения основные и наиболее передовые методы и методики криминального анализа и аналитического поиска в реальном времени, что позволяет значительно повысить эффективность и результативность раскрытия преступлений по горячим следам и не раскрытых ранее преступлений, а также предотвращать готовящиеся преступления.

Аналитическая работа в системе выполняется в автоматизированном режиме: на первом этапе по поступившему в систему запросу с помощью разработанных алгоритмов аналитического поиска автоматически осуществляется поиск, результаты которого отображаются в текстовой форме и на географической карте; на втором этапе оператором в ручном режиме осуществляется визуальный анализ полученных данных и принимается окончательное решение либо системе задаются дополнительные уточняющие запросы.

Система позволяет оператору выполнять многие виды криминального анализа: криминальной обстановки, общего профиля, конкретного расследования, групповой преступности.

Используя все эти виды анализа интегрально, можно видеть картину целиком — предикативно и постфактум, т. е. систему событий, лиц, объектов, связанных причинно-следственными связями в пространстве и времени.

Поскольку система является надстройкой над существующими базами данных, она может как отображать явно указанные связи между лицами, так и строить визуальные связи между лицами, которые, на первый взгляд, между собой не связаны. Система использует несколько алгоритмов поиска связей. Первый алгоритм — рекурсивный поиск взаимосвязей фигурантов, участвовавших в разных событиях. Второй — визуальный поиск связей. В процессе вывода специальным образом структурированной информации в визуальную среду отображения становятся очевидными связи типа «место совершения — подельник — преступник», «преступление — подозреваемый — подельники».

Инструментарий системы базируется на математических моделях и методах интеллектуального семантического анализа, визуального темпорального анализа, анализа поведенческого профиля, анализа скрытых закономерностей.

Интеллектуальный семантический анализ включает в себя мощное ядро по работе с семантикой. Анализ неструктурированных данных происходит в режиме реального времени. Для унификации поисковых функций и построения поведенческого профиля используется алгоритм классификации или «тегирования», а также антиципационный алгоритм (схема предвосхищения — цель поиска известна заранее).

Семантическое ядро системы позволяет строить сложные поисковые запросы, включающие в себя всевозможные динамические и статические компоненты — ограничения по времени, методу совершения преступления, дислокации и т. д. Все функции выполняются мгновенно и позволяют максимально быстро визуализировать информацию и выполнять аналитическую работу.

Отображение хронологии произошедших событий и временное разграничение позволяют оперативно выявлять скрытые пространственно-временные закономерности между различными событиями. Это осуществляется с помощью *визуального темпорального анализа*.

Наиболее постоянным и точным с точки зрения психологии преступника является его поведенческий профиль. Он отображает многие параметры деятельности преступника — привычный способ совершения преступления, места совершения и прочие мелкие зависимости, которые в совокупности соответствуют одному профилю. На этом основывается *анализ поведенческого профиля*.

Наличие тех или иных поведенческих признаков с определенной долей вероятности может свидетельствовать о том, что данный субъект может быть причастен к событию. Из этого принципа формируется так называемый групповой поведенческий анализ. Безусловно, поведенческий профиль преступника никак не может существовать без влияния на других субъектов. Поэтому в криминальной практике часто заметны совпадения по тем или иным поведенческим параметрам у разных субъектов, когда-либо участвовавших в единых событиях. Анализ группового поведенческого профиля позволяет определять подельников, сообщников без явный связей между собой.

Анализ скрытых закономерностей основывается на том, что между лицами, каким-либо образом причастными к правонарушению, объективно существуют связи (родственные, по роду профессиональной деятельности, географические — по привязке к месту жительства, месту отбывания наказания и т. п.). Подобные связи существуют также между лицами и событиями, а также между различными событиями. Такие связи могут быть явными, опосредованными и скрытыми. Кроме того, группа преступлений, совершенных одним и тем же лицом, обязательно имеет определенные характерные общие черты, которые явно не зафиксированы. Выявление таких скрытых закономерностей с высокой долей вероятности всегда может идентифицировать связь между преступником и всеми совершенными им преступлениями. Безусловно, некоторые события могут «выбиваться» из общего потока из-за своей спонтанности или внешних факторов. Однако, исходя из предыдущего принципа, такие проявления можно нивелировать.

В RICAS поиск скрытых закономерностей осуществляется с базированием на интеллектуальном ядре обработки семантики. Семантический анализ является основополагающим, поскольку связи выражаются не всегда явно и их следует искать в контексте.

Система RICAS разрабатывалась с использованием современных, оптимизированных технологий в веб-пространстве и поддерживает мультиплатформность. Ее можно использовать на любых стационарных и мобильных устройствах при наличии защищенного канала связи; интерфейс системы не перегружает пользователя.

Самой известной компанией, специализирующейся на прогнозировании преступлений, является Palantir Technologies, вышедшая на коммерческий рынок из тени спецслужб.

Разработанное Palantir специализированные решения способны собрать воедино самую разную информацию (данные ДНК, записи систем видеонаблюдения и телефонных переговоров), отслеживать передвижения по номерным знакам арендованных машин и многое другое.

Механизм действия этого программного обеспечения заключается в анализе персональных данных и выявлении транзакций, которые всегда идут в тесной связке с паттернами, сопровождающими те или иные преступления. Иными словами, у спецслужб имеются внушительные массивы данных, среди которых сведения о финансовых сделках, отпечатки пальцев и образцы ДНК, планы зданий и топографические карты, данные радиоперехвата, «горячие» новости из СМИ, сообщения информаторов, информация из соцсетей и др.

Программное обеспечение Palantir уже помогло раскрыть преступную сеть, готовящую теракты в нескольких странах мира. Его также использовали в Афганистане для прогнозирования атак моджахедов. Кроме того, решение Palantir позволило обнаружить членов мексиканского наркокартеля, убивших сотрудника таможенной службы США, а также разрешить множество не таких громких, но не менее важных случаев, в том числе найти педофила в Нью-Йорке уже через час после нападения на ребенка, обнаружив его на видеозаписях с камер полицейского управления.

Департамент полиции Нью-Йорка совместно с Microsoft разработал Domain Awareness System (DAS) — систему, которая агрегирует и анализирует информацию об общественной безопасности из отчетов, камер наблюдения, наблюдений очевидцев и т. д. Затем эту информацию о потенциальных угрозах и криминальной активности в режиме реального времени получают следователи и аналитики департамента.

Похожим образом работает ShotSpotter — акустическая система наблюдения, которая фиксирует выстрелы из оружия и оповещает об этом полицию. Сенсоры ShotSpotter позволяют определить место, где произошел инцидент, с точностью до двух футов.

Но городская жизнь состоит из множества звуков, часть которых можно принять за выстрелы из оружия. Чтобы избежать таких ошибок, звуки, которые сенсоры определяют как выстрелы, отправляются экспертам. Если оказалось, что действительно произошел выстрел, то информация о том, где, когда и сколько выстрелов было совершено, отправляется полиции. Весь этот процесс — с момента, когда вы-

стрел был засечен, до отправки информации полиции — занимает около 40 секунд. Данная технология используется уже в 75 городах США.

Система помогает не только оперативно реагировать на происшествия, но и узнавать о них — жители некоторых районов часто не сообщают в полицию о преступлениях, очевидцами которых являются. Так, в Милуоки (штат Висконсин) только о 14% всех выстрелов, которые зафиксировал ShotSpotter, было сообщено в полицию.

Другой частью тренда в использовании новых технологий для повышения осведомленности является использование социальных медиа и, в частности, Twitter. Полиция все чаще полагается на эту социальную сеть и использует для коммуникации с жителями города. Например, во время беспорядков, устроенных спортивными болельщиками в Ванкувере (Канада), полиция использовала Twitter для того, чтобы быть в курсе ситуации, а после того, как беспорядки были устранены, Twitter и Facebook стали каналами, через которые свидетели могли сообщить полиции имеющуюся у них информацию.

Полиция Берлина рассматривает возможность установки программного обеспечения, которое сможет предсказывать преступления, почти как показано в научно-фантастическом фильме «Особое мнение». Даже проект носит такое же название «Precobs», как в фильме.

Разработанная немецкой фирмой программа предсказывает, где и когда с наибольшей вероятностью произойдет преступление.

Нужно сказать, что похожие программы уже несколько лет успешно работают в нескольких американских городах. Например, в 2011 г. Санта-Крус (штат Калифорния) первым в мире внедрил математическую модель расчета вероятности преступлений, которая каждый день составляет новый маршрут для патрульных машин, основываясь на статистике преступлений по улицам. Учитываются день недели, время суток, наличие/отсутствие трансляции футбольных матчей по телевидению и другие факторы.

Патрульные полицейские Санта-Круса каждый день получают новый маршрут для патрулирования с указанием 10 горячих точек маршрута. Вот как выглядит эта информация в интерфейсе Google Maps: для каждого квадрата размером 150 на 150 м указывается вероятность совершения преступления в 24-часовой период, распределение этой вероятности по двум видам преступления (автомобильные и домашние), время начала двух самых опасных часовых интервалов.

Немецкая программа Pre-Crime Observation System работает примерно по такому же принципу, вычисляя вероятность совершения

преступлений по тем или иным координатам с учетом прошлой статистики.

Полиция Амстердама поставила задачу разработать программный продукт, который мог бы автоматически систематизировать тысячи полицейских отчетов, отбирая те, что имеют отношение к торговле людьми. Система должна была не просто отбирать подозрительные случаи, а находить закономерности, устанавливать круг людей, возможно причастных к преступному бизнесу, т. е. обнаруживать и идентифицировать потенциальных подозреваемых.

Главной идеей было создание хорошей системы анализа и визуализации данных полицейских отчетов. В качестве такого средства как нельзя лучше подходит анализ формальных понятий. Этот метод был предложен в 80-х гг. прошлого века немецким математиком и философом Р. Вилле. Анализ формальных понятий позволяет визуализировать объектно-признаковые зависимости путем построения так называемых решеток формальных понятий, или решеток Галуа. Основная математическая идея заключается в возможности построения полной решетки по любому бинарному отношению и математическому описанию понятия в виде пары объекты — признаки. В данном случае объекты — это отчеты, а признаки — информация, содержащаяся в них, например ключевые слова, даты, упоминаемые люди.

В ходе работы специалисты проанализировали около 70 тыс. полицейских отчетов, составленных с 2008 г. В основном это были отчеты патрульных полицейских, проводивших осмотр автотранспорта или патрулировавших улицы Амстердама. Лишь примерно в тысяче случаев полицейским было известно, что речь действительно идет о лицах, имеющих отношение к торговле людьми.

Все индикаторы (их можно выявить в тексте автоматически) разделили на группы:

— статические признаки (национальность, проблемы с документами, крупная сумма наличных, женщины не разговаривают, документы женщин находятся у водителя, проститутки, насилие, следы насилия);

— изменяющиеся признаки (район «красных фонарей», дорогая машина, женщины в машине, торговля в машине, каникулы, регулярное посещение сомнительных клубов, регулярная доставка девушек в клуб);

— признаки социального окружения (человек был замечен с подозреваемым или известным преступником, сам был под подозрением).

Также индикаторы подразделялись на ранние и поздние, т. е. возможные и явные, сильные признаки, соответственно.

Выделенные признаки заносились в таблицу. Глядя на нее, можно было определить, сколько подозрительных признаков есть в том или ином отчете. Полицейские при составлении отчета перечислили такие индикаторы, как «дорогая машина», «проблемы с документами», район, где работают проститутки.

Отчет, содержащий слова-индикаторы, требовал более пристального внимания правоохранительных органов. Чтобы обнаружить и идентифицировать лиц, причастных к торговле людьми, полицейские анализировали формальные понятия.

Эта работа проходит в три этапа:

— из большого множества отчетов выделяются персоны, которые могли быть потенциально вовлечены в «трафикинг»;

— строится детальный профиль этих лиц, в котором отражены индикаторы и их изменение во времени;

— анализируются социальное окружение (социальная сеть) подозреваемых и эволюция этого окружения с течением времени.

Разработанный инструмент позволил полицейским в интерактивном режиме с помощью таблиц формальных понятий выделить ряд признаков и выявить потенциальных подозреваемых.

Далее с помощью разработанной системы было проанализировано и визуализировано в виде диаграммы социальное окружение человека. Программа показала, с какими людьми и при каких обстоятельствах имел дело подозреваемый. То есть, по сути, были очерчен круг лиц, возможно причастных к ОПГ.

Компания Fujitsu Laboratories Ltd совместно с Университетом электрокоммуникаций (Япония) разработала алгоритм для поимки преступника в городе. Алгоритм основан на теории игр, которая математически описывает технологию защиты и нападения как технологию для принятия решений. Раньше технологию было сложно применить в городских условиях, так как объем информации увеличивался с размером уличной сети города. Справиться с этой проблемой позволит *технология «сжатия сети»*.

Разработка планов безопасности общественных сооружений (вокзалов, аэропортов) исторически основывалась на интуиции и опыте, однако в последние годы стала очевидной необходимость обеспечения повышенной безопасности с помощью искусственного интеллекта (ИИ). Алгоритмы способны развернуть ресурсы безопасности в соответствии с движением людей и психологическими характеристиками преступников.

Лаборатория компьютерных наук и искусственного интеллекта Массачусетского технологического института создала алгоритм, который с помощью технологии глубокого обучения позволяет ИИ использовать шаблоны человеческого взаимодействия, чтобы предсказывать, что может произойти дальше. Исследователи загружали в программу видео с примерами социальных взаимодействий людей и тестировали ее, проверяя, насколько хорошо она «обучилась», чтобы быть в состоянии давать прогнозы.

Визуальные материалы для ИИ включали 600 часов видео с YouTube и телевизионных сериалов. В то же время такой выбор мог показаться сомнительным, так как в числе критериев были доступность и реализм.

Ученые представили компьютеру видео, где люди показаны за одну секунду до выполнения одного из следующих четырех действий: обниматься, целоваться, приветствовать жестами руки и пожать руку. Искусственный интеллект был в состоянии правильно угадать в 43% случаев по сравнению с людьми, которые угадывали в 71%.

Наделение ИИ способностью понимать визуальные действия, подобно тому как это делают люди, может стать предшественником разработки интеллектуальных камер безопасности, которые будут способны как можно раньше вызывать скорую или полицию.

Это не первая попытка прогнозирования ситуации с помощью видео, но на этот раз были достигнуты болел точные результаты. Причина заключается в том, что, во-первых, новый алгоритм отличается от предыдущих попыток видеопрогнозирования, в которых приоритетом была точность пиксельного представления. Он прогнозирует развитие ситуации, используя абстрактное представление, и фокусируется на важных признаках, при этом он самостоятельно обучается и использует так называемые визуальные представления, чтобы отличать визуальные сигналы, которые играют важную роль в социальных взаимодействиях, от тех, которые таковыми не являются. Это вполне естественно для человека, но является сложной задачей для ИИ.

Доктор Шимей Пан из Университета Мэриленда (США) и работающие с ней специалисты создали в 2017 г. нейронную сеть, которая с высокой точностью определяет, страдает ли тот или иной пользователь соцсети Facebook какой-либо зависимостью — алкогольной, табачной, наркотической.

Возможности такой диагностики система ИИ приобрела в процессе обучения — достигла упражнениями, которые исследователи разработали с помощью трех баз данных. Одна содержала 21 млн постов, написанных 100 тыс. пользователей, участвовавших в психологических тестах; другая — 5 млн лайков, оставленных 250 тыс. посетителей соцсети; третья база включала данные на более чем 13 тыс. пользователей, о которых было известно, что они страдают той или иной

зависимостью. Итог обучения: нейронная сеть доктора Шимей Пан выявляет наркоманов с точностью 84%, алкоголиков — с точностью 81%, а курильщиков правильно определяет в 86 случаях из 100. И это не предел — ИИ продолжает обучаться. И когда-нибудь достигнет 100%-ной эффективности.

Японское министерство, контролирующее таможню, в 2017 г. начало полевые испытания ИИ и дронов для борьбы с контрабандой, планируя полностью внедрить такую технологию в преддверии Олимпийских игр 2020 г.

В настоящее время таможенные инспекции в аэропортах и гаванях проводят визуальную проверку рентгеновских снимков для выявления контрабанды наркотиков и взрывчатых веществ. В дополнение к визуальным осмотрам Министерство финансов Японии планирует использовать ИИ. С его помощью будут проанализированы уже имеющиеся в базе данных изображения, чтобы помочь выявлять контрабанду в рентгеновских изображениях.

Также будут подвергнуты анализу данные таможен о въезде и выезде людей из Японии, об экспорте-импорте грузов, чтобы определить, когда высока вероятность провоза контрабанды.

Распространение авиакомпаний-лоукостеров привело к резкому увеличению числа прибытий авиалайнеров поздней ночью и ранним утром, особенно из Азии. Новая технология может помочь ускорить проведение проверок в аэропортах, даже если ими занимаются всего несколько таможенников.

Особая активность в работах по созданию ИИ наблюдается в КНР. Первая в Китае национальная лаборатория по разработке технологии «мозгоподобного» ИИ 13 мая 2017 г. открылась в городе Хэфэй, являющемся административным центром провинции Аньхой (Восточный Китай). Создание этой лаборатории было утверждено Государственным комитетом по делам развития и реформ КНР. Она базируется в Китайском научно-техническом университете и нацелена на развитие парадигмы «мозгоподобных» вычислений и их приложений.

Данный университет известен своей лидирующей ролью в разработке технологии квантовой связи, он размещает национальную лабораторию в сотрудничестве с ведущими китайскими научными учреждениями, включая Университет Фудань и Шэньянский институт автоматизации Академии наук Китая, а также оператора крупнейшего в Китае сервиса интернет-поиска — Baidu.

Ректор Китайского научно-технического университета, председатель национальной лаборатории Вань Лицзюнь сообщил информационному агентству Синьхуа, что возможность имитировать способности человеческого мозга по сортировке информации поможет создать

полную парадигму разработки технологии ИИ. Лаборатория будет проводить исследования по управлению машинным обучением, включая распознавание сообщений и использование визуальных нейросетей для решения задач.

В России также используют в предупреждении преступности и терроризма новейшие технологии, использующие ИИ и большие данные.

Например, основной автоматизированной информационно-поисковой системой (АИПС) ОВД на транспорте является программно-технический комплекс (ПТК) «Розыск-Магистраль». Этот комплекс начал внедряться в оперативно-служебную деятельность в 2000 г. Он предназначен для выполнения в автоматизированном режиме следующих функций:

— выявления в пассажиропотоке лиц, находящихся в розыске, а также лиц, представляющих оперативный интерес для правоохранительных органов, посредством автоматического сравнения баз данных по лицам, находящимся в федеральном и местном розыске, лиц, представляющих оперативный интерес, утраченных и похищенных документов и т. д. с транспортными базами данных;

— круглосуточного пополнения баз данных информацией, поступающей из ОАО «РЖД», его филиалов и структурных подразделений; предприятий авиатранспорта; ГИАЦ МВД России; информационных центров МВД, ГУВД, УВД, УВДТ; подчиненных линейных подразделений и других правоохранительных органов;

— предоставления возможности поиска по базам данных АИПС в различных режимах;

— выгрузки данных из информационных массивов АИПС и их передачи в вышестоящие подразделения для формирования общероссийского (межрегионального) информационного массива;

— осуществления по запросу пользователя аналитической обработки имеющейся в базах данных ПТК информации с целью выявления и раскрытия преступлений в сфере пассажирских перевозок;

— проведения аналитических разработок по регистрируемым преступлениям и делам оперативного учета;

— формирования статистической отчетности о результатах работы системы как по выявлению лиц, находящихся в розыске и представляющих оперативный интерес, так и по количеству и качеству выданной информации по запросам пользователей.

Помимо описанных выше функций в системе «Розыск-Магистраль» реализовано использование программных модулей — автоматизированных рабочих мест (АРМ), позволяющих выявлять и раскрывать преступления, совершенные в сфере пассажирских перевозок.

В основу работы аналитических модулей заложен принцип отраслевой интеграции информации. Для каждого направления работы (по линии уголовного розыска, борьбы с незаконным оборотом наркотиков, борьбы с организованной преступностью и др.) существует свой АРМ, позволяющий посредством специально разработанных алгоритмов извлекать из общего банка информацию и анализировать данные, необходимые для выявления и раскрытия конкретных видов преступлений.

Для информационной поддержки нарядов патрульно-постовой службы и оперативных сотрудников служат мобильные терминалы ПТК «Розыск-Магистраль». Эти терминалы представляют собой карманные персональные компьютеры и предназначены для оперативного доступа сотрудников правоохранительных органов к информации баз данных федерального и регионального уровней, таких как «Розыск лиц», «Паспорта», «Оружие», «Угон» и др.

Мобильные терминалы позволяют:

— выявлять лиц, находящихся в федеральном или местном розыске, представляющих интерес, использующих документы, числящиеся как утраченные или похищенные;

— выявлять автотранспорт, находящийся в розыске;

— осуществлять контроль над перевозками подакцизных товаров железнодорожным транспортом.

Мобильные терминалы системы «Розыск-Магистраль» работают с ежедневно обновляющейся локальной базой данных или могут осуществлять доступ к серверу баз данных в режиме реального времени по существующему каналу связи, в том числе и с применением веб-технологий.

Систему «Искусственный интеллект на границе», охраняющую российско-казахстанскую границу в пределах Челябинской области, с 2016 г. тестируют разработчики. Разработчиком системы «Искусственный интеллект на границе» является Объединенная приборостроительная корпорация.Несколько комплектов системы готовят под установку на дальневосточных, южных участках рубежей России.

Фиксацией нарушений занимаются беспилотники, инфракрасные датчики, сейсмосенсоры, радиолокационные устройства, а передаваемая ими информация обобщается компьютерной системой с интеллектуальной программой. Наработав базу данных, программа начинает прогнозировать опасности.

Стоит задача сухопутные участки государственной границы России оснастить интеллектуальной системой, способной автоматически собирать и анализировать информацию о нарушении рубежей страны. Благодаря этому пограничники будут в дистанционном режиме контролировать ситуацию на границе.

На морских направлениях продолжится наращивание возможностей системы автоматизированного технического контроля за надводной обстановкой.

На сухопутных участках границы устаревшие технические средства охраны границы будут планово заменены на современные образцы. При этом стратегической целью технической политики станет последовательный переход подразделений к дистанционному контролю за охраняемыми участками государственной границы с одновременным сокращением использования личного состава в их физической охране.

Речь идет о подвижных и стационарных комплексах технического наблюдения нового поколения со скрытым (практически невидимым) расположением на местности. Контролировать обстановку на удаленных и труднодоступных направлениях будут БПЛА.

Кроме того, российские программисты разработали систему, которая в целях контроля за оперативной ситуацией автоматически взаимодействует с различными техническими средствами охраны: видеокамерами, инфракрасными и сейсмическими датчиками, радиолокационными станциями и беспилотниками, фиксирующими факты нарушения. Она не только предназначена для сбора различной информации, но и содержит элементы ИИ. Это позволяет пограничникам произвести анализ и прогнозирование ситуации, выработать готовые предложения по охране границ, просчитать действия и маршрут нарушителей, а также меры, необходимые для пресечения действий злоумышленников, с оценкой возможных рисков. При этом учитываются реальные условия местности, статистика нарушений, погодные условия, расположение пограничных постов и нарядов и многие другие факторы.

Система полностью базируется на отечественных программных решениях, которые гарантируют защиту информационных ресурсов от утечек данных, хакерских атак, других посторонних вмешательств. Данные комплексы прошли положительную апробацию в Кабардино-Балкарии, Карачаево-Черкесии, Северной Осетии и Ингушетии.

§ 3. Использование искусственного интеллекта, больших данных и квантовой криптографии для предупреждения финансовых мошенничеств

Аналитическое подразделение Microsoft по борьбе с преступлениями в сфере высоких технологий Digital Crimes Unit (DCU) было создано в ноябре 2013 г.

Важным моментом здесь остается соблюдение прозрачности схемы получения данных через открытое ГЧП. У пользователей не должно оставаться сомнений относительно преследуемых целей и типов используемых сведений.

Большие данные выступают здесь в роли ультимативного инструмента расследования и предотвращения киберпреступлений. Внедряя очередную схему, злоумышленники повсюду оставляют цифровые следы. По отдельности эти малые изменения обычно игнорируются. Однако на уровне больших данных преступление с использованием сетевых технологий выглядит как характерный паттерн. Полностью скрыть его не удастся, как бы тщательно ни маскировались отдельные проявления.

Стало гораздо легче отследить нелегальные ключи активации программных продуктов. Раньше сами разработчики выявляли только украденные однопользовательские лицензии, когда их пыталось одновременно использовать несколько человек. Сейчас обмен данными позволяет увидеть, что корпоративный ключ одной из программ был украден или происходит проверка генератора ключей.

С помощью визуализации больших объемов совместных данных можно видеть необычные всплески активности на серверах регистрации, что может указывать на тестирование украденных или сгенерированных ключей. Без средств визуализации эти аномалии, скорее всего, оставались бы незамеченными.

Традиционными средствами веб-мониторинга противодействовать пиратству сегодня уже вряд ли возможно. В мире существует свыше 600 млн сайтов; с использованием больших данных выявление незаконных загрузок контрафактного программного обеспечения заметно упростилось.

Однако пиратство — далеко не единственное явление, с которым борются в DCU. Сегодня на технологиях анализа больших данных Microsoft создает целую инфраструктуру для предотвращения любой нелегальной сетевой активности.

Большинство сетевых атак и рассылок спама выполняются с зараженных компьютеров, формирующих ботнеты. Определение их состава и управляющих серверов — важная задача обеспечения глобальной информационной безопасности. В этом направлении работают отечественные компании, включая «Доктор Веб» и «Лабораторию Касперского».

Применяя технологии анализа больших данных, в Microsoft разрабатывают алгоритмы, упрощающие определение управляющих серверов и перехват контроля над ними. Также провайдеры предупреждаются о том, что компьютеры их абонентов заражены. Такое сотрудничество помогает узнать дополнительные детали о сетевой активности и вычислить дальнейшие шаги преступной группы.

Криминальные схемы постоянно меняются. Чтобы вовремя реагировать на них и отслеживать новые тенденции, сейчас важно разрабатывать универсальные аналитические инструменты, способные работать с любым набором больших данных.

Корпорация IBM объявила, что приспособила самообучающийся суперкомпьютер Watson, способный работать с информацией на естественном языке, для использования в сфере информационной безопасности.

Специалисты IBM и исследователи из восьми американских университетов планируют загрузить в самообучающуюся систему содержимое библиотеки X-Force, которая включает материалы, охватывающие два десятилетия исследований в сфере информационной безопасности, подробную информацию о 8 млн спамерских и фишинговых атак и описания более 100 тыс. уязвимостей.

На первых порах документы для Watson будут подбирать и размечать вручную, но затем машина станет справляться с этой задачей без помощи людей. На это в IBM и рассчитывают. Предполагается, что после завершения обучения Watson будет оперативно собирать и сопоставлять общедоступные сведения о новых угрозах, в том числе информационные бюллетени, статьи, отчеты компаний, видео, даже публикации в блогах. Он будет в курсе всего, что происходит, и за счет этого сможет самостоятельно опознавать проблемы и предлагать рекомендации по их решению.

В IBM исходят из предположения, что поток информации об угрозах если еще не превысил человеческие возможности, то непременно это сделает. Национальная база данных по уязвимостям уже сейчас содержит более 75 тыс. записей и быстро растет. Каждый год публикуется около 10 тыс. исследовательских работ, так или иначе связанных с информационной безопасностью, и более 60 тыс. постов в блогах по той же теме. Watson способен проанализировать их все. Люди — нет.

Умение Watson работать с неструктурированной информацией и сведениями, изложенными на естественном языке, сочетается с более традиционными методами анализа больших данных. Система замечает аномалии, указывающие на атаки, выявляет скрытые закономерности и прослеживает связи между различными документами. Кроме того, в Watson встроены мощные средства визуализации.

Новая система борьбы с компьютерным мошенничеством на основе больших данных была разработана в компании Visa. В отличие от предшественников она учитывает до 500 особенностей каждой транзакции и анализирует происходящее с точностью до отдельных

банкоматов. За год система останавливает мошеннические платежи на сумму примерно 2 млрд долл. США в год.

В том же направлении движутся и другие компании, благополучие которых зависит от эффективности системы выявления мошеннических транзакций. Кто-то подобно Visa модернизирует свои средства защиты самостоятельно; кто-то внедряет или адаптирует готовые решения; кто-то обращается к фирмам, предлагающим поиск аномалий как сервис.

Один из крупных американских банков подключил к борьбе с мошенниками разработанный в IBM суперкомпьютер Watson.

Система IBM, использующая элементы Watson, анализировала поток транзакций в реальном времени, оценивая подозрительность каждой из них. На оценку, среди прочего, влияла история отношений банка с торговой точкой, которая инициировала сделку. Чем больше мошеннических транзакций в ее послужном списке, тем меньше к ней доверия.

В IBM утверждают, что система на 15% увеличила количество выявленных мошеннических обращений к банку и на 50% сократила число ложных срабатываний. При этом сумма, которую удалось защитить от мошенников, выросла на 60%.

Те же методы работают и в других областях, причем не менее действенно. Министерство труда Германии приспособило их для анализа заявок на получение пособий по безработице. Скоро стало ясно, что около 20% пособий выплачивалось незаслуженно. Такое применение больших данных позволили министерству сократить расходы на 10 млрд евро.

Американская Комиссия по ценным бумагам и биржам (SEC) тоже автоматизировала поиск мошенников, но в данном случае речь идет не о мелких жуликах, обналичивающих краденые кредитки, и даже не о фальшивых безработных. В SEC метят выше и выводят на чистую воду мегакорпорации, совершающие финансовые нарушения.

Система выявления мошенничества, которую разрабатывают по заказу SEC, анализирует не только финансовые показатели (это самой собой разумеется), но и менее структурированные данные — вплоть до лексики, использованной в пояснениях к отчетности компании.

Компании ZestFinance, AvantCredit и Xoom обосновались в нишах, которые известны высоким уровнем риска, и теснят конкурентов за счет использования более совершенных технологий.

Типичный клиент AvantCredit — это человек с плохим кредитным рейтингом, попавший в трудную ситуацию. Возможно, он внезапно

остался без работы, возможно, его настигли непредвиденные медицинские расходы. Обычные банки не верят, что он сможет вернуть деньги, и отказываются с ним работать, а те, кто все же готов дать заем, компенсируют свой риск чудовищной процентной ставкой.

AvantCredit предоставляет кредиты величиной до 10 тыс. долл. США и не требует хищнических процентов. Вместо традиционного кредитного рейтинга компания использует статистические модели и алгоритмы машинного обучения, которые учитывают тысячи параметров: информацию, которую клиент предоставил сам, сведения, почерпнутые из социальных сетей, его историю транзакций и многое другое. Чем точнее прогноз, тем меньше невыплаченных кредитов и тем выгоднее условия, которые может предложить компания. Алгоритмы, вникающие во все детали, способны дать куда более справедливую оценку платежеспособности человека, чем банковские служащие при личной встрече.

Xoom работает в другой области, но суть та же: пока конкуренты повышают тарифы, чтобы покрыть убытки, причиняемые мошенниками, эта компания избегает убытков с помощью больших данных и предлагает клиентам более выгодные условия. Xoom представляет собой платежный сервис для перевода наличных из Соединенных Штатов в Индию, на Филиппины, в ЮАР, а также страны Латинской Америки и Европы. Как правило, им пользуются приезжие из стран третьего мира, чтобы отправить деньги оставшейся на родине семье. Риск в таком бизнесе неизбежен, но алгоритмы, с помощью которых Xoom оценивает благонадежность транзакций, позволяют сократить его до минимума. Лишь 0,35% переводов приводит к убыткам. Это втрое больше, чем у платежных систем вроде Visa или MasterCard, но и задача, которая стоит перед Xoom, сложнее.

Компании, занимающиеся обеспечением кибербезопасности, всегда полагались на все более усложнявшиеся программы, которые на примере известных им вирусов обучались распознавать новые, неизвестные. К ним добавились алгоритмы, которые следят за работой других программ и оповещают об опасности, если в этой работе происходит что-то неожиданное.

Некоторые системы защиты заключают подозрительно ведущие себя программы в виртуальный контейнер и с помощью разных методов пытаются «разорвать» вредоносный код и выявить его намерения.

Появление больших объемов информации позволило сделать важный шаг на пути к созданию программ защиты, которые позволяют перехватывать 60—70% вирусов, оставшихся незамеченными традиционным антивирусным «софтом». Обучающиеся машины позволяют выявить ДНК вирусных семейств, а не просто отдельные вирусы.

Этот подход был почерпнут из мира *даталогии*, или науки о данных, и оказался очень результативным благодаря огромной базе, быстро собранной компаниями, которые начали отслеживать поведение зараженных вирусами компьютеров. Автоматизация выявления таких аномальных шагов необходима потому, что человек или даже большая группа людей не сможет выявить их достаточно быстро.

Центр по обмену и анализу информации о финансовых услугах — влиятельная организация по кибербезопасности в финансовой сфере — объявил в октябре 2016 г. о создании подразделения, целью которого является борьба с киберпреступностью и укрепление кибербезопасности финансовых институтов. Как сообщили в FS-ISAC, создание этого подразделения — результат переговоров восьми банков (Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street и Wells Fargo).

Функции самого Центра по обмену и анализу информации о финансовых услугах примерно такие же, но он объединяет 7 тыс. банков. В связи с этим крупные финансовые институты решили, что им необходимо выделиться в отдельную группу, так как хакеры в первую очередь атакуют именно их, а не более мелкие банки. Новое подразделение, которое называется центром по финансовому системному анализу и устойчивости, также будет координировать деятельность банков и американского правительства в этой сфере.

В 2015 г. в структуре Банка России создан Центр мониторинга и предупреждения компьютерных атак, осуществляемых в кредитно-финансовой сфере (FinCERT). Основная цель создания Центра — координация работ по противодействию криминальным элементам, активность которых направлена на личное обогащение с использованием методов несанкционированного доступа к IT-инфраструктуре организаций кредитно-финансовой сферы. Также организовано взаимодействие FinCERT с МВД России, ФСБ России и Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

Кроме того, Банк России планирует создать лабораторию, специализирующуюся на изучении технологий и последствий компьютерных атак. Лабораторию предполагается создать в структуре самого Банка России — на базе Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. Прототипом такого исследовательского центра может стать уже существующий в Малайзии его аналог.

Специалисты лаборатории будут изучать способы и исходы компьютерных угроз, включая атаки на банкоматы, POS-терминалы и устройства самообслуживания. Кроме того, сотрудники Банка России

будут анализировать мошеннические интернет-ресурсы, мобильные устройства, новая структура будет помогать кредитно-финансовым организациям корректно снимать и опечатывать передаваемые на исследование объекты. Центробанк РФ, со своей стороны, будет готовить описание средств и методов атак на устройства самообслуживания, а также рекомендации по противодействию атакам на устройства самообслуживания.

О возможностях защиты информации в современных организациях с помощью *квантовой криптографии* сделал доклад А. Львовский на международной конференции «Вперед в будущее: роль и место России», приуроченной к 175-летию Сбербанка.

Противоборство между киберпреступниками и киберполицейскими идет давно — на каждый новый более изощренный метод защиты придумывают новые методы взлома. До сих пор борьба шла в сфере математики и кибернетики — создавались новые криптографические алгоритмы, новые методы дешифровки, новые программы для взлома, новые вирусы. Но уже близко время, когда на поле битвы выйдет физика, и это будет *квантовая физика*.

Обычные методы шифрования имеют одно неустранимое слабое место — участникам разговора нужно обменяться ключами шифра. Пользоваться обычной линией связи для передачи шифра нельзя: если злоумышленник эту линию прослушивает, все усилия по шифрованию пропадут зря. Поэтому наиболее важные криптографические шифры, используемые для передачи совершенно секретных государственных или военных донесений, посылают со специальными охраняемыми курьерами. Такой способ, естественно, чрезвычайно дорог. Поэтому для повседневных применений, таких как передача номера кредитной карточки с компьютера пользователя на сервер при интернет-шопинге, используют криптографические системы с открытыми ключами, основанные на несимметричности некоторых математических операций. Так, умножить одно число на другое очень просто, но решить обратную задачу факторизации — разложения числа на множители — значительно сложнее. Например, обычному компьютеру для разложения открытого ключа длиной 2 килобита потребуется несколько сотен лет. Так устроен, в частности, широко применяемый алгоритм RSA.

Но очень скоро такие системы шифрования окажутся бесполезными, появится инструмент, способный взламывать их за несколько минут, — *квантовый компьютер*. «Классический» компьютер запоминает и обрабатывает информацию, записанную в двоичном коде — 0 или 1, закодированную в магнитных полях или электрических зарядах. В квантовом компьютере данные записываются в состояниях

квантовых объектов — ионов, атомов, фотонов, сверхпроводящих контактах Джозефсона, которые могут находиться в суперпозиции состояний, т. е. в них одновременно могут быть записаны сразу множество значений между 0 и 1. В момент измерения суперпозиция разрушается, квантовый бит — кубит — выдает с определенной вероятностью либо 1, либо 0. Если мы возьмем множество кубитов в определенных состояниях, заставим их взаимодействовать друг с другом, а потом считаем данные, мы можем получить решение сразу множества задач одновременно.

Пока настоящие квантовые компьютеры, состоящие из десятков кубитов, еще не созданы. Очень сложно удержать кубиты в определенном состоянии длительное время. Пока лучшего результата здесь добилась IBM, которая с помощью квантового компьютера из пяти кубитов смогла разложить на множители число 15. Канадская компания D-Wave выпускает квантовые компьютеры из тысячи кубитов, с которыми экспериментируют в Google и NASA. Однако машина D-Wave — не универсальный квантовый компьютер, и ее преимущество по сравнению с классическими компьютерами многими оспаривается. Российские физики пока работают только с одиночными кубитами. В частности, первый в нашей стране сверхпроводящий кубит был создан в Российском квантовом центре в 2015 г.

Даже когда универсальные квантовые компьютеры будут созданы, они подойдут не для всех вычислительных задач. Однако они имеют колоссальное преимущество перед классическими компьютерами в целом ряде применений, многие из которых чрезвычайно важны. Универсальные квантовые компьютеры могут совершить революцию в сфере обработки больших данных, т. е. методах вычленения скрытых закономерностей и связей из больших массивов данных. Они, например, смогут оценивать закономерности потребительского поведения и предлагать товар более точно подобранной аудитории, выискивать данные о террористах в огромных массивах «цифровых следов». Не исключено, что именно квантовые алгоритмы помогут вывести на новый уровень технологию искусственного интеллекта.

Однако поистине «взрывной» характер, предопределивший технологическую гонку в этой области, носит именно способность квантового компьютера быстро разлагать числа на множители, т. е. взламывать криптографические системы с открытыми ключами. Именно это делает квантовый компьютер оружием в кибервойне — атомной бомбой XXI в.

Хотя до создания полноценных квантовых ЭВМ остается еще от 10 до 20 лет, специалисты по кибербезопасности очень серьезно воспринимают эту потенциальную угрозу. Американское АНБ в январе

2016 г. выпустило предупреждение и назвало криптографические алгоритмы, которые потенциально могут выдержать квантовую атаку.

Спасение от квантовых хакеров может принести квантовая криптография. Защищенные каналы связи, которые используются, например, для транзакций с кредитными картами, основаны на применении ключей — кодов для зашифровывания и дешифровки сообщений. Квантовая криптография — это способ использовать законы квантовой физики, чтобы обеспечить безопасность передачи ключей. Уникальное свойство квантовой криптографии — это ее способность фиксировать любую попытку подслушать информацию при передаче.

Информация в квантовых каналах связи кодируется в квантовых состояниях фотонов — в их поляризации. Например, фотоны, поляризованные по вертикали, могут кодировать единицу, а по горизонтали — ноль. Измерить поляризацию можно только единожды, после чего состояние необратимо меняется, а значит, если кто-то посередине линии связи попытается определить, что именно по ней передается, это сразу станет понятно получателю.

Квантовая криптография, в отличие от квантовых компьютеров, уже вполне работающая технология.

Первые лабораторные устройства для защищенной квантовой связи появились еще в конце 1980-х гг., сейчас на поставках этих систем специализируются около 10 компаний. Например, компания ID Quantigue обеспечивала защиту данных при пересылке результатов подсчета голосов на выборах в Швейцарии. По прогнозам аналитиков, объем этого рынка в 2020 г. составит 900 млн долл. США.

Препятствием для повсеместного применения квантовой криптографии является ограниченное расстояние, на которое можно пересылать фотоны. Проходя по оптическому волокну, половина фотонов теряется каждые 10—15 км, что делает передачу ключа на расстояние более 200—300 км практически невозможной.

Отчасти решить проблему может космос — Китай в этом году запустил первый *«квантовый» спутник QUESS*. Такой спутник проводит сеансы квантовой связи со станциями, расположенными на Земле, пока пролетает над ними. Это позволяет обмениваться защищенной информацией между любыми точками, над которыми проходит орбита — как бы далеко друг от друга они ни располагались. Теоретически такой способ передачи можно «взломать», однако для этого злоумышленнику придется физически захватить спутник и при этом остаться незамеченным. На практике такое вряд ли реализуемо.

Спутниковая квантовая связь, однако, недешева. Альтернативным решением проблемы расстояния может стать *квантовый повторитель* — пока гипотетическое устройство, позволяющее создавать за-

путанные пары фотонов, из которых можно извлечь секретный ключ. У физиков есть теоретическое понимание, как должен быть устроен квантовый повторитель, однако его практическая реализация потребует значительного улучшения технологий квантовой телепортации и квантовой памяти для света. В России есть специалисты и проводятся исследования мирового уровня по этой теме.

Еще одно препятствие — отсутствие нормативной базы, регламентирующей квантовые системы связи. Поэтому сейчас многие компании пытаются создавать гибридные устройства, совмещающие обычные телекоммуникационные стандарты с элементами квантовой защиты. Именно по этому пути идет Российский квантовый центр, который впервые в России запустил квантовую линию связи по обычной оптоволоконной линии между двумя отделениями Газпромбанка.

§ 4. Борьба с биткойн-преступностью и использование технологии блокчейн для предупреждения преступлений

В 2016 г. Европол, Интерпол и Базельский институт управления договорились о создании совместной рабочей группы, специализирующейся на цифровых валютах.

В задачу группы входит сбор и анализ информации о преступном использовании цифровых валют, расследование вопроса о хранении доходов, полученных преступным путем, организация ежегодных семинаров и встреч представителей трех ведомств и других учреждений, а также создание сети специалистов по биткойн-преступности.

Одновременно нью-йоркский стартап Chainalysis и Европейский центр Европола по борьбе с киберпреступлениями подписали соглашение о сотрудничестве и обмене данными, чтобы противостоять онлайн-преступлениям.

Постоянно вскрывающиеся факты использования криптовалюты в криминальных целях подрывают доверие к ней у многих добропорядочных граждан.

В июле 2017 г. в США заочно обвинили задержанного в Греции россиянина А. Винника в организации схемы по отмыванию более 4 млрд долл. США через популярную биткойн-биржу BTC-e. По данным американского Минюста, Винник не только создал биржу, но и был причастен к взлому ее более популярного конкурента Mt. Gox.

Согласно данным нескольких американских ведомств россиянин был основателем биржи BTC-e и, как утверждается в обвинительных документах, управлял ею с 2011 г., позволяя преступникам всего мира отмывать доходы в нескольких криптовалютах: помимо биткойна им

были доступны операции с Litecoin, Namecoin, Novacoin, Peercoin, Ethereum и Dash, а также их переводы в доллары, евро и рубли.

В заявлении Минюста США значится, что Винник «вел безнес значительного масштаба» в США, хотя представляющая биржу компания зарегистрирована на Кипре, а на сайте биржи указано, что ее офис находится в Болгарии.

В общей сложности через BTC-e было отмыто более 300 тыс. биткойнов и десятки тысяч единиц других криптовалют, а среди ее клиентов было немало американцев. Именно поэтому одним из первых обвинительных пунктов стало отсутствие регистрации компании в Министерстве финансов США[1].

Кроме того, Минюст посчитал, что Винник пренебрег борьбой с отмыванием денег: площадка была популярным местом для вывода средств, вырученных в результате продажи наркотиков, оружия, выкупов за хакерские атаки и прочую нелегальную деятельность.

В связи с этим россиянину также предъявлены обвинения в заговоре с целью отмывания денег и в легализации преступных доходов. Клиентам биржи предоставлялась максимальная анонимность: независимо от суммы администрация не требовала подтверждения личности и не обременяла пользователей лишними формальностями.

Коллегия присяжных суда Сан-Франциско уже утвердила обвинения, а Управление по борьбе с финансовыми преступлениями Минфина США назначило бирже BTC-e штраф в размере 110 млн долл., а лично Виннику — 12 млн долл. США.

В России BTC-e заблокирована с января 2016 г. по решению Приморского районного суда Санкт-Петербурга, который постановил, что информация, размещенная на площадке, на территории страны считается незаконной.

По данным статистического сервиса Bitcoinity, за последний месяц перед арестом Винника на BTC-e пришлось 3,73% от общемирового объема транзакций — это более 177 тыс. биткойнов, что эквивалентно 444 млн долл. США, или 26,5 млрд руб.

Немалая часть этих средств прошла через биржу с использованием биткойн-миксеров (сервисов для разбивки крупных транзакций на более мелкие, чтобы их нельзя было отследить по блокчейну), после чего была обменена на привычные валюты — доллары и евро. Деньги выводили крупные поставщики и торговцы наркотиками, преимущественно ведущие дела в биткойнах, которые столкнулись с угрозой потери денег из-за потенциального разветвления криптовалюты.

[1] См.: URL: https://m.lenta.ru/articles/2017/07/27/btce_end.

Поддержка наркобаронов в Tor — не единственное сомнительное достижение Винника. Сообщество сетевых активистов WizSec (Bitcoin Security Specialists) отметило, что россиянин уже несколько лет значится главным подозреваемым в уничтожении первой в мире биткойн-биржи Mt. Gox.

Меморандум о взаимопонимании между блокчейн-компанией и Европолом должен способствовать поиску и наказанию биткойн-вымогателей.

Chainalysis специализируется на идентификации злоумышленников, отслеживая их действия в блоковой цепи. Команда разработчиков стартапа работает над программой, которая будет соблюдать конфиденциальность клиентов и в то же время предотвратит взлом системы.

В 2015 г. была сформирована государственно-частная инициатива «Блокчейн альянс» с целью борьбы с преступной деятельностью в области блокчейна и биткойна.

«Блокчейн альянс» — это некоммерческая организация, которая была создана Палатой цифровой коммерции и организацией Coin Center. В состав альянса входят «Инициатива цифровой валюты» Медиа лаборатории МТИ, разработчик Г. Андресен, компания BitFinex и некоторые другие компании и организации. Все они объединились для того, чтобы рассеять все опасения относительно преступного использования криптовалюты биткойн и технологии блокчейн в целом. Причиной создания альянса стало то, что для успешного развития блокчейна нужно объединиться и изменить ошибочное представление о биткойне как о валюте преступников.

Альянс координирует свои действия с Департаментом юстиции, включая ФБР и Службу маршалов США, а также с Секретной службой США, Министерством внутренней безопасности США и Комиссией по срочной биржевой торговле, в планах альянса также взаимодействие с другими американскими и зарубежными агентствами.

Исполнительный директор Coin Center Дж. Брито отметил, что цель альянса состоит в том, чтобы гарантировать, что преимущества, которые блокчейн и биткойн способны предоставить миллионам пользователей, не останутся недооцененными лишь из-за потенциальной опасности нецелевого использования биткойна небольшими группами людей.

Standard Chartered Pic и DBS Group Holdings Ltd собираются создать блокчейн-реестр инвойсов (документов, сопровождающих внешнеэкономические сделки), чтобы сократить издержки и предотвратить мошенничество, с которым сталкиваются компании, финансирующие международную торговлю.

Соображения конфиденциальности мешают банкам обмениваться информацией о совершаемых ими транзакциях, что позволяет недобросовестным клиентам использовать одни и те же документы многократно. Именно поэтому технология блокчейн, гарантирующая прозрачность всех транзакций, могла бы стать решением проблемы инвойс-мошенничества.

Блокчейн — цепочка блоков, в которую можно «вписать» любую информацию, но без изменения предыдущих записей — может помочь оцифровать любую информацию в мире, а доступ к ней без рисков ущерба сможет иметь любой желающий. Блокчейн выступает этаким «эликсиром доверия»: благодаря архитектуре сети (невозможно редактировать изменения, уже внесенные в базу данных, без согласия большинства участников) провайдер инфраструктуры, который раньше выступал гарантом доверия, теряет свою исключительную роль.

Блокчейн можно сравнить с учетной книгой. Из нее нельзя тайком вырвать страницу, в ней нельзя подрисовать нолик к уже записанному числу — записи книги хранятся в виде копий распределенно, в тысячах экземпляров у разных людей (точно так же, как цепочки блоков в сети блокчейн хранятся на множестве узлов). Поэтому блокчейн можно использовать в любых сферах, где децентрализованные реестры позволят проводить операции с цифровыми активами безопаснее и эффективнее.

В конце 2015 г. DBS и Standard Chartered протестировали распределенную платформу TradeSafe, на которой планируют запускать инвойс-реестр. Кроме того, они активно сотрудничают с сингапурским ведомством, ответственным за развитие инновационных технологий.

Но внедрение блокчейна снимет проблему мошенничества только в том случае, если перейти на распределенную цепь решится сразу большинство банков.

В мире нет единых стандартов в регулировании цифровых валют, и каждый центральный банк руководствуется собственными подходами: от формального разрешения (включая рекомендации для индустрии о возможных рисках, исследования в данной области и проч.) или применения общих принципов регулирования в сфере платежей до полного запрета такой деятельности. Если рассмотреть, какие могут быть последствия в условиях формального разрешения осуществлять деятельность с цифровыми валютами, то центральным банкам, придерживающимся такого подхода, следует обратить внимание на негативную статистику банкротств цифровых бирж (в том числе связанных с мошенничеством и хакерскими атаками). Решением данных проблем могло бы стать лицензирование деятельности, связанной с

виртуальными валютами, например деятельности бирж виртуальных валют; администрированием и эмиссией виртуальных валют, их хранением и управлением ими третьих лиц.

Многие специалисты полагают, что осуществление полного запрета на указанную деятельность в условиях общемирового регуляторного тренда на формальное разрешение такой деятельности в рамках специальных лицензий может привести к свертыванию инновационных проектов в данной сфере и перенесению их в более прозрачную регуляторную юрисдикцию.

Автор первой книги про биткойны А. Форк полагает, что блокчейн может использоваться в рамках национальной платежной системы. Создается отдельный независимый блокчейн для использования в качестве национальной платежной системы. Граждане попадают в блокчейн, когда получают «персональный счет», привязанный к паспорту. Любой участник может пользоваться переводами в этой системе без комиссии. Законодательно закрепляется, что одна единица в этом блокчейне равна рублю. И все деньги (любое число) первоначально эмитированы на одном «персональном счете» (например, Банка России).

«Персональный счет» — это цифровой документ на предъявителя. Он представляет собой набор букв и цифр. Его можно смело передавать другой стороне без раскрытия личности. Только государственные органы могут верифицировать пользователя по счету. Для этой платежной системы могут быть применимы различные интерфейсы: приложение для компьютера, веб-версия (оплата через личный кабинет), оплата с помощью мобильных устройств, в том числе NFC, QR-code, оплата с помощью платежных карт.

Преимуществами такой платежной системы являются 100%-ная прозрачность движения средств в стране; скорость движения денег (практически мгновенно — до 2 секунд); подтверждение за 10 минут; надежная защита безопасности; контроль за движением бюджетных средств, простота управления ими (может быть осуществлено силами одного человека); невозможность отмывания денег. Блокчейн также предусматривает дополнительные возможности (автоматическое налогообложение физических и юридических лиц, применение на разных платформах, в том числе мобильное приложение и т. д.).

Национальные банки Белоруссии, Казахстана, Великобритании, Молдовы внимательно изучают возможности блокчейна.

При этом необходимо отличать саму технологию от конкретных криптовалют. Технологии распределенной обработки (включая bloclchain и bitshares) действительно изучаются на уровне как регуляторов, так и коммерческих организаций. В Банке России создана рабочая группа, которая изучает вопросы технологий распределенной обработки и учета финансовой информации. Ее цель — проанализировать основные тенденции и практики в этой области, а также определить подходы к регулированию.

§ 5. Использование для предотвращения террористических актов технологий, позволяющих видеть сквозь стены

Что сегодня известно о технологиях, помогающих видеть сквозь стены?

1. Обратно-рассеянное рентгеновское излучение (ОРРИ) — технология, при которой рентгеновские лучи от источника не проходят сквозь объект, а отражаются. Так как объект не надо просвечивать насквозь, возможно использовать излучение с интенсивностью на несколько порядков ниже, чем при проникающем излучении.

К числу веществ с малой атомной массой относятся взрывчатые и наркотические вещества, алкоголесодержащие жидкости, ткани тела человека. Это позволяет легко идентифицировать скрытые органические материалы или людей, которые могут представлять угрозу безопасности.

Использование технологии ОРРИ позволяет:

— получать изображения органических предметов, плохо различаемых при обычно используемой технологии проникающего рентгеновского изучения;

— размещать источник и приемники излучения в устройствах досмотра, расположенных с одной стороны от досматриваемого объекта;

— создавать за счет малой мощности излучения устройств, использующих данную технологию, системы, безопасные для операторов и людей.

2. Переносной радар «Голограф» (испытания в частях российского спецназа начались в 2014 г.) обнаруживает людей и животных через стены, уже поступил на испытания в спецподразделения Вооруженных Сил РФ. Разработка Центрального научно-исследовательского института химии и механики предназначается для использования в контртеррористических операциях и должна помочь быстро скоординировать действия отряда и обезопасить заложников. Доработка устройства возможна после испытаний радара военными.

Это устройство в первую очередь необходимо подразделениям антитеррора, которые работают с учетом сохранения жизни заложников. Когда при выполнении операций надо обеспечить сохранность окружающих объектов, «Голограф» также окажет помощь бойцам спецназа.

Радар мог бы спасти очень много жизней в ситуациях, когда есть какие-то материалы или объекты, которые нельзя повредить. Например, борт самолета, где придется работать врукопашную. Благодаря новому прибору можно разобрать цели, посмотрев, кто где находится и где неожиданно обрушиться на врага, — это 50% успеха.

Радар «Голограф» работает при помощи сверхкоротких радиоимпульсов на частоте от 1 до 4 ГГц, пропуская их через любые материалы и принимая отраженный сигнал, обнаруживает движение на расстоянии до 6,5 м. Устройство обладает небольшими габаритами и весом 4,5 кг, выдерживает падение на бетон с высоты 1 м и может использоваться при температурах от –20 °С до +50 °С.

Радар прост в использовании, предусмотрена возможность работы с помощью одной руки. Любой человек, даже новобранец, сможет пользоваться устройством через 15 минут после того, как ему объяснят принцип работы. В нем очень мало настроек, практически нет — есть кнопка включения и очень доступная индикация.

«Голограф» способен распознавать движения сквозь кирпич, бетон, дерево, гипс, глину, сухой грунт и штукатурку. Как рассказал представитель разработчика, в каждом отдельном случае у радара разные возможности, но главное, чтобы материал не содержал воды.

Все зависит от материала стены — сквозь дерево он «видит» на метр, если это кирпич — на полметра, а бетон уже должен быть тоньше, потому что содержит железо. Кроме того, очень важно, насколько материал стены влажен: если это свежепостроенное здание и кирпич или пеноблоки не высохли, то видно хуже — волны гасятся, мешает вода.

Помимо сырого кирпича проблемой может стать совместное использование «Голографа» с устройствами, заглушающими сигналы сотовой связи. Данная возможность ограниченно испытана, при низкой мощности излучателей радар не реагирует на мобильные телефоны, Wi-Fi-роутеры.

3. Ученые научились видеть людей через стены с помощью Wi-Fi. Компания Technische Universität Ilmenau (ФРГ) создала в 2017 г. уникальный высокочувствительный компактный прибор, который позволяет с высокой степенью детализации смотреть сквозь препятствия. Разработчики устройства утверждают, что оно дает возможность заглянуть за бетонные и кирпичные стены даже многометровой толщиной. Специалисты компании убеждены, что их «всевидящее око» поможет в полицейских и спасательных операциях, а также в борьбе с терроризмом.

Физики из Массачусетского технологического института (МТИ) придумали в 2016 г., как с помощью обычного Wi-Fi-передатчика видеть людей сквозь стены, причем не просто видеть, но и даже определять вес и рост человека. Ученые уверены, что новая технология понадобится спецслужбам и правоохранительным органам.

Физики из МТИ несколько преобразовали работу обычного Wi-Fi-маршрутизатора и «научили» его в буквальном смысле видеть объекты, находящиеся в соседней комнате. Технология работает довольно просто: маршрутизатор передает Wi-Fi сигналы через стену, которые отражаются от предметов и возвращаются назад, отображая картинку на экране компьютера. Затем ученые «натаскали» модифицированные передатчики на распознавание человеческих силуэтов, а дальнейшее улучшение алгоритма привело к тому, что маршрутизаторы «научились» определять точный рост и вес человека.

Такая технология, по большому счету, уже достаточно давно известна, но, как признали ученые из Массачусетса, она была рудиментарной. Вопреки этому мнению, 23-летний студент из Мюнхенского технического университета Ф. Холл в 2017 г. доказал, что Wi-Fi уже достиг возможностей, позволяющих получать качественные голограммы или трехмерные фотографии объектов в другой комнате, используя всего два небольших устройства. Ему потребовалось всего 20 секунд, чтобы сканировать в достаточно качественную объемную картинку все, что было у него за стеной. «Можно различить фигуру человека или собаку на кушетке, — пояснил разработчик, — любой предмет размером более 4 сантиметров».

Чтобы «смотреть сквозь стену», Холл использовал лишь две крохотные антенны вроде тех, которыми оснащены обычные смартфоны. Полученная антеннами информация обрабатывалась специальной программой, которая выдавала ее в виде качественной 3D-голограммы.

4. В принципе сквозь тонкие преграды позволяет «видеть» обыкновенный прибор ночного видения, действующий на основе приема и распознания инфракрасного излучения. Известны и «просвечивающие» сканеры, которые используют в аэропортах для поиска спрятанных под одеждой предметов. Но, скажем, для условий боевых действий нужно что-нибудь более «зрячее», способное на большом расстоянии распознавать противника, спрятавшегося не за фанерной ширмой или тканевым пологом, а за кирпичными стенами, панельными плитами и т. п.

5. Перспективно выглядит разработка ученых Мэрилендского университета (США). Они сканируют пространство за преградой при помощи радиоволн в терагерцевом диапазоне так называемых Т-лучей.

Приборы, использующие излучение такой частоты, уже применяются в медицине. В отличие от рентгеновских Т-лучи совершенно безвредны для биологических объектов. Но сложность их использова-

ния заключается в том, что применение до сих пор было возможно только при температурах, близких к абсолютному нулю.

Но есть проблема визуализации изображения, полученного отраженным от объекта Т-лучом. В медицине эта задача решалась при помощи графеновых пластин — модификации углерода с повышенной подвижностью электронов в кристаллической решетке. Благодаря этому свойству Т-луч получает возможность «нагреть» и «выбить» эти электроны из графеновой пластины, вследствие чего на пластине возникает положительный потенциал, который и помогает зарегистрировать и визуализировать исследуемый объект.

Но как американским ученым удалось довести столь сложное оборудование до размеров, при которых его можно использовать в реальной боевой обстановке? Или же был испытан всего лишь лабораторный образец, демонстрирующий принципиальную пригодность метода?

6. Симферопольская компания «ЭМИИА» разработала технологию, позволяющую «видеть» движение людей, животных, жидкостей, а также различных объектов сквозь стены.

Новый прибор использует эффект Доплера — изменение частоты и длины волн, регистрируемых приемником, вызванное движением их источника и (или) движением приемника. В текущем виде система объединяет два компьютера и специальные сканирующие устройства.

В зависимости от типа и материала преграды система позволяет «смотреть» сквозь стены и другие оптически непрозрачные препятствия в радиусе до 50 м. А настоящее время изобретатели переносят свое детище на мобильную платформу и разрабатывают микрочип, который можно будет внедрять в различные аппараты и носимые гаджеты.

«В перспективе устройство может выглядеть как планшетный компьютер или шлем для бойца. Оно может устанавливаться на беспилотные летательные аппараты и передавать информацию на землю. Эта технология сможет заменить аварийные датчики и охранные устройства», — сообщают в компании «ЭМИИА».

7. В Росгвардии апробированы уникальные портативные радары, способные видеть людей даже через толстые стены. Изделие позволит спецназовцам вычислять террористов не только в зданиях, но и в замаскированных блиндажах и подземных тоннелях.

Новейший радар-стеновизор РО-900, разработанный группой компаний «Логис-Геотех», способен определять местонахождение движущегося человека на расстоянии до 21 м, при этом он видит сквозь несколько кирпичных или бетонных стен общей толщиной до 60 см. Это позволит бойцам Росгвардии на безопасном расстоянии обнаружить террористов не только внутри зданий, но и на их противоположной стороне, определить траекторию перемещения, а боевиков, стоящих неподвижно, радар обнаружит по дыханию.

Стеновизор РО-900 уже прошел все испытания, подтвердил характеристики и в настоящее время поставляется одной из российских спецслужб. К изделиям также проявляют интерес МВД России и другие силовые ведомства. Особую заинтересованность выразили представители МЧС России, которые планируют использовать их для поиска людей в завалах.

Стеновизор РО-900 работает по принципу георадара-локатора, который способен проводить радиоволны не только по воздуху, но и через грунт и стены зданий и регистрировать все отражения от препятствий.

Прибор похож на обыкновенную рацию без антенны. Он оснащен 3,5-дюймовым цветным дисплеем, который в реальном времени отображает результаты радиолокационной разведки. Полученные данные выводятся на экран в виде движущихся по диагонали красных полос — вертикальное направление экрана отображает информацию о расстоянии, на которое переместился человек, а горизонталь позволяет определить время, за которое он совершил маневр. При этом сам стеновизор очень компактен, его вес не превышает 1 кг.

Радар также регистрирует повторяющиеся движения с небольшой амплитудой, засекая таким образом расширение грудной клетки во время вдоха или биение сердца. Уже после 20 секунд анализа полученных данных радар выводит информацию об обнаружении затаившегося человека на дисплей в виде горизонтальной синей черты.

Эксперты считают, что стеновизор станет огромным подспорьем при боях или контртеррористических операциях в городах.

§ 6. Глобальная навигационная система и электронная слежка в целях предотвращения преступлений и актов терроризма

Глобальная навигационная система — это совокупность методов, программных и технических средств, позволяющих организовать фиксацию пространственно-временной информации и получение ее правоохранительными органами. Целью создания данной системы является повышение уровня информационно-аналитического обеспечения деятельности правоохранительных органов при осуществлении расследования и предупреждение преступлений[1].

Глобальная навигационная система представляет собой совокупность средств получения, а также программно-аппаратных комплек-

[1] См.: *Дусева Н. Ю.* Технико-криминалистические основы использования глобальной навигационной системы в расследовании и предупреждении преступлений: автореф. дис. ... канд. юрид. наук. Волгоград, 2015.

сов обработки и передачи пространственно-временной информации. Комплекс средств получения пространственно-временной информации включает в себя следующие подсистемы: ГЛОНАСС, подсистему стационарной связи, подсистему мобильной связи, подсистему радиочастотной идентификации, подсистему видеофиксации, подсистемы фиксации фактов обращения и персонализации.

Подсистемы, входящие в состав глобальной навигационной системы, отличаются набором фиксируемых данных, принципами работы, а также формой представления полученной информации. Для оптимизации комплексного использования составных частей глобальной навигационной системы необходима интеграция всех массивов пространственно-временной информации, зафиксированной их средствами, в единый информационный комплекс. Однако различия в принципах фиксации пространственно-временной информации в системах с автоматической фиксацией данных (ГЛОНАСС, стационарные системы связи, системы мобильной связи, системы радиочастотной идентификации, системы видеофиксации) и системах фиксации фактов обращения и персонализации диктуют необходимость разделения алгоритмов их использования в интересах правоохранительной деятельности.

Для обеспечения оперативности получения пространственно-временной информации о контролируемых объектах, а также представления данной информации в удобном для визуального восприятия виде необходима интеграция систем с автоматической фиксацией данных в единую структуру. Основой для данной интеграции могут служить существующие программно-технические комплексы систем мониторинга транспортных средств, функционирующие на основе спутниковой навигации, которая позволяет получать информацию о контролируемых объектах в виде карты с указанием их местонахождения в определенный момент времени. Одновременное отображение на карте местности пространственно-временной информации из всех систем с автоматической фиксацией данных позволяет провести упреждающие меры по пресечению преступлений.

С учетом назначения формируемой глобальной навигационной системы к перечню ее основных функциональных возможностей необходимо отнести: мониторинг контролируемых объектов, отображение местоположения контролируемых объектов на электронной карте местности, аналитическую обработку полученных данных.

Системы с автоматической регистрацией данных, входящие в состав глобальной навигационной системы, предполагают минимальное участие человека в процессе фиксации и хранения в них пространственно-временной и иной информации, что обеспечивает отсутствие «человеческого фактора» при ее обработке и сводит к минимуму ее возможные искажения.

В едином комплексе с глобальной навигационной системой следует рассматривать и новые *технологии электронного контроля*.

После событий 11 сентября 2001 г. создан ряд интересных *технологий дистанционной слежки*, которые могут найти повсеместное применение[1].

После ликвидации У. бен Ладена командой американского спецназа SEAL Team 6 в поле зрения журналистов попала секретная программа Пентагона под названием «Метки, отслеживание и поиск», или TTL. Целью этого проекта является создание средств, которые позволяют выследить особо важных лиц, скрывающихся в районе боевых действий или даже среди населения другой страны.

В настоящее время арсенал средств слежки охватывает практически все возможные способы идентификации и сопровождения человека: от классических сканеров отпечатков пальцев и радужки глаза до тепловой сигнатуры конкретного человека и микроскопической пыли, распыляемой с беспилотных самолетов и светящейся в лучах радаров.

Антитеррористическая батарейка. Первой и достаточно простой была технология инфракрасных маяков, которую используют как солдаты, так и секретные агенты. Маяк представляет собой программируемую ИК-лампу, работающую в импульсном или непрерывном режиме, и источник питания. Свет, излучаемый таким маяком, не виден невооруженным глазом, но хорошо заметен в прибор ночного видения (ПНВ) или тепловизор. В июне 2009 г. «Аль-Каида» выпустила электронную книгу, посвященную тактике шпионов из числа местного населения, которые работают на США. Среди описания тактики действия вражеских агентов авторы «Аль-Каиды» публикуют фотографии инфракрасного маяка, приспособленного для работы от обычной девятивольтовой батарейки типа «Крона», которую несложно купить в Пакистане. В книге утверждается, что эти устройства пакистанские шпионы, нанятые американцами, используют для наведения беспилотных самолетов. Возможно, имеется в виду, что агенты таким образом, практически ничем не рискуя и не связываясь со своими «работодателями», отмечают маяками автомобили и здания, где скрываются террористы.

Надо отметить, что похожие инфракрасные маяки используют и американские солдаты для того, чтобы пилоты вертолетов и операторы БПЛА могли отличить их от бойцов противника. Сегодня инфра-

[1] URL: http://www.nanonewshet.ru/articles/2011/tekhnologii-slezhki-kak-idet-okhota-na-lyudei.

красные маяки уже морально устарели. Есть сообщения, что полевые агенты получили в распоряжение специальные мобильные телефоны, оснащенные встроенным инфракрасным лазером. В пыльном воздухе лазерный луч с большого расстояния виден в ПНВ или тепловизор, что позволяет агенту указывать на цель, не приближаясь к ней. Кроме того, такой «лазерный телефон» может в режиме реального времени давать целеуказание ракетам Hellfire, что потенциально снижает вероятность побочного ущерба.

Квантовая точка на карте. Чтобы отслеживать передвижение определенного человека и выделять его из толпы, американские военные разрабатывают специальную жидкость, которая позволяет обнаружить объект с большого расстояния.

Компания Voxtel разрабатывает продукт под названием NightMarks. Он представляет собой прозрачную жидкость, состоящую из крошечных нанокристаллических квантовых точек на основе селенида кадмия. Этот материал способен поглощать ультрафиолетовое (200—400 нм) или инфракрасное (700—1600 нм) излучение, а затем эффективно передавать энергию на специальные нанокристаллические люминофоры, которые светятся как в видимой (400—700 нм), так и в ближней инфракрасной области спектра.

Достаточно нанести такую жидкость на одежду или кожу человека (простым рукопожатием, с помощью БПЛА или другим способом), и беспилотный разведчик сможет надежно отслеживать яркую метку с большого расстояния. Эффектами поглощения и испускания света можно управлять, что позволяет изменить оптические свойства квантовых точек и создать множество своеобразных спектральных штрихкодов. Таким образом, появляется возможность отслеживать и надежно идентифицировать множество объектов.

Компания Tiax работает над аналогичными метками, которые могут со временем разлагаться. Это позволит избежать путаницы в большом количестве объектов наблюдения, а также снизить вероятность обнаружения факта слежки.

Использование RFID-чипов. Они похожи на те, что применяются для метки товаров в магазинах. В настоящее время армия США уже широко использует эту технологию идентификации своих сил на поле боя и логистики.

Специалисты Sandia National Laboratories разработали RFID-метки, которые способны реагировать на радиолокационный импульс и с высокой точностью определять местоположение объекта слежки. Например, обычные чипы, используемые в магазинах, имеют дальность действия в несколько метров, в то время как RFID-метки от Sandia имеют радиус до 20 км. Особенностью технологии является высокая

скрытность — метки «отзывают» только после облучения специальным радиолокационным импульсом.

Подобные RFID-чипы можно использовать не только для оперативной слежки за людьми и автотранспортом, но и в качестве превентивной меры по контролю за оружием, например встраивать их в переносные зенитные ракетные комплексы или противотанковые ракеты. В случае попадания этого оружия в руки террористов его будет достаточно легко обнаружить и быстро уничтожить ракетным ударом.

Миниатюрные RFID-метки могут работать с компактными радарами вроде M600 SpotterRF. Прибор размером с ноутбук разработан прежде всего для охраны периметра военных баз, но имеет большой потенциал для скрытой слежки; использует радиоволны X-диапазона и может обнаружить пешеходов на расстоянии до 1 км, а автотранспорт — до 1,5 км. Радар оснащен датчиком GPS и интегрирован с сервисом Google Earth, что позволяет отслеживать местоположение объекта на интерактивной карте.

Технологии уникальных запахов. Технологии оптического и радиолокационного слежения совершенны, но потенциально обнаружимы и поддаются обратному инжинирингу, т. е. враг может разобрать найденный маяк и придумать контрмеры. По этой причине военные ищут дополнительные способы тайной слежки. Технология компании Tracer Detection Technology предполагает использование уникальных запахов, позволяющих безошибочно выделить искомый объект из толпы. Специалисты компании изобрели специальный парафиновый карандаш, наполненный перфторуглеродами, термически стабильными соединениями, которые используются повсеместно — от производства холодильников до парфюмерии. Пары перфторуглеродов могут отслеживаться с помощью различных датчиков, например газового хроматографа. Достаточно провести карандашом по объекту слежки, и он в течение нескольких часов будет источать специфичный, незаметный для человеческого носа аромат. При этом изоляция в наглухо запертой комнате или под несколькими слоями одежды не поможет — по данным исследования, представленного в Министерство юстиции США, перфторуглеродные маркеры проникают сквозь закрытые окна, контейнеры и запертые чемоданы. Остаточные следы маркера сохраняются даже после тщательного смывания.

Технологии биомаркеров. В 2007 г. на одном из брифингов сил специальных операций США кратко упомянули об использовании в качестве технологии слежки биомаркеров — биологических веществ, которые позволяют надежно идентифицировать человека. Подробно-

стей об этой технологии нет, судя по всему, она представляет собой протеин, в котором зашифрован определенный код-идентификатор.

На руке человека такая метка выглядит как обычный синяк, можно снять с себя всю одежду, тщательно вымыть тело и сбрить все волосы, но маленькая незаметная биометка позволит идентифицировать человека в любом случае. Тактика использования биомаркеров остается загадкой, особенно это касается считывания информации и внедрения биометки. Теоретически биомаркер может оставаться в человеке на всю жизнь, что позволяет быстро выявить террориста, который выдает себя за другого человека.

Технология трехмерного моделирования лица человека. Все описанные выше технологии имеют один существенный недостаток: нужно подобраться к преследуемому поближе. Однако это не всегда возможно.

Чтобы от подобного «невидимого ока» скрыться было совершенно невозможно, компания Photon-X разрабатывает технологию трехмерного моделирования лица человека по нескольким снимкам с оптических и инфракрасных камер беспилотников. Специальное программное обеспечение позволяет создать детальный профиль головы человека с помощью мультиспектральных датчиков и анализа движения лицевых мышц. Новая система позволит идентифицировать человека в толпе и сопровождать его без необходимости установки каких-либо маяков. Разумеется, оптические сенсоры не могут следить за человеком внутри здания, но зато они могут легко найти его даже на многолюдной улице большого города. Далее при необходимости врага можно уничтожить ракетой или привлечь агентов, которые установят маяк. Система Photon-X решает главную задачу — слежение за большим количеством людей на обширных пространствах.

Возможности программы спутникового слежения за мобильными телефонами. Современные GPS-технологии могут помочь выполнить поиск телефона, а также многих других объектов через спутник. Осуществляет все это спутниковая система, работающая через специальную программу слежения (/gps/programma-slezhenija-za-telefonom).

Если система слежения используется для наблюдения за людьми, то у наблюдаемого человека с собой всегда должно быть специальное устройство — персональный GPS-трекер или сотовый телефон фирм Nokia, iPhone, HTC с поддержкой функции GPS и операционной системой, например, Android. Таким образом, этот мобильный телефон превратится в своеобразный «маячок» с установленной на нем специальной программой слежения. Если использовать программу слежения для наблюдения за людьми, то мобильный телефон легко можно положить в портфель или карман объекта, который нуждается в вашем контроле, или если необходимо GPS-слежение за автомобилем, мобильный телефон можно положить и в «бардачок». После определения программой слежения точных координат, местонахождения и скорости данные отправляются на сервер системы. Все эти данные программа слежения получает с заранее заданной периодичностью.

Проследить за тем, как проводится GPS-слежение, можно в режиме онлайн: с компьютера или мобильного телефона. Помимо местонахождения наблюдаемого объекта в настоящий момент GPS-программа слежения позволяет на электронной карте проследить направление движения и его скорость. GPS-система слежения сохраняет всю историю передвижений отслеживаемых объектов.

Сегодня каждый желающий, вооружившись специальным программным обеспечением, имеет возможность проследить за действиями любого абонента сотовой связи, т. е. при помощи специальных программ, таких как ShadowGuard, например, можно прослушать переговоры по чужому телефону или же прочитать переписку по СМС. Еще несколько лет назад это было похоже на шпионскую фантастику, но сегодня это реальность, и огромное количество людей воспользовалось такой возможностью. А там, где имеется спрос, как известно из законов рынка, рождается и предложение. И на сегодняшний день появилось множество сервисов, которые предлагают воспользоваться такой невероятной возможностью.

Электронное антитеррористическое наблюдение. Серьезный шаг сделали и разведывательные технологии после событий 11 сентября 2001 г., когда были приняты беспрецедентные меры, даже охарактеризованные в СМИ как конец существования конфиденциальной информации в США. Особого внимания заслуживает крупномасштабный проект Министерства обороны США «Тотальная информационная осведомленность» (ТИО). Он предполагает разработку и эксплуатацию новейших ИКТ, с помощью которых можно осуществлять тотальное наблюдение за счет массированного увеличения источников информации, перехвата сообщений любого характера, оперативного анализа в режиме реального времени, т. е. сбора колоссального количества данных, а главное — молниеносную реакцию спецслужб. Как утверждается, эти меры будут противодействовать террористическим угрозам за счет мониторинга местонахождения, передвижений и деловой активности населения, т. е. сбора максимально широкой информации обо всех подозрительных явлениях, указывающих на планы террористов.

Система ТИО интегрирует всеобъемлющие цифровые данные об американских гражданах, а также об иностранцах, имеющих контакты с населением США, которые следует подразделить на два типа: личностные (деловые, функциональные) и биометрические. Первые

предполагается черпать из всех существующих баз данных как государственного, так и отраслевого назначения: медицинских, образовательных, торговых, туристических, телефонных, корпоративных, ветеринарных и т. д., а также из источников, куда проникли все отслеживающие электронные устройства: банковские счета, кредитные карточки, аренда машин, транспортные агентства, медицинские и ветеринарные записи, телефонные и иные коммуникативные сообщения, письменные, электронные, телефонные заявления граждан в госорганы и т.л. Биометрические данные — это изображение радужной оболочки и сетчатки глаз, отпечатки пальцев, ДНК, графические снимки лица и т. д.

Если учесть, что при этом используется хорошо зарекомендовавшая себя традиционная техника сбора данных, например просеивание телефонных счетов, магазинных дисконтных карточек и т. д., но уже через виртуальное сито, то сбор информации по линии ТИО достигнет беспрецедентных масштабов. Возникнет уникальная централизованная система, которая, преодолев разобщенность и недостатки многочисленных имеющихся баз данных, будет содержать точные данные, где находился и что делал конкретный человек в заданное время. И тогда каждый гражданин США, будь то потенциальный террорист или лояльный гражданин, окажется под информационным колпаком спецслужб.

Новый этап в эпоху слежения за объектами связан с космическими летательными аппаратами, в частности спутниками, возможности которых с учетом постоянно совершенствующейся фотовидеоаппаратуры безграничны. Причем передающие спутники могут двигаться по определенной траектории, фиксируя все на своем пути, а стационарные — предметы и их передвижение в одной географической точке. Спутники, оснащенные специальными приборами, не только видят, но и слышат, отслеживая разнообразные коммуникативные процессы. Это своеобразные динамические базы данных, они не только собирают и хранят информацию, но и могут отправлять ее на Землю в заданном режиме. Наличие кода предохраняет ее от расшифровки. Спутникам мирного назначения проложили дорогу спутники-шпионы, существующие уже более 40 лет, оснащенные обычными или инфракрасными фотокинотелекамерами, электрооптическими сканерами и иной аппаратурой, несущие свою службу и сейчас.

Вся Земля находится в зоне видимости космических аппаратов. Маршруты спутников ничем не ограничены, поэтому с их помощью любое государство способно заглянуть в «огород соседа», причем не одномоментно, а неограниченное время. Вероятно, с точки зрения военных и политических целей (например, как выполняются двусторонние или многосторонние государственные обязательства) они вряд ли заменимы.

В ряде стран, в первую очередь в США, созданы системы геопространственной разведки — прежде всего в целях национальной безопасности, а также использования в гражданских целях. Спутниковая геопространственная информация находит применение и в борьбе с терроризмом.

В Германии введена единая компьютерная антитеррористическая база данных. Этот информационный банк состоит из двух частей: основной и расширенной. В основную включен набор данных, необходимых для идентификации личности (имя, пол, дата рождения, адрес, гражданство, владение языками, цветная фотография и приметы подозреваемых в террористической деятельности). Доступ к этой информации получат все разведывательные органы и службы по борьбе с преступностью.

В расширенную базу введена информация о семейном положении подозреваемого, его профессии, образовании, конфессиональной принадлежности, номерах автомобилей, банковских счетов и телефонов; данные о передвижении по миру, принадлежности к террористическим ячейкам, навыках владения оружием и обращения со взрывчатыми веществами, круге общения, связях с террористическими ячейками. Эту информацию заинтересованные ведомства смогут получать по спецзапросу. Однако субъекты спецзапросов строго не оговорены. Тогда этот запрос могут организовать и сами террористы, выявив тем самым круг потенциальных сторонников и недоброжелателей. Кроме того, возможны «утечка» информации изнутри и взлом извне или то и другое вместе. Тогда тщательно собранная, всеобъемлющая информация может оказаться во власти посторонних людей, а главное — криминальных структур. Нетрудно представить удовлетворенность последних, когда нужная информация будет подана буквально «на блюдечке».

Разведывательные системы становятся все более универсальными: в автоматическом режиме они не только собирают информацию, но и осуществляют ее анализ, делают выводы. Именно так работают системы глобальной слежки: в ряде англоязычных стран — ECHELO, в Европе — ENFOPOL, у нас — СОРМ-2.

Революционным событием является возможность с помощью современных ИКТ обозревать не отдельные участки, регионы, а целиком планету. Совсем недавно произошел беспрецедентный в мировой истории случай, когда известная компания Google Earth выставила на сетевое обозрение все без исключения уголки планеты. Появилось множество информации об объектах, о которых никто не ведал, и да-

же о тех, которые скрывались, например о секретных базах, аэродромах, кораблях, подлодках и т. д. Посредством новейших просматривающих устройств современное человечество в конце концов сумело рассмотреть свою колыбель и место обитания — Землю — в зеркале, называемом электронной информацией.

На повестку дня встала проблема имплантантов с помощью чипов, способных давать информацию о человеке везде и в любое время суток. Комиссия Евросоюза 16 марта 2005 г. согласилась с заключением № 20 Европейской группы по этике в науке и новым технологиям, заявив, что использование электронных имплантантов для слежки за людьми законно, если такой контроль будет закреплен законодательно.

§ 7. Распознавание лиц преступников и террористов на базе нейронных сетей

Почему технологии распознавания лиц будут все более востребованы в системах безопасности? Зачем помнить постоянно растущее количество паролей для разных сервисов и придумывать все более сложные способы идентификации себя в Интернете, когда у каждого человека с рождения есть уникальный идентификатор — его лицо? Крупнейший онлайн-торговец, китайская Alibaba Group, в 2015 г. объявила о скором запуске системы Smile to Pay, которая позволит покупателям входить на сайт и подтверждать покупки, глядя в камеру смартфона. И это лишь одно из множества перспективных направлений технологии распознавания лиц.

В вопросах распознавания лиц для обеспечения безопасности железнодорожного транспорта главным экспертом может выступить Япония. Именно в этой стране в сферу рельсовых перевозок людей и грузов внедрено максимальное количество высокотехнологичных решений. И это при том, что Япония считается мировым лидером по объему пассажиропотока, проходящего через вокзалы (а вокзалы здесь нередко объединяют и наземный, и подземный транспорт). Однако метрополитен Страны восходящего солнца, в частности Токио, вывели в авангард очень печальные события. Система безопасности в столичной подземке кардинально обновилась после марта 1995 г., когда религиозные фанатики из секты «Аум Синрикё» распылили на двух станциях ядовитый газ. Теперь токийское метро буквально напичкано современными видеокамерами — на 290 станций их приходится несколько тысяч! Установлены камеры и во многих вагонах скоростных поездов. Также есть камеры, которые специализируются на вычленении предметов и людей, не двигающихся в течение долгого времени. Все видеозаписи поступают в единый ситуативный центр,

куда стекается также вся информация от патрулирующих метро полицейских. Кроме того, имеются и специальные стереовидеокамеры, способные «засечь» посторонний предмет или человека на путях и скомандовать поезду остановиться.

В 2012 г. «Хитачи Кокусай Электрик» представила систему с камерой скрытого слежения, позволяющую обрабатывать базу данных в 36 млн лиц за 1 секунду.

Согласно заявлениям «Хитачи» эта высокая скорость обнаружения достигнута распознаванием лиц путем распознавания картинок на этапе записи камеры наблюдения и группировки полученных похожих лиц. Система объединяет лица, которые поворачиваются в рамках 30° и имеют минимальный размер на картинке 40 × 40 пикселей.

Планируется, что система скрытого видеонаблюдения будет внедряться в больших корпорациях, на крупных вокзалах и заводах. Применение такой системы в аэропорту или на вокзале поможет обнаружить злоумышленников, чьи фотографии заранее занесены в базу данных как «находящихся в розыске».

В 2014 г. ФБР США объявило об успешном запуске в эксплуатацию *системы распознавания нового поколения (NGI)*. Ее целью является расширение возможностей ведомства по идентификации граждан, и она должна заменить старую, основанную исключительно на отпечатках пальцев. С 2011 г. система работала в экспериментальном режиме.

Основной особенностью NGI является то, что она получает и обрабатывает биометрические данные автоматически. Система работает за счет информации, получаемой с камер видеонаблюдения по всей стране. Она выявляет уникальные черты лица того или иного человека и сохраняет их в базе данных. Затем при расследовании преступления она сможет провести быстрый анализ снимков и обнаружить злоумышленников. Для идентификации человека достаточно обнаружить, например, характерный шрам на его лице или татуировку на теле.

ФБР разработало NGI совместно с Lockheed Martin, Security Solutions и IBM. Целью программы объявили борьбу с терроризмом и преступностью благодаря улучшению способов биометрической идентификации, а также выработке новых методов анализа архивной информации в результате исследований, оценки и применения перспективных технологий.

С помощью этой системы теоретически можно распознать человека на любой фотографии, если информация о нем содержится в базе данных. Подобные менее комплексные методы идентификации давно используют такие компании, как Facebook, их технологии позволяют

автоматически идентифицировать того или иного пользователя на загруженной в социальную сеть фотографии. Проект разработки NGI рассчитан на 10 лет, и в него вложено 1,2 млрд долл. США. О старте программы официально объявили в 2008 г., когда ФБР заключило первый контракт на ее реализацию с фирмой Lockheed Martin.

В 2011 г. система автоматического распознавания лиц начала функционировать в экспериментальном режиме. Правоохранительные органы США получили от ФБР программное обеспечение, которое позволяло мгновенно сравнивать фотографии подозреваемых с базой данных. Число американских ведомств, использующих ее, постоянно растет.

NGI позволяет вести наблюдение за людьми, занимающими ответственные должности. Например, к ним относятся кассиры, учителя, работники социальных служб, т. е. те, кому необходимо сдать отпечатки пальцев и фотографию при приеме на работу. Система позволяет правоохранительным органам каждого штата в течение 24 часов узнать, не совершил ли человек, претендующий на такую должность, какое-либо преступление. ФБР только предупреждает местные правоохранительные органы о том, что соискатель уже был однажды арестован, а дальше им предлагается принимать решение, что с ним делать, самостоятельно.

Эта система помогает также следить за гражданами, освобожденными из мест заключения досрочно. Если бывший арестант совершит преступление в одном штате страны, то эта информация очень быстро будет доступна властям остальных штатов.

Помимо распознавания лиц NGI способна идентифицировать человека по его зрачку. В последнее время фотографии зрачков заключенных активно собирают в американских тюрьмах. Теоретически они могут использоваться для идентификации злоумышленников на месте преступления.

Пока что NGI далека от совершенства. Низкая разрешающая способность большинства камер видеонаблюдения не позволяет системе эффективно распознавать лица людей и тем более их зрачки. Но ее использование приносит плоды уже сейчас.

Системы идентификации нового поколения ведут поиск лиц по базе с фотографиями более 50 млн граждан. В штате Нью-Йорк система распознавания лиц уже работает в Управлении автотранспорта. Благодаря ей власти арестовали более 100 человек и открыли почти 1000 расследований.

В США в июне 2017 г. начались первые испытания системы распознавания лиц в нескольких аэропортах. Пассажирам авиакомпании JetBlue Airways, ставшей инициатором эксперимента, не придется да-

же доставать свои паспорта и прочие документы, чтобы попасть на борт самолета. Ведь новой системе достаточно бегло взглянуть на лица людей, чтобы проверить их через базы данных служб безопасности и зарегистрировать на рейс. Для того, чтобы воплотить этот проект в жизнь, JetBlue Airways объединила усилия с Таможенной службой и Пограничным патрулем США. За программную сторону проекта отвечает компания SITA.

Работа новой системы основывается на сверке лица человека с хранящейся в базе данных фотографией. Людям не нужно будет предъявлять вообще никаких бумаг или заранее регистрироваться, чтобы принять участие в этой программе. В процессе распознавания человеку всего лишь нужно встать напротив камеры, которая моментально отсканирует лицо и сверит его с базой данных.

Другая американская авиакомпания — Delta Air Lines — тоже собирается использовать распознавание лиц для упрощения аэропортовой рутины. На этот раз биометрический сканер будет применяться на стойках сдачи багажа. После печати ярлыка, который прикрепляется на сумку или чемодан, пассажира пригласят к автомату, оборудованному технологией распознавания лица, для сканирования и сверки с фотографией в документах.

Delta вложила в автоматизированную стойку регистрации багажа 600 тыс. долл. США. На эти средства в Международном аэропорту Миннеаполис/Сент-Пол летом 2017 г. установлены четыре подобных автомата.

Технологией заинтересовалась и Австралия. К 2020 г. страна планирует ввести биометрическую проверку пассажиров во всех австралийских аэропортах, включая сканирование отпечатков пальцев и лица. Несмотря на то что единой биометрической системы пока нет, потенциально в базу данных можно загрузить всю информацию о путешественниках, включая сведения о билетах, туристическую историю, возможные судимости и проч. В будущем искусственный интеллект на основе этих данных сможет определять, представляет пассажир угрозу или нет. Испытания системы пройдут в аэропорту Канберры, столицы Австралии. Целью проекта является автоматизация проверки 90% пассажиропотока.

Подобные испытания в этой области проводят финская авиакомпания Finnair, голландская KLM, а также международный аэропорт Париж — Шарль де Голль. В некоторых случаях система распознавания лиц будет только дублировать действия сотрудников службы безопасности, так как в настоящий момент она не показывает 100%-ного результата и иногда неточна.

На чемпионате мира по футболу 2014 г. в Бразилии полиция была оснащена солнечными очками со скрытыми камерами, которые от-

слеживали и идентифицировали по криминальной базе до 400 пар глаз в секунду на расстоянии до 12 миль (оптимизированы для работы на расстоянии 50 м). Очки — скрытая камера подключены по беспроводной сети к базе данных, которая сравнивает лица с профилями 13 млн эталонов и воспринимает 46 тыс. точек на лице для распознавания и идентификации совпадения.

Очки — скрытая камера могут не только идентифицировать преступников, но и отображать полицейскому дальнейшие указания к действию на мероприятии.

Ученые Института Макса Планка в Саарбрюккене в Германии демонстрируют способ идентификации человека по нескольким фотографиям, даже если на большинстве из них его лицо закрыто. Разработанная исследователями система, которую они называют «Безликая система распознавания», тренирует нейронную сеть с помощью множества фотографий, содержащих как закрытые от наблюдения, так и хорошо видимые лица, а затем использует эти знания, чтобы идентифицировать человека с закрытым лицам, ища сходства в области головы и на других участках тела. Точность системы меняется в зависимости от того, сколько есть фотографий в наборе с хорошо видимым изображением лица. Даже тогда, когда есть только 1,25 копий изображений полностью видимого лица человека, система способна идентифицировать скрытые от обзора лица с точностью 69,6%; если есть 10 копий изображений хорошо видимого лица, точность увеличивается до 91,5%.

В Швеции компания Axis создала первый в мире «умный» кодек (программный преобразователь сигнала), созданный для IP-видео и IP-видеонаблюдения. Камера служит только первым звеном, не только воспринимает и транслирует, но и интеллектуально обрабатывает изображение. Большое количество охранных агентств используют технологии аналитики как начальный уровень защиты, особенно ночью.

К 2020 г., ожидают в Axis, в видеонаблюдении предстоит все еще развивать качество изображения и светочувствительность. Но одновременно появятся камеры со встроенными системами аналитики или же со средствами передачи метаданных другой системе (метаданные — это, например, любые косвенные сведения о состоявшемся контакте двух лиц: с кем, когда, где, сколько длился, какой была тема и т. п.).

В Axis в числе продвинутых технологий называют систему контроля доступа, сетевую систему контроля дверей, IP-аудио.

Одним из самых важных новых направлений Axis считают то, что панорамные камеры заменят PTZ-камеры начального уровня. Угол обзора у такого прибора составляет 360°, и она одна может заменить

сразу четыре камеры. Еще одно новшество — *мультисенсор*. Мультисенсорная камера, которая имеет угол обзора 180°, появилась около года назад, но сейчас выпускаются и камеры с углом обзора 360°. Она позволяет следить за дорогой, за площадью, за зданием.

Французская компания Orange Labs разработала алгоритм, способный искусственно состаривать и омолаживать изображения лиц на фотографиях и устанавливать их сходство с изображением на исходном фото. Это первый алгоритм, который генерирует высококачественные изображения лиц в любой заданной возрастной группе с сохранением узнаваемости человека. Для его создания исследователи использовали две *генеративные состязательные нейросети*.

В процессе обучения нейросети проанализировали, как выглядят лица шести возрастных категорий (до 18 лет, 19—29, 30—39, 40—49, 50—59 и старше). Для этого в них загрузили по 5 тыс. фотографий людей из каждой возрастной категории. Таким образом нейросети узнали паттерны изображения, характерные для определенного возраста, и смогли применить их для состаривания и омоложения изображения любого лица.

Обученный алгоритм ученые испытали на 10 тыс. изображений из базы IMDB-Wikipedia, а затем проверили результат с помощью программы, которая сравнивает две фотографии и определяет, изображен ли на них тот же человек. В 80% случаев программа сумела идентифицировать людей, которых искусственно изменили на фотографи.

Технологию можно применять для розыска пропавших много лет назад, а также лиц, много лет скрывающихся от правосудия.

Китайская компания Baidu, занимающаяся созданием веб-сервисов, в начале 2017 г. успешно использовала технологию искусственного интеллекта для поиска человека. Пропавший ребенок воссоединился с семьей спустя 27 лет.

Сотрудничая с благотворительной группой baobeihuijia.com, занимающейся поиском пропавших людей, специалисты Baidu воспользовались программой распознавания лиц для того, чтобы вычислить местонахождение потерянного ребенка. Специалистам удалось выяснить, что 33-летний мужчина по имени Фу Гуи — это и есть маленький мальчик, похищенный после школы в далеком 1990 г.

Фу Гуи, как и его настоящая семья, был зарегистрирован на ресурсе Baidu. Мужчина выложил в Сеть свою фотографию в 10-летнем возрасте, а его родители искали мальчика по фотографии в четырехлетнем возрасте. Именно эти снимки и сопоставил искусственный интеллект. Кровное родство было подтверждено с помощью теста ДНК.

Компания Baidu использует базу из 200 млн изображений для того, чтобы совершенствовать работу системы распознавания лиц. Глава

компании Baidu Р. Ли внес предложение о создании централизованной базы данных со сведениями о пропавших детях, чтобы помочь воссоединиться еще многим семьям.

Еще в 2010 г. в России создана первая *полностью отечественная биометрическая система моментального распознавания личности в толпе*. Разработана она компанией-интегратором «Техносерв» и называется «Каскад-Поток». Система ничем не уступает зарубежным аналогам. Она идентифицирует личность в режиме реального времени путем сопоставления видеоданных, полученных, например, с камер видеонаблюдения, с изображениями в базах данных оперативных учетов. На все это уходит лишь доля секунды, а вероятность правильного распознавания достигает 94%.

В 2013 г. в петербургском метро в дополнение к уже действующим камерам, пунктам досмотра и рамкам-металлодетекторам внедрена «интеллектуальная» система видеонаблюдения. Базируется она на комплексе «КАРС» (комплексной автоматической розыскной системе). Он основана на системе «Интеллект», разработанной ФСБ России для розыска преступников. Решение состоит из сети видеокамер и серверов для обработки информации. Опираясь на биометрические данные, система способна автоматически распознавать людей в толпе и анализировать их сходство с лицами, занесенными в базу данных преступников и подозреваемых. Если сходство превышает 90%, система оповещает об этом полицейских. Мало того, система даже умеет следить за потенциальным правонарушителем с помощью нескольких камер.

В московском метрополитене уже создано *единое информационное радиопространство*, позволяющее сотрудникам подземки быстро связываться со службой охраны, станции и поезда оборудованы системой видеонаблюдения, на платформах установлены колонны экстренного вызова. Планируется оснастить каждую станцию дополнительными камерами, а также турникетами, способными распознать взрывные устройства, опасные предметы, отравляющие и радиоактивные вещества.

Заслуживает внимания и аппаратно-программный комплекс *биометрической идентификации лиц*, находящихся в розыске или представляющих оперативный интерес для органов внутренних дел (АПБИ «АТИГ»), который кроме лицевой геометрии при распознавании использует все четыре основных алгоритма биометрической идентификации, известные науке на сегодняшний день:

— алгоритм векторного сравнения (VFA);
— алгоритм сравнения иерархических графов лица (HGM);
— алгоритм анализа локальных особенностей лица (LFA);
— алгоритм анализа структуры кожного покрова лица (STA).

Этот аппаратно-программный комплекс разработан компанией «НТК ПрофИТ», транспортной полицией в инициативном порядке установлен в аэропорту Белгорода и с осени 2014 г. введен в эксплуатацию. Видеокамеры этого комплекса расположены на контрольном пункте, и система фиксирует всех пассажиров, пересекающих контрольный рубеж. При выявлении признаков сходства проходящего пассажира с разыскиваемым преступником (находящимся в розыске не только за преступления террористического характера, но и за иные противоправные деяния) система сигнализирует об этом сотрудникам полиции.

Уже первые месяцы эксплуатации аппаратно-программного комплекса принесли положительные результаты в отождествлении лиц, находящихся в федеральном розыске[1].

Российская компания «Вокорд» выпустила собственную систему дистанционного биометрического распознавания лиц Vocord FaceControl. «Вокорд» до сих пор работает с сервисами и устройствами, не связанными с распознаванием лиц.

Vocord FaceControl 3D работает с синхронными изображениями со стереокамер, строит 3D-модель лица в кадре (это занимает меньше секунды) и автоматически ищет совпадение полученной модели с моделями в имеющейся базе данных. Можно сопоставить 3D-модель и с обычными фотографиями.

Разработку проекта Vocord FaceControl 3D «Вокорд» начал с двухмерного распознавания лиц и сразу столкнулся с проблемой. Если человек отворачивался от камеры больше чем на 15° в любой плоскости, построить модель лица уже не удавалось. Поэтому инженеры «Вокорда» разработали систему, которая на основе синхронных снимков с нескольких камер строит трехмерную модель лица. Эта модель сравнивается с фотографией на пропуске или в доступной базе, система идентифицирует личность человека на снимке и сохраняет модель в архиве.

Но даже с переходом на 3D-моделинг получить хорошее качество снимков мешало плохое качество съемки стандартных обзорных камер. Крупным компаниям невыгодно было разрабатывать и производить камеры только для распознавания изображений — ниша была слишком узкой. «Вокорд» разработал свою технику на стыке классических обзорных камер и камер машинного зрения, которые обладали высокой чувствительностью, адаптировались к освещению, автоматически управляли объективом и делали снимки более четкими.

[1] См.: URL: https://m.cyberleninka.ru/article/n/ispolzovanie-avtomatizirovannyh-informatsionno-p (дата обращения: 19.01.2017).

Клиенту предлагается не отдельный «софт», а полноценный аппаратно-программный продукт — это стало прорывом в области распознавания лиц.

Компания NTechLab разработала сервис FindFace для поиска людей по фотографиям в «ВКонтакте». Сервис предлагает 30 бесплатных поисков ежемесячно, чтобы использовать его чаще и получить дополнительные настройки, нужно купить платную подписку. Большинство обычных пользователей познакомились с технологией распознавания лиц именно благодаря FindFace.

Правоохранительные органы уже используют технологию приложения FindFace, позволяющего связать фотографию человека, сделанную на улице, с его профилем в социальных сетях, для поиска преступников и нарушителей.

В мае 2016 г. создатель технологии А. Кухаренко договорился с правительством Москвы о тестировании технологии распознавания лиц на видео, которые снимают городские камеры. Их в столице очень много: 98 тыс. на подъездах, 20 тыс. во дворах.

Изображения людей, проходящих мимо камер, сверяются с загруженной в систему базой преступников или пропавших людей. Если на человеке показывается высокая степень сходства, то предупреждение об этом отсылается сотруднику полиции, который находится рядом. Алгоритм также сможет выделять отдельных людей в любой части города и находить их страницы в социальных сетях, из которых почти всегда можно узнать многое об их жизни, искать участников протестных митингов. Даже если человек забыл телефон дома, его перемещения по городу можно будет отследить, если он попадет в объективы камер, и связать с профилем в «ВКонтакте». В полиции используют технологию для раскрытия преступлений: берут фотографии, прогоняют через приложение, находят профили людей, видят, что они вчера были онлайн, делают запрос во «ВКонтакте», там выдают IP-адрес, откуда человек заходил.

Нейронная сеть дает набор признаков, по которому можно отличить одного человека от другого (цвет и форма глаз, мимика и др.). Но большинство признаков, которые выдает нейронная сеть, не видимы человеческому глазу. Точность определения изображения нейронной сетью составляет около 90%, а человеком — 25% (при объеме базы, например, 10 тыс. фотографий).

Алгоритм NTechLab дает возможность сравнивать пары лиц с 99% степенью точности и проводить поиск по достаточно большой базе фотографий менее чем за 0,3 секунды с точностью более 70%. Эта технология была признана лучшей на мировом чемпионате The MegaFace Challenge, организованном Университетом Вашингтона в

2015 г. В этом чемпионате приняли участие более ста команд со всего мира, в том числе и команда Google.

Для поиска человека по базе из 1 млрд фотографий такому алгоритму потребуется меньше 1 секунды. Подобная скорость поиска может решить множество задач не только в масштабах города, но и страны и даже мира, например, при поиске преступника в режиме реального времени. К преимуществам алгоритма помимо скорости поиска по базам фотографий глобального масштаба относится очень высокая точность распознавания. Это стало возможным благодаря глубинному обучению и правильно подобранной архитектуре нейронной сети.

Что ждет технологии 3D-распознавания лиц в России и в мире? С распространением автоматизации бизнес-процессов они получат все более широкое внедрение. Уровень качества технологий (точность распознавания сейчас превышает 95%) уже довольно высок, а экономия времени и ресурсов огромна. Чуть больше 10 лет назад фотографии предполагаемых преступников или банковских мошенников сравнивали с имеющейся базой изображений вручную, и после 30-й фотографии человек начинает работать медленнее и ошибаться гораздо чаще. Сегодня все системы распознавания лиц не просто автоматизированы, а используют искусственные нейронные сети. Это позволяет им работать с колоссальным объемом данных, сокращать количество ошибок и увеличивать скорость.

Компания IDX и разработчик — Центр речевых технологий в 2017 г. вывели на российский рынок сервис удаленной биометрической идентификации личности — по лицу и голосу. Партнеры рассчитывают, в частности, на принятие законопроекта, разрешающего такой способ идентификации для открытия счетов и выдачи кредитов в банках. К 2019 г. объем этого рынка в России может вырасти до 325 млн долл. США.

IDX добавила технологии аутентификации по лицу и голосу от компании «Центр речевых технологий» (входит в группу Газпромбанка) в свою систему управления идентификацией. Таким образом, эти компании смогут идентифицировать клиентов не только с использованием документов, но и с помощью биометрических данных. Для этого достаточно, чтобы человек один раз создал и сохранил с помощью специального приложения «цифровые слепки» голоса и лица в информационной системе (принадлежащей, например, банку, оператору связи, страховой компании, авиакомпании). С согласия клиента такие биометрические данные могут быть использованы для удаленного удостоверения личности всеми участниками рынка без нарушения цифрового суверенитета субъекта персональных данных.

Идентификация с использованием биометрии может занять более 50% рынка идентификации в течение ближайших пяти лет в кредитных организациях.

Проведение удаленной идентификации — обязательное требование «антиотмывочного» законодательства, сейчас предусматривающее только два способа — через подтвержденную учетную запись клиента на портале госуслуг и подтверждаемый особым способом набор персональных данных (паспортные данные и т. д.).

§ 8. Использование дронов против браконьеров, террористов и контрабандистов

Одними из первых, кто начал использовать беспилотники для охраны правопорядка, стали полицейские США. Федеральное управление гражданской авиации (FAA) авторизовало уже более 74 правительственных агентств по использованию беспилотников в воздушном пространстве страны, 17 из которых — правоохранительные. Наиболее известные среди них — Montgomery County в Техасе, Mesa County Sheriff's Department в Колорадо и Grand Forks из Северной Дакоты.

Разрешение FAA позволило силовикам абсолютно легально задействовать беспилотники для детального обследования мест преступления и поиска пострадавших людей. Однако американские полицейские активно привлекали вышеуказанные агентства к работе и раньше, до получения агентствами необходимых юридических прав. Известно, что с 2013 г. группа Grand Forks успела обработать около 30 запросов силовых структур, среди которых числятся четыре случая сбора данных об обстоятельствах самоубийств. С помощью дронов даже было обнаружено тело пропавшего охотника.

М. Гудман в книге «Будущее преступности» приводит такой пример: в 2013—2014 гг. на 80% сократился браконьерский отстрел слонов и носорогов в Африке. Секрет открывался просто. Американское правительство и корпорация Google в порядке гуманитарной помощи африканским странам, особо страдающим от браконьерства, предоставили подразделение патрульных и боевых дронов и обучили местный обслуживающий персонал обращению с этим грозным оружием. Единственной модификацией боевых дронов, используемых против браконьеров, было то, что с них были сняты огневые установки и установлены липучие сети и поражающие дротики со снотворным.

Полицейские США пытаются использовать дроны и в более сложных операциях, например таких, как наблюдение за потенциально опасными преступниками.

Британские полицейские начали использовать практически бесшумные мультикоптеры Black Hawk, позволяющие вести видеозапись со звуком.

Также стало известно о планах британской полиции использовать беспилотники в операциях по преследованию преступников. По различным оценкам, это обойдется силовикам намного дешевле и будет безопаснее, чем применение мотоциклов, машин и вертолетов. Покупка дрона и его длительная эксплуатация обойдутся в сумму меньшую, чем одна погоня с использованием вертолета (что возможно далеко не всегда) и двух полицейских машин. Кроме того, применение беспилотников никак не угрожает жизни полицейских.

О первом успешном применении квадрокоптера британской полицией стало известно еще в феврале 2010 г., когда с помощью аппарата AirRobot AR100B, оснащенного системой видеонаблюдения и тепловизионной камерой, силовики графства Мерсисайд на западе Англии смогли разыскать в густом тумане автомобильного вора. Подобные дроны применяются в Великобритании до сих пор. Известно, что технология аппарата первоначально разрабатывалась для нужд военной разведки. Он практически бесшумный и может работать ночью, передавая изображение в режиме реального времени.

В 2016 г. рабочая группа при Совете руководителей национальной полиции и Центр прикладной науки и технологий обсуждали возможность использования БПЛА для преследования подозреваемых, использующих двух- и четырехколесные транспортные средства для совершения преступлений, говорится в заявлении Службы столичной полиции Лондона.

В последнее время лондонские полицейские борются с ростом краж, совершенных грабителями на мопедах и мотоциклах. За 12 месяцев в британской столице подобным образом было украдено более 3 тыс. телефонов.

В то же время служба столичной полиции была вынуждена пересмотреть свою тактику преследований после инцидента, повлекшего за собой гибель 18-летнего Г. Хикса. Молодой человек погиб в погоне на высокой скорости, пытаясь на мопеде уйти от двух патрульных машин. Использование дрона может снизить шансы повторения подобного инцидента.

В конце 2015 г. дроны поступили на службу токийской полиции. Они вошли в специальный отряд по борьбе с другими дронами.

В настоящий момент беспилотники используются в правоохранительных органах целого ряда стран. Однако стоит отметить, что пока полицейские лишь оценивают потенциальные возможности подобных аппаратов. Так, в апреле прошлого года мэрия города Дубай запустила в небо дрона-полицейского, основной задачей которого ста-

ло слежение за экологическим порядком в местах отдыха и пустыне, а именно обнаружение тех, кто бросает мусор мимо урн. Подобные дроны-полицейские смогут быстро появляться в различных местах, снимая на камеру всех нарушителей. При этом особо отмечается, что если дроны хорошо себя зарекомендуют, силовики ОАЭ всерьез задумаются об использовании этих аппаратов для более сложных задач.

Во Франции и Японии беспилотники активно используются для дистанционного наблюдения за «скоплениями людей». Однако особый интерес вызывают отдельные подразделения, которые создаются в этих странах с целью борьбы со случаями несанкционированного использования дронов. В частности, полиция Токио совсем недавно заявила, что квадрокоптеры, нарушающие те или иные правила полетов, будут отлавливаться с помощью специальных дронов большого размера. Принцип работы здесь предельно прост: к большому квадрокоптеру снизу прикрепляется сеть размером примерно 2 × 3 м. Далее такой аппарат догоняет мелкие дроны-нарушители и, поймав их сетью, выносит из запретной зоны.

Впервые на практике подобный метод отлавливания дронов-нарушителей был опробован в феврале 2016 г. С этого момента «дроны-отлавливатели» исправно несут службу в рядах силовиков. Как сообщает полиция Токио, основная цель подобных работ — защита важных локаций «с учетом самых худших возможных сценариев», из чего можно сделать вывод, что речь здесь, возможно, идет не столько об обезвреживании дронов-папарацци, ведущих наблюдение за частной жизнью знаменитостей, сколько о противодействии серьезной угрозе со стороны дронов-террористов, вооруженных взрывчаткой. В современных условиях вещь весьма актуальная, особенно если учесть, что, по сообщению Министерства обороны РФ, уже известны случаи использования беспилотников, начиненных взрывчаткой, в Сирии. Также летом 2016 г. ФСБ предупреждала о планах террористов использовать дроны для совершения терактов в Европе.

Согласно сообщению пресс-центра МВД в России беспилотники различных типов стали использоваться полицейскими начиная с Олимпийских игр 2014 г. в Сочи. Дроны позволяют сотрудникам правопорядка эффективнее контролировать дорожную обстановку, проводить воздушную разведку, бороться с браконьерами и др. Ранее стало известно, что в июне 2016 г. дроны позволили сотрудникам авиационного отряда МВД по Республике Адыгея за полгода выявить более 150 нарушений ПДД. А в Красногвардейском и Майкопском районах беспилотники позволили обнаружить нарушения в сфере недропользования и незаконные вырубки лесов.

Серьезных правовых проблем по использованию беспилотников в рядах силовиков в нашей стране нет. Однако стоит отметить, что даже

этот факт не приводит к активному распространению дронов-полицейских в России — стражи порядка пока лишь присматриваются к возможности использования подобных аппаратов. При этом, по словам представителей МВД России, потенциальные возможности использования квадрокоптеров велики — они могут применяться полицейскими в различных ситуациях, вплоть до обезвреживания опасных преступников.

Израильская компания Laser Detect Systems (LDS) представила на выставке HLS&Cyber Expo в Тель-Авиве первый в мире беспилотник SpectroDrone, оснащенный датчиками для определения взрывчатки и самодельных взрывных устройств с безопасного расстояния.

Беспилотник использует разработанную компанией лазерную систему обнаружения взрывчатки и других опасных материалов в газах, жидкостях, порошках с расстояния в несколько километров. SpectroDrone способен выполнять эти задачи, имея оперативный радиус действия в три километра.

Предполагается, что новый аппарат можно применять для розыска баз и складов террористов, а также для обнаружения мин и фугасов в зонах локальных конфликтов. В настоящее время для этих целей используют системы обнаружения взрывчатки, размещаемые на автомобильной технике, а также носимые комплекты и служебных собак.

В стране помимо беспилотников планируется использовать инфракрасные камеры для поимки преступников и определения людей с холодным и огнестрельным оружием.

Мэр индонезийского Макасара заявил, что с 2017 г. преступников в городе будут ловить дроны. Город планирует запустить дроны, которые будут преследовать нарушителей во время погонь. Также аппараты будут оснащены системой распознавания лиц, чтобы иметь возможность определять находящихся в розыске в толпе. Макасар уже собирает различные биометрические данные своих жителей. Среди этих данных лица, отпечатки пальцев и сканы радужки глаза. «У нас есть биометрические данные всех наших жителей — 1,8 млн человек», — сказал мэр города. Мэр назвал общественную безопасность приоритетным направлением своей деятельности на весь 2017 г. Помимо дронов, рассказал он, некоторые улицы оснастят инфракрасными камерами, чтобы определить людей с холодным и огнестрельным оружием. В городе 80% преступлений совершают мотоциклисты, так что тепловые камеры направлены в первую очередь на них, так как определить оружие в автомобиле им не удастся.

Перспективным для полиции является компактный квадрокоптер Snipe («Бекас») производства компании Aero Vironment. Он проектировался в качестве дополнительного источника информации о противнике для пехотинцев армии США, внедряется с 2016 г.

Основное предназначение наноквадрокоптера — ведение визуальной разведки на близлежащем участке местности. Snipe оснащен четырьмя несущими винтами и весит всего 140 г. До момента применения дрон хранится в небольшом легком и прочном футляре.

Находясь в воздухе, Snipe производит видеосъемку с помощью оптической и инфракрасной камер в режиме реального времени с высоким разрешением, включая темное время суток. Мобильность камер обеспечивается встроенным механизмом поворота. Полученная картинка отображается на блоке управления оператора.

На борту беспилотника находится радиоаппаратура — встроенное УВЧ-радио и программно-определяемая радиосистема SDR, что делает его доступным для широкого круга покупателей.

Крошечный квадрокоптер, несмотря на свои габариты, уверенно чувствует себя при порывах ветра до 24 км/ч, не создает лишнего шума, что позволяет ему оставаться невидимым для противника даже с близкого расстояния. В случае потери радиосвязи Snipe автоматически возвращается к оператору.

Американский производитель нелетального оружия Taser International заявил, что готов предоставить полиции США беспилотники, оснащенные электрошокерами. Компания провела переговоры с представителями полиции на конференции в Сан-Диего.

Летом 2015 г. полиция США впервые в истории использовала робота для нейтрализации преступника. С помощью робота Remotec F-5, снабженного взрывчаткой, полицейские Далласа убили М. К. Джонсона, застрелившего пятерых полицейских во время уличной акции. «После этого инцидента нам поступали вопросы, возможно ли оборудовать оружием Taser автономное транспортное средство», — говорит представитель Taser International С. Таттл. Тазер — электрошоковое оружие нелетального действия с радиусом действия до 10 м, позволяющее проводить задержание правонарушителя с минимумом увечий.

В полиции США считают, что применение вооруженных тазером дронов может сохранить жизни сотрудников полиции во время опасных операций, однако признают, что этот вопрос остается дискуссионным. «Неприятие обществом идеи, что беспилотные летательные аппараты могут быть оборудованы каким-то видом оружия, — это препятствие, которое предстоит преодолеть», — говорит представитель департамента полиции Портленда П. Симпсон.

В исследовательской группе Police Foundation добавили, что такие технологии могут быть эффективным средством борьбы с преступностью, однако опасения правозащитников по этому поводу вполне обоснованны. «Многие люди обеспокоены тем, что если вы можете вооружить беспилотник электрошокером, то ничто не помешает вам

оборудовать его огнестрельным оружием», — говорит президент организации Дж. Буерман.

В 2015 г. власти штата Северная Дакота (США) приняли закон, позволяющий оснащать дроны нелетальным оружием. Полиция штата имеет право запускать беспилотники с электрошокерами, слезоточивым газом и травматическим оружием.

Вооруженные дроны могут стать по-настоящему грозной силой против преступников, и для этого в некоторых странах уже прорабатывается законодательная база. Например, законодательные органы Северной Дакоты еще в августе 2015 г. разрешили силовикам использовать любое оружие на беспилотниках, кроме огнестрельного. Иными словами, полицейские этого штата получили возможность дополнить дроны стреляющими электрошокерами, мощными распылителями газа и травматическим оружием, стреляющим резиновыми пулями.

В настоящий момент активно ведутся эксперименты по оснащению полицейских дронов газовыми баллончиками. Более того, французская компания Drone Volt серийно выпускает беспилотник TEAR GAS, который предназначен для распыления газа или перечного экстракта. Однако о подобном практическом использовании дронов ничего неизвестно — французские силовики пока используют эти аппараты лишь для дистанционного наблюдения за скоплениями людей.

Необходимо отметить, что потенциал использования беспилотников в рядах правоохранителей может быть ограничен не столько технически, сколько юридически. Так, американский Союз защиты гражданских свобод ACLU уже выразил опасение, что вооружение полицейских беспилотников может стать причиной необоснованного применения оружия, поскольку оператор дрона не присутствует на месте событий лично, а значит, не сможет адекватно ориентироваться по обстановке. Также в настоящий момент активно ведутся дискуссии с гражданскими правозащитными организациями по поводу законности использования дронов для наблюдения за подозреваемыми: является ли наблюдение за потенциальными преступниками вторжением в их частную жизнь и есть ли в подобных случаях какие-либо исключения?

§ 9. Применение роботов в профилактической и оперативной работе полиции

В начале 2016 г. стартап Knightscope из Пало-Альто штата Калифорния (США) разработал флотилию роботов, цель которой — обеспечение общественной безопасности.

Робот Knightscope K5 может видеть, слышать, ощущать и фиксировать запахи и использует этот набор возможностей для борьбы с преступностью. По задумке разработчиков, некоторых преступников отпугнет даже присутствие робота. Высота роботов достигает 1,5 м, вес — 136 кг. Для их передвижения используется технология, сходная с той, которая применяется в беспилотных автомобилях Google. K5 получает информацию с ряда сенсоров, анализирует ее и сопоставляет с законами и прочими данными, на основе которых может выявить факт какого-либо нарушения. Если робот обнаруживает подозрительную активность, он отправляет отчет уполномоченным лицам.

Машины записывают все, что происходит вокруг них (в радиусе 360°), на камеры с высоким разрешением — обычные и инфракрасные. При необходимости устройства могут использовать микрофон и динамики для общения оператора с прохожими. Роботы сопоставляют ряд предзаписанных параметров, например звуков, с потенциальными преступлениями — машины способны реагировать на выстрел, разбитое стекло и т. д. Если подозревается нарушение, робот сохранит гео-тэг, сделает фотографии, передаст видеопоток. Устройство запечатлит номера находящихся поблизости автомобилей, лица прохожих.

В Кремниевой долине для «охраны» кампусов и дата-центров были задействованы 24 устройства. Глобальная задача компании — создать систему предотвращения преступлений, основанную на роботах. Стартапу уже удалось собрать около 12 млн долл. США. Конечно, о замене охранников супермаркетов или сокращении полицейских речь не идет, однако устройства могут помочь при расследовании ряда преступлений и, возможно, предотвратить совершение некоторых из них.

Еще более умный патрульный робот создан в Китае — Anbot. Его главное отличие от калифорнийского аналога в том, что он не только замечает внештатную ситуацию, но и легко может в нее вмешаться, во-первых, применив электрошоковое оружие (есть подозрение, что где-то внутри робота также спрятан резервуар и для слезоточивого газа), во-вторых, погнавшись за нарушителем (машина разгоняется до 18 км/ч). Робот оценивает обстановку благодаря аудиодатчикам и камерам, размещенным со всех сторон. Кроме того, он способен реагировать на истошные крики жертв. Также у аппарата есть сенсорный экран, на котором можно нажать кнопку SOS и попросить об экстренной помощи. Робот весит всего 78 кг, зарядки аккумулятора хватает на 8 часов.

Также в Китае (Пекин) в рамках международной конференции 2015 г. «World Robot» состоялась презентация трех боевых роботов китайского производства, предназначенных для борьбы с терроризмом.

Один из них выполняет функцию химика-разведчика и сапера. В его обязанности входит обнаружение отравляющих и взрывчатых веществ, после чего он немедленно передает информацию военнослужащим спецподразделений. Второй робот будет заниматься утилизацией обнаруженных боеприпасов. Он весит всего около 12 кг и может транспортироваться на спине бойца. Основное его предназначение — помощь в индивидуальных миссиях.

В случае возникновения «горячих» ситуаций в дело вступит *тре*тий робот-боец. Он оснащен оружием небольшого калибра и гранатометом. В комплексе с современными прицелами робот сможет уничтожать террористов на дальней дистанции. Разработчиком является компания из Харбина HIT Robot Group. Среди потенциальных покупателей боевых роботов значится пекинская полиция. Набор из трех машин может обойтись в 1,5 млн юаней (235 тыс. долл. США).

В начале июля 2016 г. полицейского робота впервые использовали для убийства преступника: в Далласе был подорван подозреваемый в стрельбе по полицейским. Полиция решилась на использование робота для убийства преступника, так как тот отказался вести переговоры с правоохранительными органами. К гаражу, где скрывался стрелок, направили робота, обычно используемого для обезвреживания взрывных устройств. Робот не предназначен для убийства, но может переносить небольшое количество взрывчатки, потому что при необходимости подрывает большие подозрительные предметы. В этот раз к нему прикрепили примерно 450 г пластичного взрывчатого вещества военного назначения C-4. Этого хватило, чтобы при детонации на небольшом расстоянии от преступника нанести ему травмы, несовместимые с жизнью. Сам робот практически не пострадал: повреждена только длинная «рука», переносящая дополнительный груз.

По словам эксперта в области военных технологий и автора книги «Изменяющийся характер войны» П. Сингера, американцы впервые использовали такую тактику внутри страны, но за рубежом американские роботы уже убивали. В Ираке военные много раз использовали в качестве самостоятельного взрывного устройства недорогого робота MARCbot (он стоит около 15 тыс. долл. США). В Далласе взрыв устроил более мощный робот Remotec Androx Mark V A-1, который был приобретен полицией в 2008 г. за 151 тыс. долл. США. Помимо обезвреживания бомб он может разбивать окна, распылять слезоточивый газ, перерезать провода, пилить и проделывать отверстия. Робот не самостоятелен, каждое действие контролирует человек за пультом.

Помимо Remotec Androx Mark V A-1 в американской полиции «служит» и большое количество других роботов. Их особенности проанализировал журналист В. Воронин[1].

Наиболее популярны роботы, подрывающие подозрительные предметы и деактивирующие взрывные устройства; их использование военными заметно увеличилось во время войн в Афганистане и Ираке.

Стоимость подобных роботов колеблется от 10 до 150 тыс. долл. США — в зависимости от механизмов поиска взрывчатых веществ и дополнительных функций. Как правило, полиция выбирает компактные модели, чтобы они могли пролезать под машины и проникать в различные помещения. Часто роботы снабжены микрофонами и двумя-четырьмя камерами, передающими изображения в центр управления, а также мощными сенсорами, определяющими химический состав бомбы. Полиция активно использует модель PackBot 510 с детектором Fido, который «нюхает» бомбу и быстро определяет тип взрывчатки. От этого зависит выбор дальнейшей тактики — подрыв или обезвреживание на месте.

Иногда роботы помогают полиции не рисковать и действовать максимально аккуратно при захвате заложников. Простые модели, снабженные панорамными камерами и мощными микрофонами, позволяют оценить количество заложников и обстановку внутри здания, вести переговоры с захватчиками, а также доставлять еду и медикаменты по требованию.

Для этих целей используются даже роботы, которые обычно не работают «курьерами». В апреле 2015 г. аппарат, обезвреживающий бомбы, передал телефон и пиццу мужчине, который планировал совершить самоубийство и представлял угрозу для остальных, потому что держал в руке нож. Через час после получения пиццы и начала телефонного разговора с полицейскими мужчина бросил нож и сдался.

Сложные роботы-разведчики, например BOZ 1, могут вскрывать двери, проламывать стены и разбивать стекла, чтобы проникнуть в закрытые помещения. Еще более мощный робот Dragon Runner, разработанный компанией QinetiQ по заказу Пентагона, умеет подниматься по лестницам, двигать механической рукой, фиксировать движения людей и подслушивать их разговоры на довольно большом расстоянии. Однажды в штате Северная Каролина этот робот пробрался к вооруженному мужчине, который заперся в своем доме и не сдался даже после пуска слезоточивого газа. Первый аппарат преступник разбил на мелкие кусочки, но когда приехал второй, между мужчиной и полицией начались переговоры (через камеру и микрофон у робота).

[1] См.: Meduza. 2016. 14 июля.

Другой робот в 2013 г. в Альбукерке штата Нью-Мексико подобрался к мужчине, который забаррикадировался в своем доме и угрожал самоубийством. Аппарат при помощи манипулятора сбросил с него одеяло, чтобы убедиться, что тот не вооружен, и только после этого в дом вбежали полицейские.

Отдельный тип роботов помогает полиции оценивать обстановку в условиях очень плохой видимости, например в абсолютной темноте. Перед тем как направить наряд полиции в темную квартиру, где могут скрываться подозреваемые, нередко активируют робота Throwbot XT (36 см в длину, вес — 0,5 кг, шум — всего 22 Дб). Благодаря специальной оптической системе он позволяет оператору, сидящему за пультом управления, четко видеть то, что недоступно человеческому взгляду. Это существенно упрощает проведение рискованных полицейских операций.

В некоторых районах Киншасы — столицы Демократической Республики Конго — автомобильным движением управляют человекоподобные роботы высотой более 2,5 м. Они работают как светофоры на перекрестках с особенно беспорядочным движением. Зеленые, желтые и красные огни размещаются на спине, груди и руках роботов. На их туловищах закреплены четыре камеры наблюдения, фиксирующие нарушение ПДД и оперативно отправляющие данные в полицейский участок. Каждый робот, изготовленный из алюминия и питающийся от солнечной батареи, стоит 21 тыс. евро.

Уже в ближайшее время в эксплуатацию попадут сразу несколько роботов, которые сильно изменят проведение полицейских операций. Например, в Германии в 2019 г. должен появиться робот-сапер нового уровня. Предполагается, что сотрудникам правоохранительных органов даже не придется приближаться к подозрительным предметам, оставленным на улице: машина сама просканирует вещи и создаст 3D-модель закрытой сумки. Работа аварийно-спасательных служб сведется к просмотру готовых кадров на компьютере: инженеры должны будут проанализировать полученную картинку, сделать выводы о том, есть ли там бомба, и дать роботам следующие задания в зависимости от ситуации.

В Дубае в 2020 г. должны появиться самостоятельные роботы-полицейские. Они будут следить за безопасностью на улицах, в парках и торговых центрах. Правда, все роботы будут безоружны, так что в экстренной ситуации не смогут вмешаться, а только передадут информацию полиции. Роботы, наделенные искусственным интеллектом, должны будут также предоставлять справочную информацию на шести языках, уметь шутить и заботиться о детях.

Кроме того, полиция Дубая запустила в 2017 г. на улицы города автономную систему наблюдения O-R3, состоящую из четырехколесных роботов и дронов. Систему наблюдения разработала сингапурская компания Otsaw Digital. Колесный робот выглядит как маленький автомобиль. Он оснащен многочисленными 3D- и 2D-лазерными сканерами, IMU-сенсорами и ультразвуковыми датчиками, GPS-навигаторами и передатчиками данных на большие расстояния. Благодаря системе избегания препятствий он может безопасно передвигаться по дорогам и тротуарам. В задней части робота встроена выдвижная платформа, с которой происходит запуск дрона, если необходимо установить наблюдение с воздуха. От наземного робота дрон может удаляться на расстояние 100 м. Система O-R3 оснащена алгоритмами распознавания лиц и автомобилей (в частности, номерных знаков), она поможет полиции Дубая находить преступников и «подозрительных лиц». Первоначально ее будут использовать в туристических районах Дубая.

В ближайшие годы у полиции появятся и специальные роботы для убийства. В Израиле в мае 2016 г. представили модель, которая выглядит чуть крупнее игровой приставки, но без проблем имитирует известный самозарядный пистолет Glock 26 на колесиках.

И совсем из области фантастики, которая фактически стала явью, — киборги. Исследователи из Университета Вашингтона в Сент-Луисе превращают насекомых в киборгов, которых можно отправить куда угодно для вынюхивания взрывчатки. Работы ведутся по заказу ВМС США. Исследователи изучают, как насекомые анализируют запахи. Обнаружено, что саранча может идентифицировать конкретные запахи, которые их научили обнаруживать, даже при наличии посторонних запахов. Насекомые-киборги будут более эффективными, чем роботы, потому что они используют массу природных датчиков.

Даже самые передовые миниатюрные химические устройства используют всего несколько датчиков. Вместе с тем, если посмотреть на антенну насекомых, то там несколько сотен тысяч датчиков различных типов. Для того, чтобы превратить обычную саранчу в машину по поиску взрывчатки, инженеры планируют вживить в ее мозг электроды, чтобы подключиться к ее антеннам в виде усиков и расшифровать электрические сигналы. Так как операторы должны получать информацию, собранную насекомыми, исследователи также разрабатывают крошечный рюкзачок, который может передавать данные. На приемнике будет загораться красный светодиод при наличии взрывчатых веществ, в то время как зеленый свет сигнализирует об отсутствии угрозы.

И, наконец, инженеры планируют нанести татуировку на крылья насекомых с помощью биосовместимого шелка, способного преобразовывать свет в тепло. Лазер, который, вероятно, будет в рюкзаке, позволит оператору контролировать действия киборга. Фокусирование лазера на левом крыле обеспечит движение насекомого влево, и наоборот. Насекомое будет функционировать так же, как дистанционно управляемый дрон.

§ 10. Новые технологии прогнозирования преступного поведения

Как известно, одним из основателей антропологической теории преступности был итальянский криминалист Ч. Ломброзо. Он считал, что преступников можно определить по особым чертам: скошенный лоб, специфическое строение ушных раковин, различные асимметрии лица и длинные руки. Чтобы доказать свою точку зрения, он провел много измерений. Поскольку Ломброзо был по образованию врачом, он провел сотни сравнительных вскрытий мозга умерших преступников и обычных людей.

Долгие годы теория Ломброзо и неоломброзианцев подвергалась жесточайшей критике.

Ученые из Шанхайского университета транспорта Сяолинь Ву и Си Джан использовали различные алгоритмы машинного зрения, чтобы изучить лица преступников и законопослушных граждан, а затем проверили, может ли машина выявить разницу.

В отличие от человека компьютерный алгоритм классификации изображений совершенно не отягощен багажом субъективности, не имеет эмоций и неточностей, связанных с прошлым опытом, расовыми, религиозными или политическими предпочтениями, полом, возрастом и т. д., он не утомляется и не страдает от последствий недостатка сна или пищи, пишут китайские ученые, предлагая свою автоматизированную систему предсказания преступных наклонностей на основе снимков лиц.

Ученые использовали четыре подхода к автоматической классификации объектов: метод опорных векторов; метод «k» (ближайших соседей); логистическую регрессию; использование сверточной нейронной сети. Этим алгоритмам они предложили набор из 1856 фотопортретов мужчин (китайцев возрастом от 18 до 55 лет, без растительности на лице, шрамов и татуировок, с нейтральным выражением лица), из которых 730 попадали под подозрение полиции или имеют криминальный опыт (235 — в связи с тяжкими преступлениями). Ву и Джан отдельно отмечают, что лица преступников были показаны на

обычных фотографиях, а не снимках, сделанных для полицейских архивов.

Пройдя обучение, все четыре алгоритма продемонстрировали определенную способность выделять лица преступников среди законопослушных граждан. Лучше других показала себя *сверточная нейронная сеть*, точность предсказаний которой достигла почти 90%. Более того, авторы указывают на конкретные черты, якобы свойственные криминальной личности, включая более выраженный изгиб верхней губы, меньший угол между уголками рта и кончиком носа, увеличенное расстояние между внутренними уголками глаз.

Китайские ученые отмечают, что хотя компьютерный алгоритм действительно «не отягощен багажом субъективности», от нее может страдать сама подборка лиц, на которой он обучался и проверялся. Исследователи могли, сами того не осознавая, отобрать лица, удобные для такой интерпретации. Судьи могут выносить более строгие решения по отношению к людям с более суровыми и жестокими чертами лица.

Естественно, работа китайских ученых нуждается в более серьезном обосновании и доработке. Нужно повторить эксперимент с людьми разного возраста, пола, этнических групп и увеличить количество наборов данных. Это должно помочь разрешить некоторые спорные моменты. Например, Ву и Чжан считают, что криминальные лица можно разделить на четыре подгруппы, а законопослушные только на три. Почему так происходит? И как этот алгоритм будет работать с другими группами людей? В то же время исследование ученых поднимает важные вопросы. Если результат действительно выдерживает критику, то как его объяснить? Почему у лиц преступников гораздо больше отклонений по сравнению с обычными людьми? Как люди определяют преступников? Это врожденное или приобретенное умение? Если ученым удастся ответить на эти вопросы, тогда, возможно, работа ученых даст новый виток развития антропометрии уголовного или иного характера.

Кроме того, власти Китая заинтересовались сферой предикативного анализа, технологии *лицевого распознавания* и другими аспектами, связанными с ИИ, которые можно будет использовать для предотвращения будущих преступлений. Анализируя модели поведения, власти будут уведомлять местную полицию о потенциальных преступниках.

Компания Cloud Walk, офис которой находится в Гуанчжоу, проводит машинное обучение систем лицевого распознавания, а также анализа и оценки больших массивов данных для отслеживания уровня риска потенциальных преступников. Те, кто является завсегдатаями магазинов по продаже оружия или часто посещает различные

транспортные узлы, вероятнее всего, будут отмечены системой. Под «подозрение» могут попасть даже посетители хозяйственных магазинов, потому как эти места рассматриваются властями зонами «повышенного риска»[1].

«Конечно, если кто-то покупает кухонный нож, то здесь нет ничего криминального. Но если этот же человек вдогонку покупает мешок и молоток, то для системы он станет подозрительным», — отметил представитель компании Cloud Walk в разговоре с журналистом Financial Times.

Программное обеспечение Cloud Walk уже связано по сети с базой данных полиции более 50 городов и провинций и может отмечать подозрительных личностей в режиме реального времени. В стране также уже действует система «личностной переидентификации», использующейся в качестве меры предупреждения преступлений: система способна производить идентификацию людей в различных местах, даже если они носят разную одежду.

«Мы можем использовать систему re-ID для поиска подозрительных людей, блуждающих туда-сюда в одной и той же зоне или носящих маски», — прокомментировал изданию Financial Times Лень Бяо, профессор сферы образного распознавания в Пекинском университете авиации и космонавтики.

Китай, безусловно, является одним из тех идеальных мест, где подобные технологии могли бы использоваться в полной мере. Благодаря использованию более 176 млн камер наблюдения правительство располагает огромными исчерпывающими базами данных о своих гражданах. Другими словами, страна предоставляет огромную площадку для сбора всей интересующей информации и, следовательно, позволяет эффективно обучать свои ИИ-системы, при этом без каких-либо юридических препятствий.

Но это далеко не единственные пути, с помощью которых Китай может расширить способности своих ИИ-систем. Правительство этой страны на днях объявило о масштабном, продуманном и профинансированном плане по превращению Китая в мирового лидера сферы ИИ к 2030 г.

Также ИИ может использоваться для защиты личной жизни, информации о здоровье, финансовом положении, в качестве средства для предотвращения хакерских атак. Искусственный интеллект может отвечать за камеры безопасности, роботов-охранников и помочь в создании более эффективных военных технологий; будет способен как минимум на 90% снизить количество случаев автокатастроф.

[1] См.: URL: https://hi-news.ru/technology/kitaj-xochet-vnedrit-texnologiyu-predskazaniya-prestuplenij.html.

Будущих преступников можно выявить по строению их мозга в детстве. Развитие и «здоровье» мозга уже в трехлетнем возрасте может предсказать будущий риск оказаться в больнице или в тюрьме. Об этом сообщается в статье, опубликованной журналом Nature Human Behaviour.

Работающий в Университете Дьюка (штат Северная Каролина) нейрофизиолог А. Каспи и его соавторы проанализировали данные по более чем 1000 жителей Новой Зеландии, которые родились в 1972—1983 гг. и в трехлетнем возрасте проходили всестороннее медицинское, психологическое и социальное обследование. Ученые выяснили и их личные истории вплоть до возраста 38 лет, в том числе данные о приводах в полицию и об обращениях к врачам.

Это позволило выделить группу из 22% людей, которые создают максимальную «нагрузку» на общество. Члены этой небольшой группы ответственны за 36% обращений к страховщикам, 57% ночных посещений больниц, 66% получения государственных пособий, 77% оставленных детей, 78% выписанных лекарств и 81% преступлений. По замечанию Каспи и его коллег, это распределение в целом следует известному принципу Парето, согласно которому 20% усилий дают 80% результата.

Ученые обнаружили, что попадание человека в эту группу можно с высокой надежностью предсказать еще в трехлетнем возрасте по результатам обследования развития нервной системы, языковых, моторных и познавательных навыков, а также особенностей характера. Несколько лет назад Каспи и его соавторы предложили обобщать результаты таких тестов в единый p-фактор, индикатор нормального развития и состояния мозга. И, хотя на положение человека в группе риска влияют также социоэкономические факторы, фактор «здоровья мозга» (так его назвали авторы статьи) может служить хорошим предсказателем будущей судьбы.

Стоит отметить, что предсказательная сила этого показателя не слишком велика. В частности, риск оказаться в группе риска для трехлеток из бедных семей с низким уровнем «здоровья мозга» всего на 19% выше, чем для их сверстников с хорошими показателями развития.

Согласно статье, опубликованной в начале 2017 г. в издании Guardian, группе неврологов из Виргинского медико-технологического исследовательского института Карильон удалось установить разницу в работе мозга настоящих преступников и тех, кто совершает правонарушение непреднамеренно. Для этого достаточно лишь проанализировать снимок головного мозга.

В ходе серии экспериментов ученые просканировали мозг 40 человек, каждого из которых просили пронести через воображаемую границу чемодан. Часть участников осведомили, что в чемодане лежат наркотики. Остальные не знали, что проносят через «границу», но подозревали, что делают что-то незаконное. Кроме того, ситуация осложнялась еще и тем, что никто из испытуемых не знал, будут ли «на таможне» проводить полный досмотр, а «таможенники» случайно выбирали людей, которых этому досмотру необходимо подвергнуть. В ходе опытов специалисты под руководством Р. Монтегю провели МРТ-сканирование головного мозга всем участникам эксперимента. Как выяснилось, во время совершения преступления у тех людей, кто осознанно нарушал закон, и у тех, кто был «преступником поневоле», проявляют активность нейроны из абсолютно разных отделов головного мозга.

Как утверждают эксперты, естественно, подобное исследование требует дальнейших изысканий, и на основании данных, полученных всего от 40 человек, рано делать какие-либо выводы. Но в случае успеха подобное обследование сможет дать новый инструмент для раскрытия и предупреждения преступлений.

Овчинский Владимир Семенович

Криминология цифрового мира

Учебник для магистратуры

Издание не подлежит маркировке
в соответствии с п. 1 ч. 2 ст. 1 ФЗ № 436-ФЗ

ООО «Юридическое издательство Норма»
101990, Москва, Колпачный пер., 9а
Тел./факс: (495) 621-62-95. E-mail: norma@norma-verlag.com
Internet: www.norma-verlag.com

ООО «Научно-издательский центр ИНФРА-М»
127282, Москва, ул. Полярная, д. 31в, стр. 1
Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29
E-mail: books@infra-m.ru. Internet: www.infra-m.ru

Редактор *Л. А. Мункуева*
Корректор *Н. Н. Циркова*
Разработка серии: *А. Л. Бондаренко*
Верстка: *А. Ю. Виноградов*

Подписано в печать 00.00.17
Формат 60×90/16. Бумага офсетная
Гарнитура «Ньютон». Печать цифровая
Усл. печ. л. 22,00. Уч.-изд. л. 21,49
Тираж 150 экз. Заказ №

По вопросам приобретения книг обращайтесь:

Отдел продаж «ИНФРА-М» (оптовая продажа)
127282, Москва, ул. Полярная, д. 31в, стр. 1
Тел.: (495) 280-15-96. Факс: (495) 280-36-29
E-mail: books@infra-m.ru

Отдел «Книга — почтой»
Тел.: (495) 280-15-96 (доб. 246)
