Академия управления МВД России

Ю. В. Гаврилин

О НАУЧНЫХ ПОДХОДАХ К ПРОБЛЕМЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕСТУПНЫХ ЦЕЛЯХ

научно-практическое пособие

Москва · 2021

УДК 343.9
ББК 67.408
Г12

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *И.В. Сподынюк,* врио начальника управления по контролю за оборотом наркотиков УМВД России по Псковской области; *А.Н. Волков,* заместитель начальника УМВД России по Кировской области – начальник следственного управления.

Гаврилин Ю. В.

Г12

О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях: научно-практическое пособие. Москва : Академия управления МВД России, 2021. – 72 с.

ISBN 978–5–907187–86–3

В работе проанализированы тенденции цифровой трансформации преступности, выделены факторы, ее обуславливающие. Рассмотрено влияние пандемии COVID-19 на состояние преступности в сфере информационно-телекоммуникационных технологий. Представлен обзор основных цифровых технологий, используемых при подготовке, совершении и сокрытии преступлений. Научно-практическое пособие содержит прогноз развития тенденций криминальной деятельности с использованием цифровых технологий и предложения по их нейтрализации.

При подготовке научно-практического пособия использованы данные, предоставленные подразделениями центрального аппарата МВД России, а также территориальными органами МВД России.

Автор выражает особую признательность компании Group-IB.

УДК 343.9
ББК 67.408

ISBN 978– 5–907187–86–3

Содержание

1. Тенденции цифровой трансформации
преступности и факторы, ее обуславливающие 4

2. О влиянии пандемии COVID-19 на состояние преступности
в сфере информационно-телекоммуникационных технологий. 31

3. Обзор основных цифровых технологий, используемых
при подготовке, совершении и сокрытии преступлений 44

4. Прогноз развития тенденций криминальной деятельности
с использованием цифровых технологий и предложения
по их нейтрализации 59

Список литературы 68

1. Тенденции цифровой трансформации преступности и факторы, ее обуславливающие

В соответствии со Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, одной из основных угроз государственной и общественной безопасности является деятельность, связанная с использованием информационно-коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе.

Согласно Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, национальная безопасность Российской Федерации в информационной сфере признается ключевым аспектом безопасности государства и охватывает всю совокупность информации, объектов информатизации, информационных систем, сайтов в сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности.

Цифровые технологии привели к значительному преображению и успеху во многих отраслях, особенно благодаря использованию сети Интернет, однако они также подвергают организации и отдельных лиц целому ряду новых рисков, возникающих в результате атак с использованием цифровых интерфейсов.

Цифровизация практически всех сфер жизни граждан, общества и государства изменила масштабы и само понимание преступности, актуализировала вопрос защиты информационных систем и информационной инфраструктуры.

3 марта 2021 г. Президент Российской Федерации Владимир Владимирович Путин на ежегодном расширенном заседании коллегии МВД России поставил задачу органам внутренних дел Российской Федерации «защитить граждан и добросовестный бизнес, который активно осваивает цифровое пространство. Для этого важно своевременно информировать людей о способах защиты от мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел. И, конечно, нужно наладить более четкое взаимодействие с банковским сообществом, интернет-провайдерами, операторами сотовой связи.

В целом показатели раскрываемости кибер- и других видов преступлений должны год от года расти не за счет статистики, не за счет бумажной отчетности, а благодаря кропотливой работе «на земле». От этого зависит реализация важнейшего правового принципа – неотвратимости наказания, а значит, и вера людей в справедливость, в силу закона, в способность государства защитить безопасность человека.

Министр внутренних дел Российской Федерации генерал полиции Российской Федерации Владимир Александрович Колокольцев в своем выступлении на указанном заседании обратил внимание на то, что «криминальные деяния, совершенные с использованием IT-технологий, составляют все бóльшую долю в общей структуре преступности: сегодня она достигла 25 %. Динамика ежегодного прироста фиксируется последние несколько лет. Данные изменения являются отражением глобальных тенденций. Своеобразным катализатором здесь стала пандемия, которая повлекла масштабный уход в онлайн многих сфер жизнедеятельности общества. Благодаря принимаемым мерам, количество раскрытых в 2020 г. IT-преступлений увеличилось в 1,5 раза»[1].

По данным ФКУ «ГИАЦ МВД России», в 2020 г. зарегистрировано 510 396 (+73,4 %) преступлений, совершенных с использованием информационно-коммуникационных технологий (киберпреступлений). В общей структуре преступности доля таких преступлений составила 25,0 %, что существенно превышает уровень 2019 г. (14,5 %). Вместе с тем раскрываемость таких преступлений пока недостаточна и в 2020 г. составила 18,6 % (в 2019 – 22,2 %).

Более половины зарегистрированных киберпреступлений относится к категориям тяжких и особо тяжких (всего – 267 613; 52,4 %).

Наиболее широкое распространение получили преступные деяния с использованием информационно-телекоммуникационной сети Интернет (300 337; 58,8 %), средств мобильной связи (218 739; 49,9 %), расчетных (пластиковых) карт (190 167; 37,3 %). Отмечается увеличение доли IT-преступлений, связанных с незаконным сбытом наркотических средств, психотропных веществ или их аналогов (ст. 228.1 УК РФ) с 8,3 % в 2019 г. до 9,2 % в 2020 г. среди всех преступлений, совершенных в сфере информационно-телекоммуникационных технологий. В структуре

[1] Владимир Путин принял участие в ежегодном расширенном заседании коллегии Министерства внутренних дел Российской Федерации. URL: http://kremlin.ru/events/president/news/65090 (дата обращения: 18.03.2021).

киберпреступлений преобладают: мошенничества (41,2 %), кражи (34,0 %) и деяния в сфере незаконного оборота наркотиков (9,2 %).

Тенденция существенного роста киберпреступлений наблюдается по всем федеральным округам. Наиболее значительно число таких преступлений возросло в г. Санкт-Петербурге (19 488; +780,0 %), г. Москве (54 707; +132,0 %), Новосибирской области (11719; +130,6 %). Она обусловлена значительными изменениями в жизнедеятельности в условиях мероприятий, проводимых в рамках ограничения распространения новой коронавирусной инфекции COVID-19.

Сохраняется высокая латентность киберпреступлений, которая обусловлена недостаточной цифровой грамотностью населения, распространением программных средств анонимизации личности, обеспечивающих сокрытие информации о совершившем преступление лице, распространение программ для мобильных устройств, позволяющих перехватывать сетевой трафик, расшифровывать имена и пароли пользователей[1].

Сказанное дает основания констатировать, что в настоящее время происходит процесс цифровой трансформации преступности, состоящий в принципиальных изменениях как в механизме совершения «традиционных» преступлений, возникших в «доцифровую» эпоху, так и в возникновении новых видов преступлений, непосредственно связанных с развитием информационно-телекоммуникационных технологий и использованием технических средств сбора, обработки, хранения компьютерной информации и ее передачи по линиям связи[2]. На этом фоне в уголовное законодательство введен ряд специальных составов, призванных обеспечить защиту информационной сферы от противоправных посягательств, в частности: кража, совершенная с банковского счета, а равно в отношении электронных средств платежа (п. «г» ч. 3 ст. 158 УК РФ); мошенничество с использованием электронных средств платежа (ст. 1593 УК РФ); мошенничество в сфере компьютерной информации (ст. 1596 УК РФ); преступления в сфере компьютерной инфор-

---

[1] Аналитический обзор «Комплексный анализ состояния преступности в Российской Федерации по итогам 2020 года и ожидаемые тенденции ее развития». Москва: ФГКУ «ВНИИ МВД России», 2021. С. 46–49.

[2] Согласно ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

мации (гл. 27 УК РФ) и др. Кроме того, такой квалифицирующий признак, как использование при совершении преступления информационно-телекоммуникационных сетей, включая сеть Интернет, включен законодателем в 15 статей Особенной части УК РФ.

На фоне распространения новой коронавирусной инфекции COVID-19, в уголовное законодательство были дополнительно введены новые составы преступлений, устанавливающие ответственность за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 2071 УК РФ) и за публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия (ст. 2072 УК РФ). Публичный характер распространения заведомо ложной информации может проявляться в использовании для этого информационно-телекоммуникационных сетей, в т. ч. мессенджеров (WhatsApp, Viber и др.), в массовой рассылке электронных сообщений абонентам мобильной связи, и т. п.[1]

Следствием цифровой трансформации преступности являются следующие тенденции.

Первая тенденция. Развитие дистанционных способов совершения преступлений, при которых исключается непосредственный контакт соучастников как между собой, так и с потерпевшими. Взаимодействие субъектов преступления с потерпевшими или третьими лицами при совершении преступлений дистанционным способом осуществляется опосредованно, с использованием средства связи и информационных ресурсов сети Интернет, в первую очередь таких, как социальные сети, электронная почта, сервисы мгновенных сообщений, онлайн-продажи и пр.[2]

Наиболее ярко данная тенденция проявляется на примере преступлений, связанных с незаконным сбытом наркотических средств и психотропных веществ. При этом, если до 2014 г. сбыт наркотических средств осуществлялся преимущественно способом «из рук в руки», то с развитием цифровых технологий он стал осуществляться с использованием электронных торговых площадок в теневом сегменте сети Интернет (преимущественно на платформе

---

[1] Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2: утв. Президиумом Верховного Суда Российской Федерации от 30 апреля 2020 г.

[2] *Gavrilin Yu.V., Pavlichenko N. V., Vasilieva M.A.* The Remote Approach of Distribution of Objects Withdrawn from Circulation: Means, Legislation Issues, Solutions // Studies in Systems, Decision and Control. Vol. 181. Big Data-Driven World: Legislation Issues and Control Technologies. Chapter 8. C. 85–93.

Hydra[1]), принимающих оплату посредством криптовалюты (обеспечивая тем самым анонимность сделок) и передающих информацию о местонахождении заранее оборудованных тайников – «закладок», в которых находятся запрещенные препараты. Для привлечения новых и удержания постоянных клиентов организаторами дистанционного сбыта наркотиков проводятся специальные маркетинговые акции, осуществляются бесплатные доставки «пробников», предоставляются скидки, осуществляются иные маркетинговые акции.

По данным ГУУР МВД России, практически 70 % зарегистрированных преступлений, связанных с незаконным оборотом оружия, совершено с использованием ресурсов сети Интернет, что обусловлено возможностью дистанционно и анонимно координировать незаконные операции, в т. ч. из-за рубежа[2]. Это в полной мере относится и к незаконному сбыту поддельных денег, ценных бумаг и документов.

Не менее ярко обозначенная тенденция проявляется и при совершении хищений денежных средств с банковских счетов физических лиц путем направления в банки распоряжений о перечислении средств потерпевших на подконтрольные субъектам преступления счета. При этом названные распоряжения создаются от имени клиента в электронном виде с использованием систем дистанционного банковского обслуживания и на основе конфиденциальной информации, необходимой для осуществления перевода, получаемой методами «социальной инженерии», состоящей в применении психологических приемов, направленных на введение потерпевшего в заблуждение относительно истинной цели поступающего ему телефонного вызова и личности звонящего. Целью такого воздействия является получение от потерпевших реквизитов банковских

[1] Гидра (Hydra) – крупнейшая торговая площадка, созданная в 2016 г., осуществляющая услуги по реализации не только наркотических средств и психотропных веществ, но и фальшивых купюр, банковских карт, поддельных документов, специального оборудования для слежения, доступа к компьютерной информации и т. д. Платформа содержит в себе интернет-магазины, предлагающие запрещенные к гражданскому обороту товары и услуги, а также предложения о трудоустройстве: от закладчиков и химиков (для изготовления наркотиков) до дизайнеров и промоутеров (для рекламы и распространения предлагаемых товаров/услуг). В магазинах, расположенных на этой площадке, размещена информация о виде, весе, цене предлагаемого наркотического средства, способах связи и оплаты. Стоимость открытия интернет-магазина на площадке Гидра – 450 долл. США, ежемесячная аренда – 100 долл. (+5 % с каждой покупки). По данным ГУ МВД России по г. Москве, на электронной торговой площадке Гидра происходит свыше 90 % всех незаконных операций с наркотиками, совершенных в интернет-пространстве, ориентированном на московский регион. См.: письмо ГУ МВД России по г. Москве от 26 августа 2020 г. № 1/11957.

[2] Письмо ГУУР МВД России от 17 августа 2020 г. № 6/4-6705.

карт и иной конфиденциальной информации, необходимой для осуществления перевода денежных средств на счет злоумышленников.

В противоправной деятельности, осуществляемой дистанционным способом, активно используется мобильная связь и SIP-телефония[1] с функцией подмены телефонных номеров. С использованием средств мобильной связи или интернет-телефонии осуществляется выведывание у потерпевших конфиденциальной информации, необходимой для совершения транзакций от их имени, побуждение их к самостоятельному совершению перевода денежных средств на подконтрольные мошенникам счета, а также иные противоправные действия. Телефонные вызовы потерпевшим совершаются якобы от имени представителей банков, сообщающих о некой «подозрительной транзакции», либо о некоем «выигрыше», для получения которого требуется «уплатить налоги».

Широкое распространение получили звонки от якобы представителей правоохранительных органов или медицинских учреждений, которые сообщают потерпевшему о том, что его близкий родственник якобы попал в сложную жизненную ситуацию (ДТП, причинение телесных повреждений и т. д.). Для вхождения в доверие мошенники могут использовать названия реальных подразделений и фамилии сотрудников. При этом мошенники, как правило, убеждают жертву не сообщать об этом другим родственникам и не перезванивать на телефон родственника, «якобы попавшего в беду». Одновременно потерпевшему сообщаются инструкции по переводу денежных средств: либо на электронный кошелек, либо на счет банковской карты, либо путем передачи наличных курьеру.

Не менее распространены мошеннические схемы, основанные на покупке или продаже товаров на электронных торговых площадках («Авито», «Юла» и т. п.), или с использованием социальных сетей («ВКонтакте», «Одноклассники», «Instagram» и др.). Злоумышленники связываются с продавцом и предлагают перечислить денежные средства в счет предоплаты приобретаемого товара. При согласии потерпевшего мошенник просит сообщить реквизиты банковской карты (номер, срок действия, данные владельца, защитный код), которые впоследствии используются при совершении хище-

[1] SIP-телефония отличается от мобильной связи тем, что для ее использования не требуется самого телефонного аппарата (оконечного оборудования) и идентификационного модуля (сим-карты), а также подключения к базовой станции подвижной связи. Соединение устанавливается через специальное положение по протоколу IP. При использовании анонимайзеров установление реального IP-адреса, примененного для соединения, носит затруднительный характер.

ния в системе дистанционного банковского обслуживания, в которую осуществляется вход от имени потерпевшего[1].

В целом следует констатировать вариативность и постоянное совершенствование способов совершения преступлений с учетом расширения спектра платежных систем, программных и технических средств. С появлением новых мер социальной поддержки звонки потерпевшим совершаются под предлогом оказания содействия в оформлении кредита или государственных пособий. Нередко возникновение новых цифровых сервисов влечет за собой появление преступлений, совершаемых с их использованием. Так, появление сервисов доставки на таких популярных электронных торговых площадках, как «Авито», «Юла» и других, повлекло за собой рост так называемого «спама», совершаемого в отношении пользователей этих сайтов и представляющего собой рассылку сообщений, обещающих пользователям получение приза, выигрыша или денежного вознаграждения при условии прохождения некоего опроса, участия в якобы рекламной акции и прочего, с целями получения «комиссионного сбора», «налогового платежа». При этом целью подобных рассылок является получение данных банковской карты потерпевшего для последующего совершения хищения находящихся на ней денежных средств.

Механизм типичного дистанционного мошенничества, сопряженного с применением методов «социальной инженерии», выглядит следующим образом: клиенту банка сообщают о якобы обнаруженной службой безопасности попытке взлома его личного кабинета в системе дистанционного банковского обслуживания или проведения несанкционированной транзакции. Для большей убедительности ему сообщается достоверная информация: ФИО, паспортные данные, номер карты и другие сведения, которые заблаговременно приобретаются в неиндексируемом сегменте сети Интернет (Даркнет) или заказываются в соответствующих телеграмм-каналах. Если клиент использует двухфакторную аутентификацию, то у него запрашивают секретный код, присланный банком в СМС, поскольку только так якобы можно отменить несанкционированную транзакцию. Узнав у пользователя конфиденциальный CVV-код, необходимый для совершения онлайн-платежей, злоумышленники могут совершить интернет-покупки на сумму, не требующую проверки через одноразовый пароль в СМС, или продать скомпрометированные данные карт. Конечной

[1] Письмо УМВД России по Смоленской области от 31 августа 2020 г. № 28/939.

же целью мошенников является перевод денег со счета потерпевшего на подконтрольный им счет (электронный кошелек).

Вариацией данного способа является следующая схема: лицо, представляющееся сотрудником банка, сообщает потерпевшему о попытке неизвестных лиц оформить на его имя кредит. Когда потерпевший сообщает, что заявок на кредит он не подавал, ему предлагается для отмены операции назвать пароли, поступившие к нему в СМС-сообщениях, после чего происходит списание денежных средств со счета потерпевшего.

Дистанционный способ совершения вымогательства основан на требовании перечисления денежных средств за разблокирование данных, содержащихся в информационной системе, подвергшейся воздействию вредоносной программы, нераспространении порочащей потерпевшего информации, полученной путем взлома его персональных страниц в социальных сетях, получении переписки в сервисах мгновенных сообщений (мессенджерах) или электронной почты.

Значительное количество мошенничеств, совершенных дистанционным способом, реализуется посредством взлома аккаунтов в социальных сетях и размещения просьбы якобы от имени известных потерпевших лиц одолжить им денежные средства, принять финансовое участие в некоем коммерческом проекте и пр.

Широкое распространение имеют факты размещения объявлений на электронных торговых площадках («Авито», «Юла» и др.) о продаже товаров ненадлежащего качества, не соответствующих заявленным характеристикам, или вовсе не принадлежащих предлагающим их лицам. Отмечается значительное число злоупотреблений доверием, направленных на побуждение граждан к совершению гражданско-правовых сделок (покупка фальсифицированных товаров, работ и услуг без намерения их выполнения, получение несуществующих выигрышей, участия в финансовых пирамидах, перевод предоплаты за несуществующий товар и т. д.). При этом у потерпевшего формируется осознанное желание осуществления денежного перевода конкретному получателю, он самостоятельно вводит в систему действующие аутентификаторы, в связи с чем пресечение подобных способов существующими антифрод-системами банков затруднительно.

Наконец, имеют место случаи хищения денежных средств с банковского счета граждан путем создания и направления в банк распоряжений о перечислении денежных средств с использованием конфиденциальной информации, необходимой для осуществления платежа, незаконно полученной в финансово-кредитной

организации, либо с использованием технических (программных) уязвимостей информационных систем дистанционного банковского обслуживания.

Принципиальной особенностью дистанционных способов совершения преступлений является территориальное разнесение мест совершения действий, образующих объективную сторону преступления, мест наступления общественно опасных последствий, мест легализации денежных средств, полученных преступным путем, а также мест нахождения кредитно-финансовых организаций, операторов связи, интернет-провайдеров, услуги и инфраструктура которых используются при совершении преступлений. Названное обстоятельство негативно отражается на сроках получения информации об обстоятельствах совершенного деяния, формирования на их основе доказательств в порядке, установленном уголовно-процессуальным кодексом, а в конечном счете – на обеспечении соблюдения разумных сроков уголовного судопроизводства.

Вторая тенденция. Совершенствование способов сокрытия преступлений, основанных на использовании сервисов анонимизации личности в цифровом пространстве. Анонимизиция направлена на подмену либо блокирование информации, позволяющей установить лицо, совершившее интернет-соединение (прежде всего, IP-адрес и MAC-адрес) при отправлении того или иного сообщения посредством электронной почты, социальной сети, сервиса мгновенных сообщений и пр. Она обеспечивает сокрытие подлинных данных о личности пользователя сети Интернет и направлена на воспрепятствование установлению лица, совершающего те или иные действия в виртуальном пространстве, включая противоправные действия.

Современная преступность, будучи хорошо осведомленной о методах и средствах оперативно-розыскной, уголовно-процессуальной и экспертно-криминалистической деятельности, широко применяет возможности интернет-сервисов, обеспечивающих анонимизацию действий в цифровом пространстве, используя при этом особенности технического построения и функционирования сети Интернет. Сказанное в первую очередь касается осуществления электронных платежей при осуществлении криминальных взаиморасчетов, а также переводов денежных средств, направленных на легализацию (отмывание) доходов, полученных преступным путем[1] и их беспрепятственный вывод за пределы юрисдикции Рос-

[1] Правовую основу деятельности по противодействию легализации (отмыванию) доходов, полученных преступным путем, составляют: Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности

сийской Федерации. Появление многочисленных программно-технических средств и способов анонимизации личности пользователя сети Интернет обеспечивает эффективное сокрытие следов противоправной деятельности, включая следы финансовых транзакций, направленных на вывод денег за рубеж, их обналичивание, инвестирование в легальный сектор экономики и др.

Совершению преступлений с использованием информационно-телекоммуникационных технологий способствует развитый криминальный рынок услуг по продаже идентификационных модулей средств мобильной связи (сим-карт), зарегистрированных на «фирмы-однодневки», без проведения процедуры идентификации абонента. Многочисленные объявления о продаже таких модулей содержатся в неиндексируемом сегменте сети Интернет (Даркнет), где также осуществляется анонимная вербовка соучастников для осуществляющих наиболее рискованные элементы механизма преступления: размещение запрещенных веществ в тайниках («кладмены»), снятие наличных денежных средств в банкоматах («дроперы») и др.

Третья тенденция. Использование криптовалют в криминальных взаиморасчетах. Сокрытие следов финансовых транзакций активно осуществляется посредством конвертации денежных средств, номинированных в национальных денежных единицах, в виртуальную валюту, оборот которой не подконтролен для уполномоченных государственных органов, что препятствует реализации механизмов противодействия легализации (отмыванию) доходов, полученных противоправным путем, применительно к подобным цифровым финансовым активам.

В общем виде криптовалюту можно определить как имущество в электронной форме, созданное с использованием криптографических средств, и учитываемое в распределенном реестре цифровых транзакций в соответствии с установленными правилами его ведения.

и о финансировании терроризма (заключена в г. Варшаве 16 мая 2005 г., ратифицирована Федеральным законом Российской Федерации № 183 от 26 июля 2017 г.); Федеральный закон Российской Федерации от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»; Указ Президента Российской Федерации от 13 июня 2012 г. № 808 «Вопросы Федеральной службы по финансовому мониторингу» (вместе с «Положением о Федеральной службе по финансовому мониторингу») и другие нормативные правовые акты. Уголовная ответственность установлена ст. 174 УК РФ «Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем», ст. 174.1 УК РФ «Легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления». Административная ответственность установлена ст. 15.27 КоАП РФ «Неисполнение требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

С точки зрения FATF (The Financial Action Task Force), под виртуальной валютой понимается средство выражения стоимости, представленное в цифровом формате и выступающее в качестве средства обмена, либо расчетной денежной единицы, либо средства хранения стоимости и при этом не подпадающее под понятие законного платежного средства, т. е. не являющееся официально действующим законным средством платежа при расчетах с кредиторами[1].

Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» цифровая валюта определяется как «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам».

Закон допускает обращение на территории Российской Федерации цифровой валюты при соблюдении определенных условий. При этом устанавливается запрет на прием цифровой валюты в качестве оплаты товаров (работ, услуг).

Использование криптовалют при осуществлении криминальных взаиморасчетов, в совокупности с осуществлением маскировки реальных IP-адресов программами-анонимайзерами, негативно сказывается на деятельности правоохранительных органов по выявлению, раскрытию и расследованию преступлений и ограничивает их возможности по использованию в процессе доказывания информации о финансовых операциях (включая наличные и безналичные расчеты, кассовые операции, перевод или размен денежных средств, обмен одной валюты на другую и т. п.) лиц, в отношении которых имеются достаточные основания полагать об их причастности к криминальной деятельности.

---

[1] См.: Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ. URL: https://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf (дата обращения: 05.06.2021).

Следует подчеркнуть, что складывающиеся тенденции развиваются стремительно: в настоящее время использование криптовалют стало основным средством финансовых расчетов в сфере незаконного оборота наркотических средств, психотропных веществ, а также иных объектов, изъятых из гражданского оборота. Растущая популярность криптовалюты предопределена в первую очередь ее свойствами: возможностью дробления одной единицы до одной стомиллионной доли, круглосуточным осуществлением транзакций, трансграничным характером, проверкой валидности операции, безвозвратностью транзакций, анонимностью переводов, дефляционным характером, децентрализованной эмиссией и др.[1]

При этом следует отметить, что криминальные взаиморасчеты – не единственная сфера противоправного использования криптовалют. В последнее время участились случаи хищений денежных средств путем мошенничества под видом продажи криптовалюты. Желание получить легкий заработок на обещанном мошенниками росте обменного курса криптовалюты обеспечивает поступление к ним многочисленных взносов доверчивых граждан. Потенциальным потерпевшим посредством мессенджеров и социальных сетей направляются письма с предложениями быстрого заработка. Клиента вводят в заблуждение относительно доходности вложений: «инвестиции» кажутся ему очень прибыльными. Впоследствии потерпевшие оказываются лишенными возможности вывести денежные средства или иным способом распорядиться ими: когда пользователь пытается вывести свой доход, ему под различными предлогами в этом отказывают. В итоге они теряют вложенные средства.

Четвертая тенденция. Рост масштабов межрегиональной и трансграничной преступности, использование при совершении преступлений сетевой инфраструктуры, расположенной за пределами Российской Федерации. В настоящее время совершение преступлений дистанционным способом, сопряженное с использованием методов «социальной инженерии», совершается, преимущественно, жителями субъектов Российской Федерации (в т. ч. отбывающими наказание по приговору суда в учреждениях уголовно-исполнительной системы), расположенных на значительном удалении от места жительства потерпевшего, либо из стран СНГ, преимущественно Украины. Более того, зачастую участники самой преступной груп-

[1] *Гаврилин Ю. В., Шурухнов В. А.* О правовых предпосылках применения отдельных способов сокрытия преступлений, совершенных с использованием информационно-коммуникационных технологий // Академическая мысль. 2017. № 1. С. 39–43. URL: https://mvd.ru/upload/site120/folder_page/010/368/829/Akademicheskaya_mysl_1-2017.pdf (дата обращения: 19.03.2021).

пы могут также находиться в разных регионах Российской Федерации. При этом широкие возможности свободного использования серверных мощностей и информационных ресурсов, расположенных в иностранных юрисдикциях, существенным образом препятствуют установлению лиц, совершивших преступления, и выяснению обстоятельств расследуемого события, подрывая базовый принцип неотвратимости наказания. Так, серверы почтовых ящиков @google.com, @yahoo.com, @aol.com и ряда других находятся на территории США. Там же располагаются хостинг-провайдеры крупнейших ресурсов, таких как FaceBook, iCloud, Instagram, Skype и др. Даже при наличии на территории Российской Федерации официального представительства иностранной компании, располагающего сведениями о ее российских пользователях, возможности получения информации о них весьма ограничены. Так, запросы, направляемые по каналам Интерпола в интернет-компании США, зачастую остаются без исполнения в связи с позицией американского законодательства о неприкосновенности частной жизни, согласно которой основанием для предоставления информации по электронным коммуникациям и компьютерной информации (IP-адреса, электронные почтовые адреса, log-файлы доступа к сайтам в сети Интернет и др.) является соответствующее постановление суда США, вынесенное по уголовному делу. Получение последнего возможно в рамках направления запроса о правовой помощи (ст. 453–456 УПК РФ), процедура направления и исполнения которого может составлять до двух лет, что существенно сокращает возможность применения данного механизма по уголовным делам (за исключением особо тяжких преступлений)[1].

Сложившаяся ситуация усугубляется текущей геополитической обстановкой. Традиционно, с рядом Европейских государств (Великобритания, Бельгия, Нидерланды, Польша и страны Прибалтики) уровень международного сотрудничества в правоохранительной сфере находится на невысоком уровне. В последние годы практически свернуто международное сотрудничество с Украиной и Грузией, что превращает данные государства в своего рода преступные анклавы, чем, естественно, активно пользуются преступники в своих противоправных целях[2].

---

[1] Письмо ГУУР МВД России от 17 августа 2020 г. № 6/4-6705.

[2] *Гаврилин Ю.В.* Криминалистика: угрозы и вызовы современности // Криминалистика и новые вызовы современности (58-е криминалистические чтения): сборник статей Всероссийской научно-практической конференции. Москва: Академия управления МВД России, 2018. С. 62.

Пятая тенденция. Формирование криминального рынка противоправных услуг в информационно-телекоммуникационной сфере (cybercrime-as-a-service), связанных с предоставлением в аренду компьютерных сетей, зараженных вредоносным программным обеспечением (ботнетов) и используемых, например, при организации DDoS-атак, рассылке фишинговых писем и пр. Широкое распространение имеет рынок услуг по неправомерному доступу к частной переписке в мессенджерах и социальных сетях, посредством электронной почты. Данные услуги открыто рекламируются в мессенджере Telegram и обсуждаются на Darknet-форумах.

Шестая тенденция. Использование технологий искусственного интеллекта в противоправной деятельности. Искусственный интеллект представляет собой комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека[1]. В настоящее время широкое распространение приобрели интеллектуальные технологии синтезирования речи, видеоизображений, с помощью которых можно создавать аудио- и видеозаписи для манипуляции людьми[2], распространения фальшивых новостей и видеосюжетов. Данные технологии могут быть применены и при совершении преступлений с использованием методов «социальной инженерии».

Отмеченные процессы и тенденции в области цифровой трансформации преступности являются закономерным следствием влияния комплекса факторов, включающих в себя экономические, технологические, социальные и правовые.

К числу экономических факторов следует отнести следующие:

– повышение ценовой доступности технических средств создания, хранения и обработки цифровой информации (стационарных и портативных компьютеров, смартфонов) при одновременном улучшении качества услуг информационной инфраструктуры (расширение зоны устойчивого радиопокрытия организаций сотовой связи, повышение уровня проникновения сети Интернет в частные домохозяйства). По данным Международного союза электросвя-

---

[1] См.: подп. «а» п. 5 Национальной стратегии развития искусственного интеллекта на период до 2030 года, утв. Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».

[2] *Коробеев А. И., Дремлюга Р. И., Кучина Я. О.* Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. № 3. С. 421.

зи, с 2005 г. число интернет-пользователей ежегодно росло на 10 % и в 2019-м, предположительно, достигло 4,1 млрд чел.[1] По итогам 2018 г. доступ к сети Интернет в домашних хозяйствах (в процентах от общего числа домашних хозяйств) в России имели 76,6 %, а размер абонентской платы за пользование услугами мобильного доступа к сети Интернет в среднем составил около 1 % от среднедушевых денежных доходов[2];

– ускорение темпов развития цифровой экономики, основной движущей силой которой являются процессы сбора, обработки и использования цифровых данных, возникающих в процессе физической, социальной или экономической деятельности физических лиц или организаций. По различным экспертным оценкам, размер цифровой экономики составляет, по оценкам, от 4,5 до 15,5 % мирового ВВП[3]. Формируются бизнес-модели, обеспечивающие получение прибыли от привлечения внимания аудитории к той или иной информации (так называемая «экономика внимания», проявлением которой является контекстная реклама, прогнозирование поведения человека и его потребительского выбора в той или иной ситуации). Увеличивается объем предоставления государственных услуг в электронной форме. Возможностью зарегистрировать юридическое лицо дистанционно, путем отправления документов на сайт ФНС России или в единый регистрирующий орган по месту регистрации посредством сети Интернет, активно пользуются недобросовестные налогоплательщики для регистрации фирм на подставных лиц, используя их в дальнейшем в противоправной деятельности[4]. Кроме того, все большее число коммерческих организаций переходит на онлайн-режим взаимодействия с заказчиками. При этом повышение зависимости нормального функционирования эко-

[1] URL: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf (дата обращения: 05.06.2021).

[2] *Абдрахманова Г. И., Вишневский К. О., Гохберг Л. М. и др.* Цифровая экономика: 2020 : краткий статистический сборник. Москва: НИУ ВШЭ, 2020. С. 16, 18.

[3] Доклад о цифровой экономике 2019. Создание стоимости и получение выгод: последствия для развивающихся стран. Организация объединенных наций. Женева. 2019. URL: https://unctad.org/en/PublicationsLibrary/der2019_overview_ru.pdf (дата обращения: 06.06.2021).

[4] Документы для образования (реорганизации) юридического лица поступают в электронном виде на сайт ФНС РФ, после чего отправляются в территориальный налоговый орган по месту расположения либо регистрации налогоплательщика. При этом установить IP-адрес, с которого направлен пакет документов, не представляется возможным. При подаче заявлений посредством направления через сайт ИФНС России регистрирующий орган зачастую сообщает об отсутствии технической возможности предоставления IP-адресов отправителей данных пакетов, поскольку точка доступа не передает исходных IP-адресов приложению.

номики от устойчивости информационной инфраструктуры повышает риски наступления кризисных последствий при осуществлении атак на ключевые ее объекты, а защита киберпространства от противоправных посягательств выходит на уровень ключевых государственных приоритетов;

– рост числа интернет-сервисов онлайн-продаж, преимуществами которых по сравнению с «традиционными» формами продаж в организациях торговли или сферы услуг является удобство для потребителей в заказе и получении товаров, работ, услуг. При этом наблюдается рост числа сайтов-«клонов», визуально сходных до степени смешения с популярными сервисами доставки («Авито», «Юла» и др.). Злоумышленники копируют цветовое исполнение, шифры, формат текста, фирменный стиль и логотипы интернет-сайтов известных организаций, в результате чего визуально отличить оригинальный сайт от сайта-клона практически невозможно. Механизм совершения преступления в данном случае включает в себя создание копии официального сайта, который отличается только доменным именем, покупку доменных имен со схожим наименованием, которые служат запасными вариантами размещения сайта-клона, направление на сайт-клон трафик через e-mail рассылки, СМС-сообщения, мессенджеры и платное продвижение в поисковой выдаче, подмена оригинальных платежных реквизитов на свои, обработка поступающих запросов и прием платежей от обманутых клиентов, которые считают, что покупают продукцию у официальной компании, прекращение какого-либо общения с обманутыми клиентами, перенос сайта на запасной домен, если основной домен блокируется.

К числу технологических факторов следует отнести активное развитие:

– технологий высокоскоростного доступа в сеть Интернет. В период с 2010 по 2020 гг. число домохозяйств в России, имеющих высокоскоростной доступ в Интернет, увеличилось с 48,4 % до 76,6 %[1]. Приведенный показатель не учитывает осуществление доступа в Интернет с использованием мобильной связи, что становится наиболее распространенным способом установления интернет-соединения. Развитие сетей мобильной связи кардинально увеличило технические возможности услуг по передаче данных. Так, например, стандарт мобильной радиосвязи 2G, созданный в 1992 г., позволяет осуществлять передачу данных со скоростью до 220 Кбит/с. Следующий стандарт мобильной радиосвязи 3G,

[1] *Абдрахманова Г. И., Вишневский К. О., Гохберг Л. М. и др.* Указ соч. С. 16.

применяемый с 2000 г., способен передавать данные со скоростью до 7,2 Мбит/с. Распространенный в настоящее время стандарт связи для мобильных телефонов 4G способен передавать данные со скоростью до 1000 Мбит/с при задержке до 20 миллисекунд (хотя на практике редко скорость передачи данных превышает 100 Мбит/с)[1]. В сотовых сетях нового поколения 5G данные будут передаваться со скоростью от 20 Гбит/с в секунду с задержкой до 4 миллисекунд. Вместе с тем сети нового типа менее централизованы и в меньшей степени базируются на физическом оборудовании. Это затрудняет защиту от атак и реагирование на инциденты[2];

– систем дистанционного банковского обслуживания. По данным Института статистических исследований и экономики знаний НИУ ВШЭ, 39 % российских интернет-пользователей совершают онлайн финансовые операции. Еще более эта практика распространена в Финляндии (94 %), Швеции (91 %) и Эстонии (90 %). Больше трети россиян (35 %) используют Интернет для заказа товаров и услуг. Намного чаще – в Великобритании (83 %), Швеции (78 %), Германии (77 %)[3];

– программных средств мгновенного обмена сообщениями (мессенджеров, (от англ. *messenger* – курьер), предназначенных для обмена текстовыми, звуковыми, фото – и видео сообщениями в реальном времени через сеть Интернет, а также организации групповых текстовых чатов или видеоконференций. В отличие от электронной почты, обмен сообщениями между пользователями идет в реальном времени, при этом у пользователя существует возможность видеть, подключены ли к сети в данный момент абоненты, занесенные в список его контактов. Наиболее популярными в настоящее время в России программами мгновенного обмена сообщениями являются WhatsApp, Viber, Telegram, VIPole, Jabber и др. Особенностью современных мессенджеров, обуславливающих их высокую популярность, в т. ч. и в криминальной среде, является использование ими криптографических алгоритмов защиты информации, обеспечивающих сквозное шифрование передаваемых пользователями сообщений и предоставляющих доступ к исходному тексту только отправителю и получателю. При этом электронные ключи для рас-

---

[1] *Буснюк Н. Н., Мельянец Г. И.* Системы мобильной связи. Минск: БГТУ, 2018.

[2] *Wheeler T., Simpson D.* Why 5G Requires New Approaches to Cybersecurity Racing to Protect the Most Important Network of the 21st Century (Почему 5G требует новых подходов к гонкам кибербезопасности, чтобы защитить самую важную сеть XXI века). URL: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/ (дата обращения: 07.06.2021).

[3] URL: https://issek.hse.ru/digec2020 (дата обращения: 07.06.2021).

шифровки сообщений создаются и хранятся на устройствах пользователей, а не на внешних серверах. В процессе отправки сообщения программным обеспечением отправителя и получателя по специальным алгоритмам генерируется уникальный ключ, дешифрование которого за разумное время представляется затруднительным, что делает передаваемую информацию труднодоступной для третьих лиц. Кроме того, за использование мессенджеров, с пользователей, как правило, не взимается плата, что делает их альтернативой телефонной связи;

– социальных сетей – интерактивных многопользовательских сайтов, контент (содержание) которых наполняется их посетителями с возможностью указания какой-либо информации об отдельном человеке, по которой аккаунт (страницу) пользователя смогут найти другие участники сети[1]. Значительный импульс развитию социальных сетей придало широкое распространение технологий беспроводной высокоскоростной передачи данных для мобильных устройств, а также снижение стоимости подобных услуг. В итоге аудитория социальных сетей ежегодно демонстрирует высокие значения процентов прироста[2]. Функциональные возможности социальных сетей по обеспечению взаимодействия участников путем просмотра профилей, размещения комментариев, иного контента (текстовых, графических, фото-, видеофайлов), отправки личных сообщений предоставляют широкие возможности для манипулирования общественным сознанием путем размещения недостоверной информации по социально значимым вопросам, а также стимулирования протестной активности, что способно привести к массовым нарушениям правопорядка и общественной безопасности;

– технологий искусственного интеллекта, позволяющих создавать более сложное вредоносное программное обеспечение, обладающее возможностями самообучения и способное осуществлять поиск решений без заранее заданного алгоритма. Примечательно, что в последнее время интернет-магазины, занимающиеся преступ-

---

[1] *Чернец В., Базлова Т., Иванова Э.* Влияние через социальные сети / под общ. ред. Е. Г. Алексеевой. Москва: Фонд «ФОКУС-МЕДИА», 2010. С. 29.

[2] По данным компании Brand Analytics, по состоянию на конец 2019 г. в России число активных авторов (пользователей, оставивших хотя бы одно публичное сообщение за месяц) в социальных сетях составило 49 млн, которые написали 1,3 млрд публичных сообщений (постов, репостов и комментариев). Самой популярной социальной сетью остается «ВКонтакте»: в ноябре 2019 г. 30,7 млн ее пользователей написали 556 млн публичных сообщений, в среднем по 18 сообщений на автора. На втором месте «Instagram» с небольшим отставанием по количеству авторов (27,6 млн). Замыкают тройку «Одноклассники», где 6,5 млн активных авторов. URL: https://br-analytics.ru/blog/social-media-russia-2019/ (дата обращения: 10.06.2021).

ной деятельностью в сфере незаконного оборота наркотиков, все чаще отказываются от интернет-сайтов и переходят на платформу организатора обмена мгновенными сообщениями – мессенджера Telegram, который позволяет использовать специальные программы, автоматизирующие процессы «Bot», не имеющие привязки к конкретному лицу, но в то же время предоставляющие возможность общения с потребителями. Для интернет-магазина бот является оптимальной системой, т. к. исключает присутствие живого оператора, не требует постоянного нахождения человека за компьютером, автономно контролирует наличие товаров по регионам и местам оборудованных тайников-закладок, значительно снижает количество точек соприкосновения между участниками сообществ, а также затрудняет выявление их деятельности;

– Интернета вещей – бытовых приборов, подключенных к Интернету и управляемых дистанционно в соответствии с заданными алгоритмами. Ориентируясь на рост объемов продаж подобных гаджетов, производители зачастую оптимизируют расходы на обеспечение защищенности данных устройств, в результате чего они становятся средствами совершения DDoS-атак и незаконного проникновения в атакуемую информационную систему;

– технологий «умных городов». Оно формирует зависимости систем жизнеобеспечения населенных пунктов, в первую очередь, объектов электроэнергетики, транспорта, связи, водоснабжения и прочего, от функционирования информационных систем, обеспечивающих управление ими.

Кроме того, в число факторов технологического характера, способствующих совершению преступлений с использованием информационно-телекоммуникационных технологий, входят:

– применение интернет-провайдерами технологии преобразования IP-адресов NAT (от англ. *Network Address Translation*), обеспечивающей экономию их емкости и возможность передачи информации из множества внутренних адресов в один внешний; возникает проблема получения у отдельных провайдеров сведений, позволяющих идентифицировать конкретного пользователя по используемому им в момент совершения преступления IP-адресу;

– использование в противоправных целях программ удаленного доступа (AnyDesk, Supremo Remote Desktop, TeamViewer, Ammyy Admin и т. д.) позволяющих получить доступ к внутренней информации на устройстве, в т. ч. к файлам, установленным приложениям дистанционного банковского обслуживания. С помощью данных программ, которые находятся в открытом доступе (в т. ч. на сервисах приложений для мобильных устройств «PlayМаркет», «AppStore»),

появляется возможность удаленно совершать переводы денежных средств на подконтрольные счета различных банков, расположенных на территории РФ, и на счета заграничных банков. После чего, используя все те же программы, преступники полностью удаляют информацию с устройств, которая могла бы помочь в установлении личности злоумышленника.

Вцелом,отмечаяопределяющееевлияниетехнологическихфакторов на состояние преступности в рассматриваемой сфере, следует отметить, что при совершении преступлений с использованием информационно-телекоммуникационных технологий злоумышленникам, как правило, нет необходимости обладать глубокими познаниями в данной сфере. Они используют уже готовые технологии, программные продукты и технические решения, которые создаются профильными организациями (включая международные корпорации) в сфере IT-технологий, приспосабливая их для совершения противоправных действий. Сотрудникам правоохранительных органов, напротив, необходимо в совершенстве владеть данными технологиями для понимания локализации цифровых следов и механизма их образования. Последнее обстоятельство повышает требования к образовательному уровню сотрудников правоохранительных органов в обозначенной сфере.

К социальным факторам относятся:

– недостаточная цифровая грамотность населения, что наглядно иллюстрируется следующими показателями: в 2018 г. только 2,7 % населения в возрасте от 15 лет и старше имели навыки изменения параметров или настроек конфигурации программного обеспечения, лишь 34,5 % имели навык копирования или перемещения файла или папки, а 31,1 % могли самостоятельно осуществить передачу файлов между компьютером и периферийными устройствами[1];

– недостаточная осведомленность граждан о возможных противоправных действиях с использованием цифровых технологий, их высокая степень доверчивости, особенно в категории лиц старшего поколения, а при достаточной информированности – легкомысленное отношение к подобной информации, в частности, о неразглашении посторонним лицам реквизитов банковских карт и иной конфиденциальной информации. Зачастую совершению преступлений способствует несоблюдение потерпевшими элементарных мер предосторожности при пользовании сетью Интернет и общении с неизвестными лицами, в т. ч. при осуществлении сделок купли-продажи;

[1] *Абдрахманова Г. И., Вишневский К. О., Гохберг Л. М. и др.* Указ соч. С. 24.

– нарушение когнитивных функций лиц – потребителей цифровых услуг – вследствие переизбытка информации, с одной стороны, и легкости ее получения – с другой. Ситуация усугубляется формированием синдрома «клипового сознания», при котором знания носят фрагментарный и разрозненный характер, ценность информации определяется яркостью образов, их эмоциональным воздействием. При этом возрастают риски массового распространения недостоверной информации с использованием социальных сетей и мессенджеров, способной привести к нарушению общественного порядка, возникновению паники, экстремистским проявлениям и иным негативным последствиям, включая искаженные оценки определенных явлений, фактов, событий, а также недобросовестному манипулированию общественным сознанием[1]. Следствием данного обстоятельства является неуправляемое желание отдельных граждан приобрести товары по ценам, существенно ниже рыночных (с большими скидками), либо помочь родственнику, якобы попавшему в беду, а также сохранить свои сбережения от якобы несанкционированного списания;

– недостаточное внимание к вопросам обеспечения информационной безопасности со стороны руководства отдельных организаций, в т. ч. недостаточность мер по защите персональных данных. Развитие информационных технологий и повышение их роли в организации бизнес-процессов обусловливают значимость и коммерческую ценность конфиденциальной информации. Разглашение конфиденциальной информации способно нанести существенный ущерб деловой репутации юридического лица. Для граждан утрата сведений, составляющих банковскую тайну, может привести к потере сбережений. Вместе с тем резонансные утечки данных, в частности, клиентов финансовых организаций, неоднократно становились объектом внимания средств массовой информации[2]. По данным группы компаний

---

[1] Ярким примером подобного манипулирования является получившее широкое распространение в США общественное движение «Black lives matter», приведшее к многочисленным погромам и беспорядкам в ряде городов в мае–июле 2020 г. после гибели афроамериканца Джорджа Флойда от рук белого полицейского Дерека Шовина.

[2] 3 августа 2020 г. стало известно о выставлении на продажу базы данных, содержащей личные данные около 1 млн московских водителей, включая: ФИО, государственный регистрационный знак автомобиля, его марку, модель и год выпуска, VIN-номер, серию и номер ПТС и свидетельства о регистрации, номер телефона владельца автомобиля. 28 января 2020 г. стало известно об утечке данных клиентов сети алкомаркетов «Красное и Белое»: в Интернет попала база программы лояльности. См.: Утечки информации в России. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0

InfoWatch, в 2019 г. число утечек в России увеличилось более чем на 40 %, в то время как в мире подобных случаев стало больше примерно на 10 %. Количество скомпрометированных записей персональных данных и платежной информации в России выросло примерно в шесть раз – до 170 млн, тогда как в мире этот показатель увеличился в два раза до 14 млрд записей[1];

– формирование в цифровом пространстве виртуального образа личности, формируемого посредством комплекса псевдоидентификаторов: аватар (графическое изображение, произвольно выбранное пользователем социальной сети или Интерент-ресурса для самоидентификации), никнейм (сетевое имя, псевдоним, используемый для общения анонимных пользователей) и др. Подобные псевдоидентификаторы позволяют одному лицу создавать несколько виртуальных образов псевдоличностей, зарегистрированных под разными учетными данными в социальных сетях, имеющих свою историю переписки, собственные номера мобильных телефонов и электронных кошельков, т. е. не имеющих общих признаков и используемых в противоправной деятельности.

К правовым факторам относятся:

– неполнота правового регулирования отношений, связанных с возникновением больших объемов цифровой информации о характере и особенностях использования цифровых устройств их пользователями: поисковых запросов, геолокации, потребительских предпочтениях, данных видеорегистраторов и навигаторов, камер видеонаблюдения, показаний разного рода датчиков и пр. В частности, остаются неурегулированными вопросы о правах третьих лиц использовать эти данные без согласия лица, чьи действия привели к их формированию;

– наличие правовых пробелов, позволяющих осуществлять голосовое общение в сетях телефонной связи общего пользования без предварительной идентификации абонента (абонентского устройства), а также использовать технологии подмены номера, в т. ч. посредством использования сервисов интернет-телефонии, передающих голосовой трафик из сетей передачи данных в телефонную сеть;

– отсутствие в действующем законодательстве указания на конкретные сроки предоставления операторами связи

%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8; 27 августа 2020 г. ЦБ и Visa предупредили банки об утечке данных 55 тыс. карт. URL: https://www.rbc.ru/finances/27/08/2020/5f468fa59a7947858f2c197e и др. (дата обращения: 10.06.2021).

[1] Число сообщений об утечках данных в России в 2019 г. выросло на 40 %. URL: https://tass.ru/ekonomika/7621137 (дата обращения: 10.06.2021).

и интернет-провайдерами информации по запросам правоохранительных органов в соответствии со ст. 64 Федерального закона от 7 июля 2003 г. «О связи» и ст. 10.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», что заметно препятствует своевременному пресечению противоправных деяний, раскрытию и расследованию преступлений. Зачастую после получения решения суда о получении информации, относящейся к охраняемой законом тайне связи, компании-операторы предоставляют информацию о входящих (исходящих) соединениях запрашиваемого абонентского номера в течение 1-2 мес.[1] При этом качество, полнота и оперативность информации, предоставляемой операторами связи и интернет-провайдерами по запросам правоохранительных органов, как правило, не отвечают предъявляемым требованиям и не соотносятся с динамикой совершения рассматриваемых преступлений. В результате утрачивается возможность незамедлительной реализации информации, полученной в процессе оперативно-розыскной деятельности, а у субъектов преступления появляется возможность сокрытия следов противоправной деятельности, в т. ч. удалять значимую для расследования информацию со своих страниц в социальных сетях и страниц потерпевших. К сказанному следует добавить также длительное получение из кредитно-финансовых организаций сведений об операциях по счетам и вкладам физических лиц, в порядке ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности». Последнее обстоятельство негативно сказывается на деятельности по возмещению вреда, причиненного преступлением, поскольку к моменту получения судебного решения на наложение ареста на денежные средства они обналичиваются подставными лицами;

– отсутствие правового требования для кредитно-финансовых организаций по организации хранения видеозаписей с устройств самообслуживания (банкоматов), определения формата и сроков хранения подобной информации, что ведет к потере сведений, потенциально имеющих доказательственное значение по уголовным делам;

– низкая эффективность реализации отдельных положений Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об инфор-

[1] См.: письмо ГУ МВД России по г. Москве от 26 августа 2020 г. № 1/11957; письмо УМВД России по Костромской области от 27 августа 2020 г. № 1/3463; письмо УМВД России по Амурской области от 28 августа 2020 г. № 1/17/3508.

мации, информационных технологиях и о защите информации», в частности:

– устанавливающих запрет на обеспечение использования программно-технических средств (анонимайзеров, VPN-сервисов, иных технологий сокрытия или подмены данных об IP-адресах пользователей) для получения доступа к запрещенным в Российской Федерации информационным ресурсам. Приходится констатировать, что за время, прошедшее со дня введения обозначенного требования в действующее законодательство, использование средств анонимизации, как минимум, не сократилось, о чем свидетельствует активное их использование при совершении преступлений дистанционным способом;

– возлагающих на организаторов распространения информации в сети Интернет обязанность хранения сведений о персональных данных пользователей и передаваемой ими информации на территории Российской Федерации. При этом такие популярные информационные ресурсы, как «YouTube», «Instagram», «Facebook», «LiveJournal», «Twitter», а также почтовые сервисы «Gmail», «Protonmail» и другие указанного требования не придерживаются, что затрудняет получение информации, имеющей доказательственное значение[1];

– отсутствие эффективного механизма контроля со стороны банковских организаций, операторов связи, регистраторов доменных имен, платежных систем за актуальностью и достоверностью регистрационных их данных клиентов (абонентов, пользователей). Так, несмотря на установленные ст. 44 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» и Правилами оказания услуг связи[2], требования к операторам связи об обязательном достоверном установлении сведений, позволяющих идентифицировать абонента, по-прежнему имеют место факты реализации сим-карт без надлежащего удостоверения личности абонента, на вымышленное лицо, по утерянным или украденным документам;

– низкий размер штрафных санкций по ст. 19.7 Кодекса Российской Федерации об административных правонарушени-

[1] Письмо МВД по Республике Татарстан от 29 августа 2020 г. № 1/2045.

[2] См.: Правила оказания услуг телефонной связи [Электронный ресурс]: утв. постановлением Правительства Российской Федерации от 9 декабря 2014 г. № 1342; Правила оказания услуг связи по передаче данных [Электронный ресурс]: утв. постановлением Правительства Российской Федерации от 23 января 2006 г. № 32; Правила оказания телематических услуг связи [Электронный ресурс]: утв. постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575. Доступ из справ.-правовой системы «КонсультантПлюс».

ях (далее – КоАП РФ) «Непредставление сведений (информации)» в размере от 300 до 500 руб. не оказывает должного воздействия на должностных лиц операторов связи и распространения информации, что способствует увеличению длительности ответов на запросы органов расследования (свыше 1 мес.), что позволяет лицам, совершающим противоправные деяния, несколько раз сменить используемые ими сим-карты, электронные кошельки и банковские карты[1];

– правовая неопределенность при квалификации преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Так, неоднозначно складывается правоприменительная практика при квалификации хищений денежных средств с банковского счета, а равно электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) в случае, если причиненный ущерб составляет менее 2 500 руб. Частью 2 ст. 7.27 КоАП РФ предусмотрена административная ответственность за мелкое хищение чужого имущества стоимостью от 1 тыс. руб. до 2 500 руб. при отсутствии признаков квалифицированных составов кражи. Однако поскольку кража с банковского счета, а равно электронных денежных средств относится к квалифицированным составам и является преступлением, относящимся к категории тяжких, то уголовная ответственность наступает независимо от суммы ущерба. По этой же причине невозможно освобождение обвиняемого в краже денег с банковской карты от уголовной ответственности в связи с применением судебного штрафа, а также прекращение уголовного дела в связи с примирением сторон. Возникает парадокс: ответственность за хищение 200 тыс. руб. наличными оказывается меньше, чем ответственность за хищение 2 500 руб. с банковского счета, поскольку в первом случае деяние будет квалифицировано по п. «в» ч.2 ст. 158 как преступление средней тяжести, а во втором – по п. «в» ч. 3 ст. 158 УК РФ – как тяжкое преступление.

Статистические данные о результатах деятельности правоохранительных органов по выявлению, раскрытию и расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий свидетельствуют о недостаточной эффективности работы в данной сфере. Так, по итогам 2019 г. раскрываемость преступлений данной категории составила 24 %[2],

[1] Письмо УМВД России по Тверской области от 21 августа 2020 г. № 5/2696.

[2] По данным ГИАЦ МВД России. См.: Официальный сайт МВД России. URL: https://xn–b1aew.xn–p1ai/Deljatelnost/statistics (дата обращения: 11.06.2021).

что существенно выше аналогичного показателя 2018 г., но, тем не менее, не соответствует общественному запросу на обеспечение безопасности в цифровой среде.

При этом противодействие преступлениям, совершенным с использованием информационно-телекоммуникационных технологий, на протяжении ряда лет является приоритетным направлением деятельности органов внутренних дел. За период с 2014 г. вопросы совершенствования деятельности органов внутренних дел в сфере противодействия преступлениям данной категории рассматривались на 12 коллегиях МВД России, в т. ч. на трех – в прямой постановке[1].

В результате реализации принятых управленческих решений в настоящее время в ряде субъектов Российской Федерации функционируют специализированные следственно-оперативные группы, в состав которых входят наиболее подготовленные сотрудники. В составе подразделений центрального аппарата МВД России, а также территориальных органов МВД России созданы специализированные подразделения по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. В целях сокращения сроков получения информации, необходимой для расследования и раскрытия рассматриваемой категории преступлений заключаются соглашения об электронном обмене информацией с финансово-кредитными организациями, операторами связи, организациями, администрирующими платежные сервисы[2]. В ряде территориальных органов МВД России накоплен положительный опыт блокирования сигнала

---

[1] Решения коллегии МВД России: от 22 мая 2014 г. № 2км/2 «О совершенствовании деятельности по раскрытию и расследованию преступлений, совершенных с использованием информационных технологий»; от 24 октября 2017 г. № 3км «О мерах по совершенствованию организации раскрытия и расследования мошенничеств»; от 1 ноября 2019 г. № 3км «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий».

[2] Так, в рамках электронного документооборота с использованием ведомственного программного обеспечения (ИСОД МВД России) осуществляется взаимодействие с головным офисом Тинькофф Банк, Банк Раунд, платежными системами Яндекс. Деньги, UBANK, Моби.Деньги, с банками группы ВТБ. В МВД по Чувашской Республике, ГУ МВД России по Нижегородской области, УМВД России по ЕАО, Костромской, Липецкой, Оренбургской, Смоленской, Тульской областям действуют соглашения о сотрудничестве с ПАО Сбербанк, другими кредитно-финансовыми организациями, территориальными органами ФНС России (направление посредством электронного документооборота запросов о получении информации о владельцах банковских карт, движении денежных средств).

сотовой связи на территории учреждений уголовно-исполнительной системы[1].

В целях совершенствования информационного обеспечения деятельности правоохранительных органов по выявлению, расследованию и раскрытию преступлений в сфере информационных технологий на базе ранее разработанного модуля «Дистанционное мошенничество» создается новый интерфейс системы данных о преступлениях и лицах, подозреваемых и обвиняемых в их совершении (подсистема ИБДФ «АБД-Центр»). Осуществляется взаимодействие с операторами сотовой связи по организации блокирования номеров телефонов, информация о которых помещена в модуль «Дистанционное мошенничество». Кроме того, прорабатывается вопрос по созданию мобильного приложения, позволяющего с использованием информации модуля «Дистанционное мошенничество» о номерах телефонов блокировать входящие вызовы[2].

Вместе с тем, несмотря на значительные усилия органов внутренних дел по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, для качественного изменения ситуации в данной сфере требуется реализация комплекса мероприятий, приведенных в заключительном разделе настоящей работы.

---

[1] Так, УМВД России по Курганской области, совместно с региональным управлением ФСИН России, на территории исправительных учреждений установлены блокираторы сигнала сотовой связи. Операторы связи уменьшили мощность сигнала и изменили вектор направленности базовой станции. Специалистами ФГУП «Радиочастотный центр» и УМВД России по Курганской области организован ежеквартальный мониторинг складывающейся ситуации. Аналогичное оборудование установлено в отдельных исправительных учреждениях ФСИН России, расположенных на территории г. Москвы, республик Калмыкия и Мордовия, Удмуртской Республики, Смоленской, Свердловской и ряда других областей.

[2] Представляет интерес опыт иностранных государств (Австралия, Канада и др.), в которых разработаны и доступны для бесплатной установки на смартфоны специальные приложения, которые блокируют входящие звонки от злоумышленников, если они звонят с номера, когда-либо помещенного в так называемый черный список номеров мошенников (ведется подразделениями правоохранительных органов на основании сообщений об инцидентах).

2. О влиянии пандемии COVID-19 на состояние преступности в сфере информационно-телекоммуникационных технологий

На фоне активного воздействия факторов, способствующих совершению преступлений с использованием информационно-телекоммуникационных технологий, приведенных в первой части настоящей работы, на продолжающийся рост их числа оказали влияние внезапные изменения, произошедшие в жизнедеятельности граждан и организаций в связи с проведением мероприятий по ограничению распространения новой коронавирусной инфекции COVID-19. Эти изменения проявились в смене привычного ритма жизни, переводе на удаленную работу, введении режима самоизоляции, ограничений на свободу передвижения, приостановлении деятельности ряда организаций сферы услуг, организации досуга и пр.

С другой стороны, перечисленные ограничения придали колоссальный импульс дальнейшему развитию цифровых технологий и их интенсивной интеграции в образовательную деятельность, финансовый сектор, а также ряд других сфер социально-экономической деятельности. Представляется справедливым утверждение президента Всемирного экономического форума Клауса Шваба о том, что прошедшие 15 недель пандемии в плане цифровой трансформации общества сделали больше, чем предыдущие 15 лет[3].

В этих условиях усилилась зависимость как всего общества в целом, так и отдельных лиц от бесперебойного функционирования сервисов оказания государственных услуг в электронной форме, систем дистанционного банковского обслуживания, каналов связи и иной информационной инфраструктуры. Повседневная деятельность большинства организаций стала осуществляться на основе коммуникаций посредством электронной почты, сервисов видеоконференцсвязи и облачных хранилищ данных. На дистанционный режим работы перешли целые сектора экономики. Помимо образовательной и финансовой деятельности, в их число вошли розничная торговля, научно-исследовательская деятельность, сфера услуг и др. При таких обстоятельствах кратно возросли риски, связанные с негативными последствиями противоправных посягательств на цифровые данные, вызванные преступлениями, совершенными с использованием информационно-телекоммуникационных техно-

[3] URL: https://cyberpolygon.com/ru/ (дата обращения: 14.06.2021).

логий, рост которых является не только российской, но и общемировой тенденцией[1].

При этом особо следует отметить появление дополнительного комплекса факторов, детерминирующих рост числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий, включая[2]:

– значительное увеличение объема использования онлайн-коммуникаций государственными и муниципальными органами, организациями и частными лицами[3], а также увеличение продолжительности времени, в течение которого потенциальные потерпевшие проводят в Интернете[4]. Особо следует отметить рост пользователей онлайн-сервисов из числа лиц пожилого возраста, недостаточно осведомленных о способах противоправных деяний в сети Интернет, что способствует увеличению числа вымогательств, распространения вредоносных программ через спам-сообщения и т. п.;

– переход значительной части организаций на дистанционный режим работы на фоне недостатка опыта применения руководящим и линейным персоналом информационно-телекоммуникационных технологий. Широкое распространение получили факты направления информации, необходимой для входа в информационные системы, посредством электронной почты или сообщений в мессенджерах, пересылки файлов, содержащих персональные данные и иную конфиденциальную информацию;

– неподготовленность бизнес-процессов большинства организаций к переводу сотрудников на дистанционный режим работы[5],

---

[1] Согласно результатам проведенного Европолом исследования «Поймать вирус киберпреступности, дезинформации и пандемии COVID-19», угроза со стороны киберпреступности во время кризиса носит динамичный характер и имеет потенциал для дальнейшего увеличения. См.: письмо ГИАЦ МВД России от 30 апреля 2020 г. № 34/2-10987 «О направлении информации».

[2] Схожие факторы приводятся и в докладе Управления ООН по наркотикам и преступности «Киберпреступность и COVID-19: риски и ответные меры». См.: письмо ГИАЦ МВД России от 30 апреля 2020 г. № 34/2-10987 «О направлении информации».

[3] По данным Минкомсвязи, сайты ведущих российских СМИ в период пандемии коронавируса увеличили свою аудиторию суммарно на 150 млн пользователей. URL: https://www.interfax.ru/russia/708250. В первые дни введения режима самоизоляции и нерабочих дней объем потребления трафика фиксированной связи вырос на 30 %, а мобильного трафика – на 40 %. URL: https://www.rbc.ru/technology_and_media/31/03/2020/5e81fa5e9a7947c6b6442bac. Аналогичные данные приводятся «Лабораторией Касперского», согласно которым увеличение трафика российского сегмента сети Интернет от 7 % до 60% в зависимости от вида трафика. URL: https://www.kaspersky.ru/about/press-releases/2020 (дата обращения: 14.06.2021).

[4] «Лаборатория Касперского» сообщила о росте онлайн-мошенничества во время пандемии. URL: https://www.kommersant.ru/doc/4337079 (дата обращения: 14.06.2021).

[5] Согласно данным «Лаборатории Касперского» о влиянии COVID-19 на стиль работы, 79 % россиян, перешедших на удаленный режим работы, не получали никаких конкретных

что создает условия распространения фишинговых почтовых рассылок (от англ. *to fish* – ловить рыбу), при открытии которых происходит запуск содержащегося в них вредоносного программного кода. Широкое распространение получила практика рассылки сотрудникам организации электронных писем, содержащих вложения, которые позволяют в тайне от пользователя получать доступ третьим лицам к его данным. Такие письма рассылаются якобы от имени руководства организации с корпоративных электронных адресов. При этом злоумышленниками используются методы социальной инженерии с искусственным созданием ситуации дефицита времени и повышенного волнения, препятствующей принятию взвешенного решения;

– активную эксплуатацию в противоправных целях опасений населением угроз, связанных с распространением вируса COVID-19, при организации онлайн-продаж фальсифицированных лекарственных препаратов, антисептиков, средств индивидуальной защиты, медицинских консультаций и онлайн-диагностики;

– несмотря на предпринимаемые на государственном уровне меры, направленные на сохранение занятости, потерю постоянного источника дохода определенной частью населения в связи с прекращением деятельности организаций сферы обслуживания, торговли, услуг, в сочетании с желанием легкого заработка, способствует росту криминальной активности в рассматриваемой сфере.

В этих условиях киберпреступники не только разрабатывают новые способы совершения преступлений, но и адаптируют существующие схемы мошенничества под условия, вызванные COVID-19. При этом следует выделить следующие ***основные направления изменений в способах преступлений, совершенных с использованием информационно-телекоммуникационных технологий:***

1. Трансформация преступлений, совершенных с использованием «социальной инженерии», направленной на получение обманным путем от клиентов финансово-кредитных организаций посредством телефонной связи конфиденциальной информации под различными предлогами (включая персональные данные, реквизиты счетов и пароли доступа к ним). При этом сами схемы реализации мошенничества фактически не изменились, но приобрели новую «упаковку» под актуальную повестку: телефонный звонок от соцработников с предложением оказания содействия в получении государственных пособий; сообщение о родственнике, попавшем в больницу с корона-

---

рекомендаций по повышению цифровой грамотности и не прошли обучение, призванное защитить сотрудников от киберрисков. URL: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-79-rossiyan-ne-poluchali-rekomendatsii (дата обращения: 14.06.2021).

вирусом и возможности за деньги подключить его к аппарату искусственной вентиляции легких; продажа цифровых пропусков не выходя из дома (выезд на автотранспорте) или рассылка сообщений о штрафах за нарушение карантина и т. д., чему способствует введение режима самоизоляции и перевод сотрудников на удаленный режим работы.

2. Эксплуатация темы COVID-19 при распространении вредоносных программ, выполняющих тайные, не запланированные его пользователем функции, направленные на хищение данных (фишинг). В период самоизоляции получили распространение случаи завладения персональными данными граждан под предлогом оказания помощи в оформлении государственных пособий, возврата денег за неиспользованные вследствие отмены рейсов авиабилеты (туристического тура, страхового полиса и т. п.), приобретения различных медицинских товаров (медицинские маски, перчатки, инфракрасные термометры и пр.) и т. п.[1] При этом потерпевший перенаправляется на заранее созданную мошенниками фишинговую Интернет-страницу, предназначенную для получения данных банковской карты и иной персональной информации. Сведения о распределении фишинга по целевым категориям в первой половине 2020 г. представлено на *диаграмме 1.*

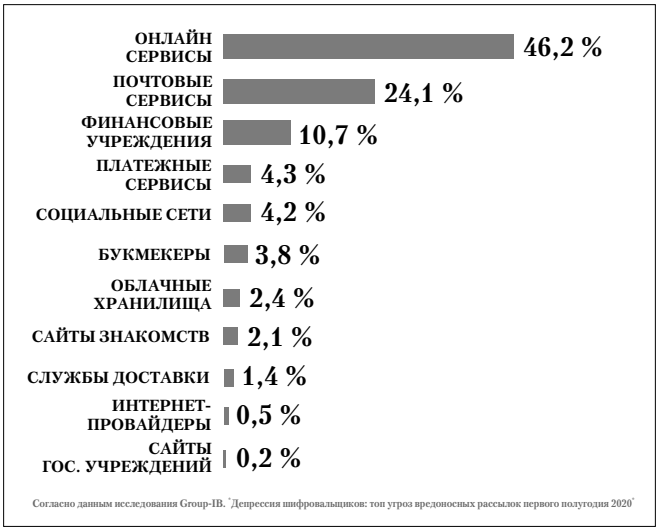

Диаграмма 1. Распределение фишинга по целевым категориям в первой половине 2020 г. (по данным компании Group-IB)

[1] По данным «Лаборатории Касперского», количество мошеннических сайтов, где у российских пользователей пытаются выманить деньги, выросло в первом квартале 2020 г. вдвое по сравнению с тем же периодом прошлого года и превысило 10 тыс. URL: https://www.kaspersky.ru/about/press-releases/2020 (дата обращения: 14.06.2021).

Имели место факты рассылки электронных писем, которые содержат фальшивое уведомление якобы от «оперативного штаба по борьбе с коронавирусом». Во вложенных файлах такого письма содержится документ с вредоносными макросами, при открытии которого происходит «заражение» устройства потерпевшего.

Установлены факты размещения информации в социальных сетях о выплатах за неиспользованные медицинские услуги по полису ОМС (вариант: получить не начисленный кэшбэк с покупок). Для этого потерпевшим высылается ссылка на сайт, где предлагается заполнить форму и узнать размер якобы полагающейся «компенсации». После ввода персональных данных на экране высвечивается сумма полагающейся выплаты, для получения которой требуется оплатить некие «организационные расходы». Далее пользователю предлагается указать номер его банковской карты якобы для зачисления денежных средств, в результате чего мошенники получают доступ к данным.

Установленные ограничения на передвижение и введенные штрафы за их нарушение способствовали появлению приложений для смартфонов, позволяющих определить, насколько далеко можно отходить от дома. При этом для регистрации в указанных приложениях требовалось указание данных банковской карты, которые использовались для целей последующего хищения.

Осложнение ситуации на рынке труда вызвало рост числа мошенничеств, совершенных якобы от имени кадровых агентств. В основе способа их совершения было направление приглашения «на собеседование к работодателю» посредством Zoom-конференции, с фактической переадресацией на фишинговый сайт.

В период майских праздников 2020 г. отмечалось распространение вредоносного программного обеспечения «Ginp» под видом видеоролика о том, как правильно носить маску: вместе с видеороликом загружается вредоносное программное обеспечение под видом приложения для просмотра ролика. При запуске приложения для просмотра ролика устанавливается вредоносное программное обеспечение, позволяющее управлять компьютером удаленно. Используется эффект чрезмерной заинтересованности пользователей в получении дополнительной информации[1].

3. Изменения в механизме вымогательств с использованием вирусов-шифровальщиков, направленных на блокирование

[1] Троян Ginp зарабатывает на коронавирусе. URL: https://www.kaspersky.ru/blog/ginp-trojan-coronavirus-finder/27762/ (дата обращения: 15.06.2021).

информации на устройстве потерпевшего путем шифрования данных и предоставления последующего доступа к ним после уплаты выкупа в виде виртуальной валюты.

Широко распространенные инструменты для организации дистанционной работы оказались высоко уязвимы с точки зрения кибербезопасности. Так, в получившем популярность сервисе видеоконференций «Zoom» выявлены критические уязвимости, позволяющие третьим лицам получить полный контроль над системой, произвести шифрование данных и требование выкупа за восстановление работоспособности системы[1].

Отмечается рост количества атак с перебором паролей на сервисы для дистанционной работы. Поскольку для выполнения своих обязанностей пользователь регулярно подключается к серверу компании, киберпреступники получают возможность подбора пароля для удаленного доступа в информационную систему. Затем они с помощью специальных инструментов повышают свои права доступа к информационным ресурсам и их модификации, шифруют критичные для функционирования бизнеса файлы и оставляют сообщение с требованием выкупа.

В начале марта специалистами компании Group-IB зафиксированы рассылки шпионской программы HawkEye с темой Free Face Mask. Письмо было отправлено якобы от менеджера китайской компании – GALAXY ELECTRONIC INDUSTRIAL, а получателями были российские компании, в т. ч. из сферы энергетики. В письме указывалось, что китайская компания якобы запустила завод по производству медицинских масок, ассортимент и характеристики которых содержатся в сертификации товара во вложении (RAR-архив Mask 2020.rar с вредоносным исполняемым файлом Mask 2020.exe и шпионской программой из семейства HawkEye (aka HawkSpy).

4. Предложение услуг, позволяющих обойти ограничения, введенные в связи с пандемией. В связи с введенными ограничениями, связанными с режимом самоизоляции, появились предложения услуг по онлайн-оплате якобы наложенного штрафа, проведению «обязательного» платного анализа, необходимого вследствие якобы имевшего место контакта с носителем вируса, изготовлению справок об отрицательных результатах тестов на COVID-19, изготовлению пропусков на передвижение и т. д. При этом, в последнем случае, потерпевшим предоставлялись недействительные про-

[1] Данные компании Group-IB. URL: https://www.group-ib.ru/landing/stay-safe.html (дата обращения: 15.06.2021).

пуска[1]. Динамика торговли цифровыми пропусками представлена на *диаграме 2*.

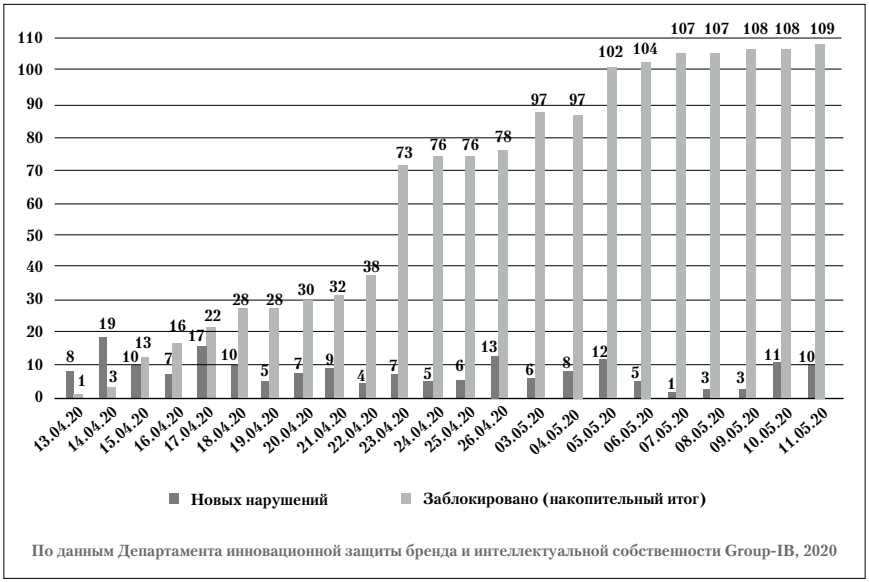

Диаграмма 2. Динамика торговли цифровыми пропусками (по данным компании Group-IB)

Мошеннические схемы по продаже электронных пропусков появились в конце марта – начале апреля 2020 г., когда мэрией Москвы были усилены ограничительные меры, направленные на снижение распространения коронавируса. Несмотря на распространяемые предупреждения мэрии Москвы о том, что цифровые пропуска оформляются бесплатно, а все сведения, указанные при оформлении пропуска, проходят обязательную проверку в федеральных органах власти, нелегальный рынок цифровых пропусков рос высокими темпами. Начиная с середины апреля фиксировался взрывной рост регистрации мошеннических сервисов: сайтов, Telegram-каналов, VK- и Instagram-аккаунтов, предлагающих купить справки-пропуска на период карантина по цене от 3 тыс. до 5 500 руб.

[1] Международная компания Group-IB, специализирующаяся на предотвращении кибератак, с конца марта обнаружила 185 мошеннических интернет-ресурсов по продаже в России поддельных справок и пропусков // Group-IB обнаружила 185 ресурсов по продаже фейковых пропусков в России. URL: https://ria.ru/20200512/1571325897.html (дата обращения: 15.06.2021).

Здесь же следует отметить предложения оплатить несуществующие «штрафы» за нарушение режима самоизоляции, распространяемые посредством СМС или сообщений в мессенджерах о якобы имевшем место нарушении установленных ограничений. Ссылаясь на несуществующее постановление ФСИН, мошенники требовали от «нарушителя» в течение суток оплатить штраф в размере 4 тыс. руб. переводом на номер абонента (Красноярский край). В сообщении говорились, что, если штраф не будет оплачен в течение 24 часов, будет возбуждено уголовное дело по ст. 236 УК РФ (Нарушение санитарно-эпидемиологических правил, повлекшее по неосторожности массовое заболевание или отравление людей). Пример подобного сообщения представлен на *фото 1*.

Фото 1. Пример сообщения об оплате несуществующего штрафа (по данным компании Group-IB)

5. Продажа товаров и услуг ненадлежащего качества, спрос на которые возрос в условиях пандемии. Медицинские маски, перчатки, респираторы, антисептики, термометры – это товары, ставшие остродефицитными в первые недели введения ограничительных мер. Предложения о покупке данных товаров по многократно завышенной цене товара направлялись на личные почтовые адреса граждан. По данным Роспотребнадзора, в период пандемии получили распространение предложения «уникальных» товаров, например: очиститель воздуха, удаляющий возбудителя вируса, маски с фильтром, отсеивающие вирус, или «чудо-средство» от COVID-19

и т. п.[1] Стоимость таких товаров оказывается сильно завышена, а эффективность не доказана. К этой же группе относятся предложения о покупке амулетов, оберегов и других магических предметов, якобы охраняющих от вируса[2].

Следует отметить, после резкого роста активности мошенников по продвижению через интернет-сайты вышеназванных товаров, впоследствии подобная активность заметно снижается, что, возможно, связано с информированием населения о данных схемах мошенничества в СМИ.

6. Эксплуатация тематики, связанной с социальными выплатами, мерами социальной поддержки и занятостью. Получило распространение предложение услуг фиктивными кадровыми агентствами, предлагающими гражданам, оставшимся без работы в результате ограничений из-за COVID-19, трудоустройство в удаленном формате. Соискатель заполняет анкету с личными данными, ему приходит письмо, что он принят на работу и теперь должен перевести деньги за «некое оборудование», которые присваиваются мошенниками без оказания содействия в трудоустройстве[3].

Вариативной разновидностью приведенной схемы является следующий пример: мошенники предлагают удаленный заработок по оцифровке текстов, при этом перед началом работы необходимо внести денежные средства в качестве комиссии за получение заказов[4].

Появились предложения, направленные на введение в заблуждение относительно оснований и порядка осуществления социальных выплат и оказания мер материальной поддержки. При этом рассылаются сообщения якобы с сайта «Госуслуг» с информацией о положенных выплатах, для получения которых требуется перевести «госпошлину», либо для проверки суммы «компенсации» ввести данные банковской карты, после чего с нее происходит списание средств.

Наблюдается рост числа сайтов-«клонов», визуально сходных до степени смешения с популярными сервисами доставки по цветовому исполнению, шрифтам и формату текста, фирменному стилю

---

[1] Роспотребнадзор сообщил о видах мошенничества в период пандемии. URL: https://www.rbc.ru/rbcfreenews/5ed5ca639a7947a832ce9916 (дата обращения: 15.06.2021).

[2] Новые виды мошенничества в период пандемии коронавируса. URL: https://www.mos.ru/news/item/73933073/ (дата обращения: 15.06.2021).

[3] Сбербанк сообщил о схемах мошенничества с трудоустройством на фоне вируса. URL: https://www.rbc.ru/society/20/05/2020/5ec4ae819a79476af7b97228 (дата обращения: 15.06.2021).

[4] См., например: URL: http://glagol-book.info/ (дата обращения: 15.06.2021).

и логотипам, в результате чего визуально отличить оригинальный сайт от сайта-клона практически невозможно. В условиях пандемии COVID-19 такие сайты-«клоны» могут маскироваться под официальные порталы государственных и международных организаций, например, Всемирной организации здравоохранения или Минздрава России, благотворительных организаций, осуществляющих помощь и поддержку граждан.

Механизм совершения преступления в данном случае включает в себя несколько этапов: создание копии официального сайта, который отличается только доменным именем, покупку доменных имен со схожим наименованием, которые служат запасными вариантами размещения сайта-клона, направление на сайт-клон трафик через e-mail рассылки, СМС-сообщения, мессенджеры и платное продвижение в поисковой выдаче, подмена оригинальных платежных реквизитов на свои, обработка поступающих запросов и прием платежей от обманутых клиентов, которые считают, что покупают продукцию у официальной компании, прекращение какого-либо общения с обманутыми клиентами, перенос сайта на запасной домен, если основной домен блокируется. В неиндексируемом сегменте сети Интернет (Даркнет) существует возможность заказать изготовление или приобрести готовые сайты-клоны для целей совершения мошеннических действий.

Получила распространение следующая схема: мошенник на «Авито» под видом продажи тестов на COVID-19 присылает клиенту ссылку для оплаты. Клиент, переходя по ссылке, попадает на поддельный сайт «Авито», не понимая при этом, что перешел по мошеннической ссылке, и производит оплату злоумышленнику.

Еще одной масштабной мошеннической схемой, активизировавшейся в период самоизоляции, стала схема с фейковой курьерской доставкой товаров, заказанных через Интернет. Злоумышленники создавали на популярных сервисах бесплатных объявлений так называемые «лоты-приманки» – объявления о продаже по намеренно заниженным ценам товаров – фотоаппаратов, игровых приставок, ноутбуков, смартфонов и т. д., а потом присылали покупателю ссылку на фишинговую (недостоверную) страницу курьерского сервиса и просили перевести деньги за товар и доставку. Средний чек одной такой «покупки» составляет примерно 15 тыс. – 30 тыс. руб. Часть жертв обманывают повторно – «разводят на возврат». Через некоторое время после оплаты товара покупателю сообщают, что в организации почтовой связи произошла нештатная ситуация: например, сотрудник почты якобы пойман на краже, а заказанный товар конфисковала полиция, поэтому для компенсации перечис-

ленной суммы необходимо оформить «возврат средств». Фактически с карты происходит повторное списание той же суммы.

7. Дезинформация относительно санитарно-эпидемиологической обстановки (фальшивые новости). Динамика распространения фальшивых новостей о коронавирусе представлена на *диаграмме 3*.

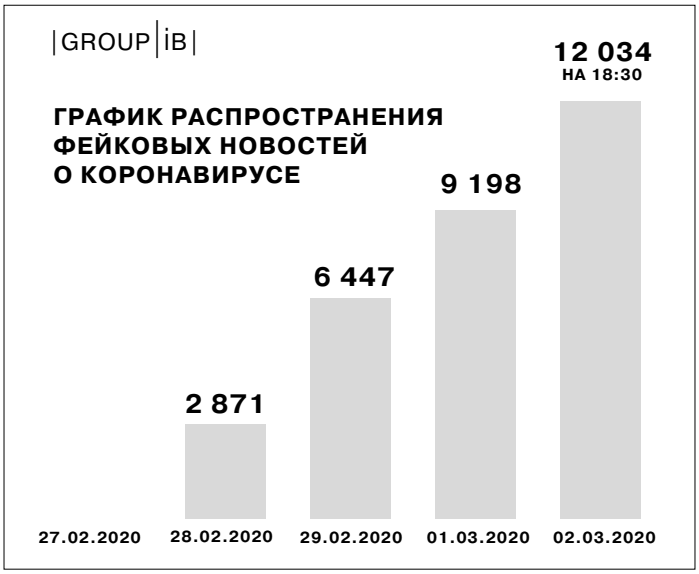

Диаграмма 3. Рост числа фактов распространения фальшивых новостей (данные компании Group-IB)

Целями распространения дезинформации чаще всего являются:

– получение финансовой выгоды за счет недобросовестной рекламы. Так, мошенники, имитируя деятельность известных компаний под хештегами #сидидома, #домалучше и т. п., предлагают желающим поучаствовать в акции и получить денежное вознаграждение, для чего требуют сообщить данные карты и одноразовый СМС-пароль. Для участия в «акции» необходимо также провести небольшой платеж;

– лжеблаготворительные акции: склонение принять участие в сборе средств пострадавшим от коронавируса, врачам, пожилым людям и т. п.;

– недоверие к деятельности государственных органов[1].

[1] 2 марта 2020 г. компания Group-IB выявила факт вброса фейковых новостей о масштабном заражении москвичей коронавирусом: якобы городскими службами

8. Вторичный обман: лицам, уже пострадавшим от интернет-преступников, предлагают получить компенсацию за участие в фальшивых опросах, недобросовестных лотереях или компенсацию НДС, но вместо этого списывают деньги и похищают данные банковских карт. Мошенники активно используют «синдром обманутого вкладчика», состоящего в том, что зачастую жертвы финансовых пирамид, поддавшись на рекламу возврата потерянных средств, добровольно вновь несли свои деньги в недобросовестные структуры типа «МММ», после чего вновь оказывались обманутыми и повторно лишенными денежных средств.

Злоумышленники действуют под видом несуществующих организаций — Международной службы «Единый центр возвратов», «Национального Лотерейного Содружества», «Центра финансовой защиты» и др. *(фото 2, 3, 4)*.

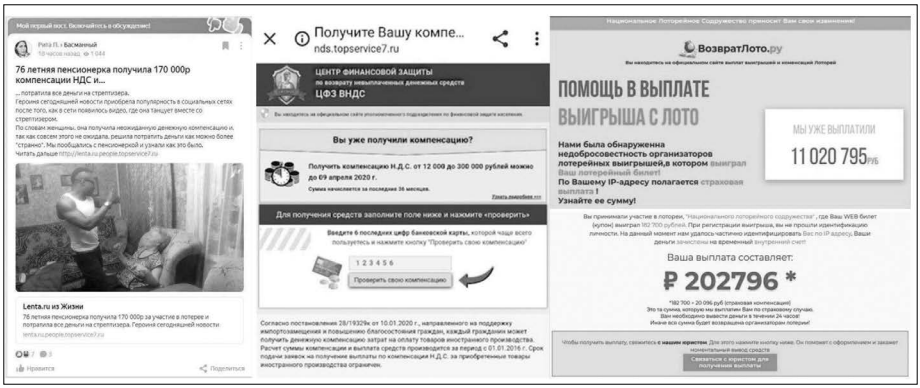

Фото 2, 3, 4. Примеры предложений по оказанию содействия в получении несуществующего выигрыша или компенсации (данные компании Group-IB)

скрываются данные о массовом заражении коронавирусом москвичей. Было зафиксировано более 12 тыс. постов, репостов, публикаций, транслирующих эту фейковую новость. Отрабатывались три основных мотива вброса: дестабилизация ситуации и усиление панических настроений накануне карантина, финансовая мотивация: недобросовестная конкуренция производителей защитных средств, продуктов, товаров первой необходимости, хулиганство. С помощью технологий графового анализа данных был выявлен факт искусственного распространения голосового сообщения. В основном информационная атака распространяется через ботов в соцсети ВК, а также через различные группы в мессенджерах. Вброс таргетируется на самую восприимчивую аудиторию, – в основном это группы в мессенджерах при детских садах, школах («группы мам»), на женскую аудиторию в сети, форумы мам и др. URL: https://www.group-ib.ru/media/double-cheating/ (дата обращения: 15.06.2021).

Посетителям необходимо рассчитать сумму компенсации, ответить на вопросы «юриста отдела страховых выплат», заполнить анкету, указав ФИО и телефон; оплатить «юридические услуги» за оформление документов, введя на фишинговом сайте номер банковской карты, имя владельца, срок действия, CVV-код.

В итоге со счета жертвы списывается небольшой «взнос», а данные банковской карты остаются в руках интернет-преступников.

10. Незаконный сбыт наркотиков. На период предпринятых противоэпидемиологических мер наркомагазинами временно были сняты с реализации сделанные ранее закладки наркотиков в ставших труднодоступными для посещения местах (парки, скверы и другие общественные места отдыха граждан). Для обеспечения возможности длительного потребления наркотиков предложены среднеоптовые продажи, обеспечена адресная доставка заказов, в т. ч. формирование закладок в местах, находящихся в непосредственной близости с местонахождением заказчика. Для адресных поставок широко использовались сотрудники курьерских служб по доставке продуктов питания.

Общее число интернет-магазинов, реализующих психоактивные вещества, сократилось, ликвидировались магазины с небольшими финансовыми ресурсами. Одновременно с этим крупные интернет-магазины активизировали свою деятельность. Об этом свидетельствуют многочисленные объявления в неиндексируемом сегменте сети Интернет о требующихся закладчиках (так называемых «кладменах»).

Перевод образовательных организаций на онлайн-обучение повлек увеличение продолжительности пребывания несовершеннолетних в сети Интернет и, как следствие, рост масштабов их вовлечения в деятельность, связанную с незаконным оборотом наркотиков[1].

Принимая во внимание сохранение вышеприведенных факторов и после окончания действия большинства ограничений, вызванных борьбой с распространением новой коронавирусной инфекции COVID-19 и способствующих росту числа преступлений, совершаемых с использованием в данной сфере информационно-телекоммуникационных технологий, в краткосрочной перспективе прогнозируется увеличение числа преступлений.

[1] Письмо МВД по Республике Татарстан от 29 августа 2020 г. № 1/2045.

3. Обзор основных цифровых технологий, используемых при подготовке, совершении и сокрытии преступлений

Как указывалось выше, в большинстве случаев для совершения противоправных действий используются уже существующие технологии, стандартное программное обеспечение. Так, для сообщения покупателям наркотических средств и психотропных веществ сведений о местах нахождения тайников с «закладками» широко используются сервисы для загрузки, хранения и передачи фотографий, такие как Imgur, Radikal, Postimg. С указанной целью используется также широко распространенный картографический сервис Google Maps, позволяющий покупателям обнаруживать место «закладки» по точным координатам, сообщаемым им при онлайн-оплате за незаконное приобретение наркотического средства посредством Telegram-бота или платформы Hydra.

Сервисы One Time Secret, Privnote позволяют после прочтения адресатом полученных по ссылкам сообщений безвозвратно удалять их через определенный отправителем непродолжительный период времени[1].

При совершении преступлений с использованием «социальной инженерии» с целью выведывания у потерпевшего конфиденциальной информации, обеспечивающей доступ к его банковскому счету, широко используется технология подмены номера абонента. Потенциальному потерпевшему поступает телефонный звонок на его номер мобильного телефона. При этом последний видит входящий вызов абонентского номера из номерных телефонных емкостей +7495... или +7499..., после чего в результате состоявшегося телефонного разговора мошенники, представляясь службой безопасности банка, путем обмана завладевают денежными средствами гражданина. Установить лицо, непосредственно совершающее преступление с использованием сетей электросвязи, препятствуют следующие обстоятельства: абонентские номера из номерных телефонных емкостей +7495... или +7499..., которые видят потерпевшие в момент совершения преступления, являются подменными, при этом сам звонок поступает в виде интернет-трафика с территорий сопредельных государств.

Пример передачи голосового трафика (указан алгоритм организации телефонной связи, характерный для подавляющего большин-

[1] Письмо МВД по Республике Бурятия от 31 августа 2020 г. № 6/2660.

ства совершенных преступлений данного вида): любое юридическое лицо, которое не имеет лицензии на оказание услуг связи, но имеет договорные отношения с любым оператором сотовой связи в качестве его абонента, заключает договор с представителями телекоммуникационных компаний со стороны Украины и осуществляет передачу голосового трафика по IP-протоколу через сеть Интернет от абонентов на стороне Украины к потерпевшим на территории России, используя свою номерную емкость виртуальных номеров, арендованную у сотового оператора с номерами сегмента +7495... или +7499... Таким образом происходит подмена абонентского номера со стороны пользователя на Украине и преобразование иностранного интернет-трафика (VoIP-сигнал), поступающего с территории Украины в телефонную сеть общего пользования формата GSM на территории России.

Указанная схема организации связи осуществляется с нарушением основных положений Федерального закона «О связи», что позволяет наладить беспрепятственную работу мошеннических call-центров на территории Украины, которые осуществляют «обзвон» граждан России под видом сотрудников банка.

Затрудняет процесс расследования преступлений, совершенных с использованием интернет-технологий, технология построения компьютерных сетей по ячеистому принципу, при котором одни рабочие станции сети, соединяясь друг с другом, выполняют роль коммутатора для других рабочих станций, что обеспечивает отказоустойчивость всей сети в целом (mesh-сети). Узлы в mesh-сети соединяются по принципу «каждый с каждым», обеспечивая широкий выбор маршрута трафика внутри сети. К наиболее популярнм mesh-сетям относятся Yggdrasill, cjDNS, Briar, Signal Offline, FireChat и др. Анализ архитектурных решений и информационно-телекоммуникационных технологий, используемых при развертывании mesh-сетей, показал возможность их использования для организации доступа к информации, распространение которой в России запрещено.

Однако наибольшие сложности возникают при установлении лица, совершившего противоправное деяние с использованием компьютерных сетей на основе анонимных защищенных подключений, в т. ч. использующих принципы «луковой» маршрутизации. Сеть TOR (от англ. *The Onion Router* – луковичная маршрутизация) построена как система прокси-серверов, позволяющих создавать анонимное соединение. Анонимность в сети TOR реализуется также с помощью разбиения каждого сетевого запроса на множество небольших фрагментов и их пересылку от отпра-

вителя к получателю через разные маршрутизаторы (виртуальные туннели) в зашифрованном виде. Для навигации в сети TOR используются специальные версии браузеров, обеспечивающих возможность выхода в анонимную сеть TOR. Именно в данном сегменте Интернета, не индексируемом традиционными поисковыми средствами (Яндекс, Google), размещается абсолютное большинство виртуальных торговых площадок по нелегальной продаже запрещенных к свободному обороту объектов (оружие, боеприпасы, наркотики и пр.).

С целью незаконного сбыта ограниченных в обороте или изъятых из оборота объектов (оружие, наркотики, порнографическая видеопродукция и т. д.), в сети TOR создаются специализированные сайты, физически размещенные на серверах вне юрисдикции Российской Федерации, предлагающие приобрести запрещенные к обороту объекты и позволяющие производить оплату. Функционально данные информационные ресурсы представляют собой интернет-магазины, реализующие криминальные товары и предлагающие незаконные услуги. После проведения оплаты покупателю сообщаются геокоординаты и высылается фотоизображение места «закладки» – тайника, в котором находится заранее размещенный в нем объект криминальной сделки.

К числу основных способов сокрытия информации о лице, совершающем противоправные действия с использованием сети Интернет, относится использование программ-ремейлеров, обеспечивающих переадресацию отправлений электронной почты и подмену информации об электронном адресе отправителя электронным адресом ремейлера или иным подменным адресом. В результате получатель электронного почтового отправления лишается возможности установить личность отправителя. Ремейлеры обеспечивают возможность реализации фишинговых схем, основанных на рассылке электронных писем якобы от имени государственных и муниципальных органов, судов, банков, иных организаций, вызывающих доверие у потерпевшего. После открытия такого письма в информационную систему потерпевшего попадает вредоносное программное обеспечение, позволяющее в тайне от него выполнять несогласованные функции: собирать и передавать злоумышленникам персональные данные (включая платежную информацию), производить системы с требованием платы за разблокировку. Использование ремейлеров при этом существенно затрудняет установление лица, совершившего преступление.

С целью сокрытия цифровых следов, позволяющих установить лицо, совершившее противоправное деяние, широкое рас-

пространение получило использование анонимайзеров, обеспечивающих подмену используемого абонентом сети Интернет уникального IP-адреса, предоставленного ему провайдером при подключении к сети. При этом происходит замена IP-адреса пользователя на IP-адрес программы-анонимайзера, а также подмена информации об используемом сетевом браузере, параметрах его настройки, удаление запросов и ответов веб-сервера от служебных cookie-файлов, используемых для формирования истории посещения определенных интернет-ресурсов пользователем сети. Анонимайзеры позволяют обходить ограничения на доступ информационным ресурсам, содержащим информацию, распространение которой в Российской Федерации запрещено[1].

Большинство анонимайзеров весьма просты в использовании: в поисковую строку вводится сетевой адрес ресурса, доступ к которому требуется осуществить не с IP-адреса пользователя, а с IP-адреса анонимайзера, расположенного, как правило, за рубежом.

Особой разновидностью анонимайзеров являются VPN-сервисы (от англ. *Virtual Private Network* – виртуальная частная

---

[1] В соответствии с ч. 5 ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», предусмотрены следующие основания для ограничения доступа к информации во внесудебном порядке:

1) решения уполномоченных органов исполнительной власти в отношении распространяемых посредством сети Интернет:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

д) информации о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи;

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено.

Кроме того, в соответствии со ст. 15.3 вышеназванного Федерального закона, ограничение доступа к информации в сети Интернет, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, производится также во внесудебном порядке на основании требования Генерального прокурора Российской Федерации или его заместителей.

сеть). Они обеспечивают создание защищенного информационного канала (туннеля) между устройством, с которого осуществляется вход в сеть Интернет, и сервером, обеспечивающим работу VPN-сервиса, расположенном, как правило, за рубежом, осуществляя переадресацию сообщений. При этом VPN-сервисы осуществляют шифрование данных, отправляемых или получаемых с их использованием.

С целью обеспечения более надежного сокрытия данных, позволяющих идентифицировать лицо, осуществившее вход в сеть Интернет, VPN-сервисы нередко используются совместно с прокси-серверами – физическими устройствами или специальными программами, обеспечивающими роль посредника между подключаемым к сети Интернет устройством и самой сетью. Учитывая, что к одному прокси-серверу могут подключаться сотни различных устройств, все они для внешних пользователей будут иметь общий IP-адрес – адрес прокси-сервера.

Для сокрытия финансового следа совершенного преступления все более широкое применение получает использование криптовалют в криминальных взаиморасчетах.

В общем виде криптовалюта представляет собой распределенную, основанную на математических принципах пиринговую виртуальную валюту с открытым исходным кодом, при использовании которой отсутствует централизованный администратор, а также соответствующие контроль и надзор (Bitcoin, LiteCoin, Ripple) со стороны государственных органов или иных третьих лиц.

Одной из ключевых особенностей использования криптовалют является относительная анонимность их пользователей. Применительно к криптовалюте биткоин это означает, что каждая транзакция подлежит регистрации с присвоением уникального номера, однако эта регистрация привязывается к электронному кошельку, который может быть открыт на вымышленных лиц, а не к личности его владельца.

Использование Bitcoin-кошелька предполагает создание открытого и закрытого ключей шифрования, при этом открытый ключ является Bitcoin-адресом, а закрытый представляет собой цепочку из 64 буквенных и цифровых обозначений, который присоединен к конкретному Bitcoin-адресу и используется при подтверждении транзакций.

С целью анонимизации транзакций в криптовалюте используются анонимайзеры, подменяющие IP-адрес устройства, с которого производился вход в сеть Интернет, а также программы-«миксеры», осуществляющие разбиение пересылаемого сообщения на отдель-

ные фрагменты, направляемые адресату разными маршрутами. При использовании такого сетевого «миксера», который собирает биткоины нескольких пользователей, несколькими операциями проводит их по сложным маршрутам, и затем возвращает владельцам, привязать биткоин к конкретному источнику становится значительно труднее, если не сказать – вообще невозможно.

Всего в русскоязычном домене сети Интернет (по данным мониторинга bestchange.ru) представлено более 400 интернет-площадок по обмену криптовалют на их рублевый эквивалент, которые находятся вне поля правового регулирования.

Интернет-магазины, посредством которых осуществляется незаконный сбыт наркотических средств и психотропных веществ, при производстве расчетов с использованием криптовалют, предоставляют существенные скидки, достигающие 15-20 %, что выступает стимулом их использования. Кроме того, как свидетельствует судебно-следственная практика, вознаграждение участникам преступных сообществ все чаще начисляется посредством использования криптовалюты Bitcoin и Ethereum[1].

Существенные угрозы информационной безопасности, вызванные активным применением бытовых устройств, оснащенных встроенными техническими средствами для взаимодействия между собой и с внешней средой («Интернет вещей», устройства IoT – от англ. *Internet of Things*), обусловлены, в первую очередь, их архитектурными особенностями.

Устройства IoT в основном не являются комплексными системами, зачастую они реализуют какую-либо узкую функцию (видеонаблюдение, мониторинг и др.). Эта функция в большинстве случаев программно привязана к возможностям конкретной аппаратной части. Устройства IoT быстро устаревают, имея весьма короткий жизненный цикл и период поддержки, а программная часть даже от одного производителя может разительно отличаться от одной модели устройства к другой. Производителям невыгодно осуществлять поддержку большого парка старых устройств с учетом растущей вариативности программного обеспечения, что усложняет их поддержку и выпуск обновлений. При этом именно в программной части таких устройств находится подавляющее число уязвимостей, поскольку для устройств IoT, даже в пределах модельного ряда одного производителя, как правило, отсутствует единая стратегия обновлений безопасности. Даже если производитель выпустит новую «прошивку», устройство ее не получает

[1] Письмо МВД по Республике Бурятия от 31 августа 2020 г. № 6/2660.

автоматически. Требуется вмешательство пользователя, который не всегда заинтересован в обновлениях безопасности при условии корректно работающего основного функционала, но при этом он заинтересован в непрерывной работе устройства без остановок на обновления.

Вследствие нацеленности на быстрое и простое внедрение, в устройствах IoT зачастую недостаточно реализуются меры по обеспечению безопасности, такие как требование сменить пароль по умолчанию или изоляция интерфейса управления устройства от сети Интернет. Это закономерно приводит к тому, что такое устройство становится легкодоступным в сети Интернет для совершения противоправных действий.

Программное обеспечение для таких устройств зачастую создается в ускоренном темпе, без каких-либо проверок качества по части информационной безопасности, с упрощением методов безопасной разработки, внедрения компонентов и тестирования. Действует принцип «Security through obscurity», т. е. «безопасность через неизвестность» – в этом случае производитель внедряет свои упрощенные методы защиты вместо реализации сложных общепринятых мер, надеясь на то, что об этом никто не узнает, по крайней мере, быстро. Однако, при изучении такого программного обеспечения (далее – ПО) методами реверс-инжиниринга такие особенности разработки быстро выявляются, найденные ошибки становятся серьезными уязвимостями, и злоумышленник, изучив такое ПО один раз, может атаковать большое количество устройств во всей сети Интернет.

Для проверки функционирования и других сервисных работ производители зачастую применяют общие для большого количества устройств учетные данные, которые становятся «входной точкой» для атаки на сами устройства и сети, в которые они подключены.

Помимо ошибок безопасности, связанных с разработкой, встречаются проблемы компоновки ПО, когда в него добавляются сторонние уязвимые компоненты. Злоумышленники в таком случае могут скомпрометировать устройство IoT случайно, атакуя вслепую уязвимый компонент по всей сети Интернет.

Для массового сегмента ПО устройства IoT создаются на основе операционной системы Linux, которая хорошо известна атакующим и для которой можно довольно легко добавить в функционал вредоносную составляющую. В некоторых случаях для реализации атаки даже хватает встроенных в операционную систему утилит, и злоумышленнику не приходится заниматься сложными действиями – доставкой и внедрением компонентов вредоносных программ.

Устройства IoT, особенно из «домашнего» сегмента, рассчитаны на упрощенное подключение к сети. В такой схеме отсутствует какая-либо сетевая изолированность, что также облегчает как компрометацию самого устройства IoT, так и его соседей по сети.

Схожие особенности имеют и сетевые коммуникации устройств IoT. Если протокол взаимодействия является стандартизированным, но допускающим различного рода послабления по защищенности, то зачастую производитель и не следует практикам защиты. Типичная ситуация – трафик коммуникаций либо не шифрован, либо сертификат шифрования не проверяется (что равносильно нешифрованным коммуникациям), не проверяется источник запросов, не проверяются форматы сообщений, наборы параметров. В совокупности это позволяет влиять на основной функционал устройства даже без вмешательства в его программное обеспечение. Если же протоколы взаимодействия были разработаны самим производителем, то возникает тот же принцип – «Безопасность через неизвестность». После реверс-инжиниринга протокол открывается полностью, и конечная защищенность взаимодействия обычно оказывается намного ниже, чем в случае использования стандартизированных протоколов взаимодействия.

Для анонимизации действий пользователя в сети Интернет могут использоваться технологии анонимных сетевых подключений, которые включают в себя как аппаратные решения, так и анонимные сети. Анонимные сети бывают трех типов:

- децентрализованные;
- гибридные;
- узкоспециализированные.

Характерной чертой анонимных сетей является отсутствие единого центра контроля (децентрализованность). Наиболее распространенными децентрализованными сетями являются I2P; TOR; TON Freenet; Zeronet; anoNet и др. При этом большинство из них функционируют «поверх» Интернета, т. е. правила взаимодействия субъектов не затрагивают основную модель коммуникации.

Аппаратное решение для анонимизации пользователя представляет собой устройство, которое можно использовать в качестве роутера или клиента, предоставляющего доступ к анонимным сетям. В качестве подобного устройства могут выступать: Rasberry Pi, роутеры и IoT-устройства.

Примером децентрализованной анонимной сети является Invisible Internet Project (I2P). Основной задачей проекта является анонимизация сервисов сети: сайтов, блогов, электронной почты, IRC, лент новостей и передачи файлов. Анонимность достигается

за счет многоуровневого шифрования, организации туннелей для передачи данных и их перестроения через определенные промежутки времени, использования идентификаторов абонентов, не связанных с реальными IP-адресами *(схема 1)*.

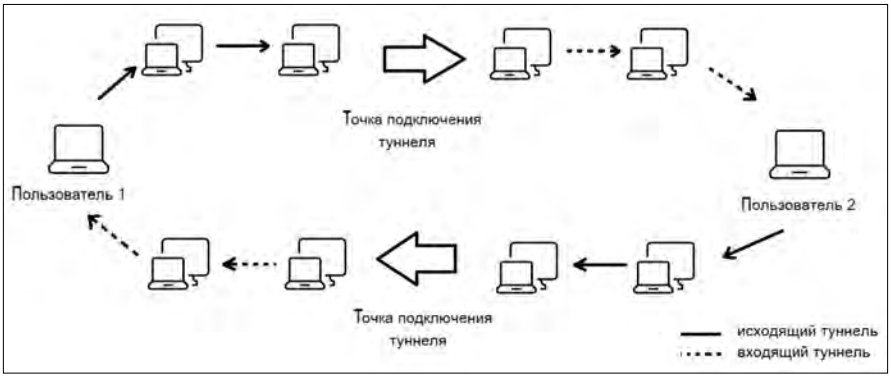

Схема 1. Алгоритм работы I2P

Примерами гибридных анонимных сетей являются: виртуальные частные сети (Virtual Private Network, VPN) и The Onion Router (TOR) *(схемы 2, 3)*. Основная задача этих сетей – обеспечение анонимности пользователей. Это достигается использованием шифрования, туннелирования, а также использованием некеширующих прокси, подменой заголовков сетевых пакетов и данных таким способом, что это не позволяет идентифицировать отправителя.

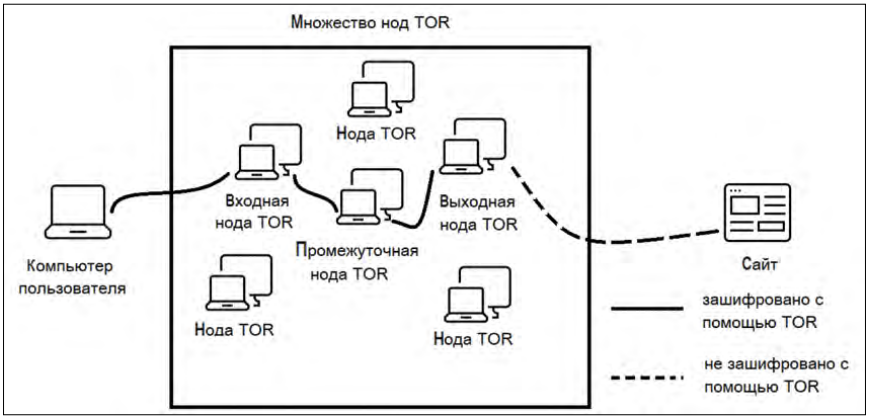

Схема 2. Архитектура TOR

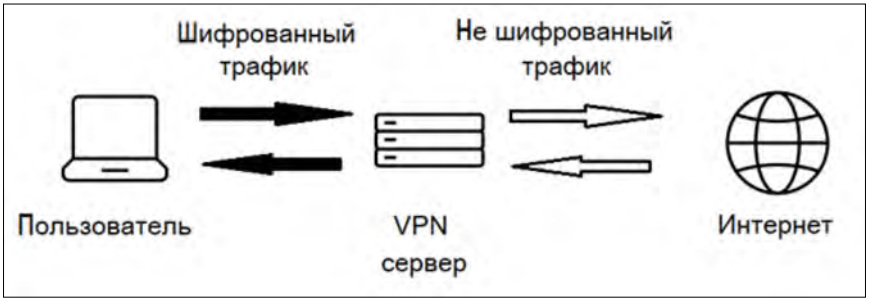

Схема 3. Алгоритм работы VPN

Наиболее значимыми угрозами использования таких сетей являются:

– отсутствие процедур проверки и контроля операторов «нод» (коммуникационных узлов). Это влечет за собой возможность злоумышленников относительно просто регистрировать «выходные ноды» таких сетей и управлять ими в соответствии со своими намерениями;

– отсутствие единых стандартов предоставления услуг и возможности оперативного решения возникающих проблем. В случае использования ресурсов таких сетей в противоправных действиях процедуры разрешения таких проблем нечеткие и осложнены множеством особенностей функционирования подобных инфраструктур;

– потенциальная возможность использования уязвимых клиентских приложений. Это может быть связано как с уязвимостями в официальном клиенте сети, так и в сторонних, либо заведомо созданных для осуществления противоправных действий;

– вмешательство в работу подобных сетей третьих сторон. В данном случае отмечаются опасения многих пользователей о том, что за работой некоторых анонимных сетей могут стоять спецслужбы различных стран. К примеру, Washington Post писала о том, что NSA (Агентство Национальной Безопасности США) деанонимизировала пользователей сети TOR с помощью подконтрольных агентству нод.

Говоря о причинах использования IoT-устройств в противоправной деятельности, необходимо отметить следующее. Количество IoT-устройств в настоящее время по разным оценкам составляет более 22 млрд. Поскольку концепция «умных» вещей активно развивается, количество таких устройств будет в дальнейшем только увеличиваться. Такие устройства имеют доступ в сеть Интер-

нет и позволяют хранить, передавать и обрабатывать информацию, получаемую из сети. При этом IoT-устройства имеют некоторые особенности, которые делают их частой мишенью киберпреступности. По сравнению с полноценными компьютерными системами практически отсутствует практика постоянного администрирования устройств IoT. Домашние роутеры, камеры, компоненты «умного» дома, роботы пылесосы и т. д. находятся во владении простых пользователей, которые не задумываются о том, что, помимо использования таких устройств, необходимо так же их информационное обслуживание, своевременное обновление, внедрение базовых практик информационной безопасности. Большинство пользователей не меняют заводские логины/пароли от панелей администрирования таких устройств, не производят обновления внутреннего программного обеспечения, что делает их уязвимыми для большого количества атак.

Используя заводские учетные данные, уязвимости в устаревшем ПО, ненадежные либо неправильно сконфигурированные механизмы безопасности и иные методы, злоумышленники получают доступ к системам управления такими устройствами. Получив доступ к одному, либо, в большинстве случаев, к тысячам таких устройств, злоумышленники могут осуществлять следующие противоправные сценарии атак:

1. Заражение вредоносным ПО уязвимых устройств в целях создания бот-сетей (botnet). Исходя из того, что рассмотренным выше проблемам подвержено огромное количество устройств, появляется все больше новых видов «бот-нетов» с тысячами зараженных IoT-устройств. Подобные бот-сети чаще всего используются для осуществления DDoS-атак, организации SOCKS-прокси провайдеров, а также распространению вредоносного контента. Развитию IoT «бот-нетов» также способствовала публикация в открытом доступе исходного кода «Mirai» – наиболее известного IoT-бота. На сегодняшний день на различных подпольных площадках в Даркнете размещены десятки объявлений о предоставлении в аренду бот-сетей, а также услуги прямого их использования. Это подтверждает тот факт, что IoT-устройства вызывают большой интерес у киберпреступного сообщества, и с ростом их количества проблема продолжит усугубляться.

2. Использование доступа к уязвимым IoT-устройствам как отправной точки для компрометации корпоративных сетей. Известны случаи, когда уязвимые IoT-устройства позволяли осуществлять проникновение в корпоративные сети предприятий (отчет Microsoft об APT28). При проведении целенаправ-

ленных атак уязвимые IoT-устройства могут помогать злоумышленникам обходить основные механизмы безопасности и осуществлять деструктивные действия в корпоративных сетях компаний.

3. Осуществление атак на устройства IIoT (Industrial Internet of Things). В последнее время все большее распространение в сфере промышленности получают IIoT-устройства. Зачастую они выполняют важные для процесса производства функции или контролируют критические процессы, в связи с чем представляют большой интерес для преступных действий. Поскольку сама сущность таких устройств схожа с «классическими» IoT-устройствами, IIoT унаследовали те же пробелы безопасности и так же являются уязвимыми.

4. Использование IoT-устройств в атаках MITM (Man-in-the-middle) или иных целенаправленных атаках на пользователей. Поскольку количество «умных» домашних устройств с доступом к сети Интернет продолжает увеличиваться, интерес злоумышленников к получению доступа к ним продолжит расти. Вариативность сценариев подобных атак с использованием домашних IoT-устройств очень велика. В случае если объект воздействия – маршрутизатор, злоумышленники, получив доступ к административной панели, могут осуществлять множество MITM-атак, таких как DNS spoofing, сниффинг трафика и т. д. Механизм таких атак основан на том, что пользователь вводит учетные данные на фишинговом ресурсе злоумышленников либо на легитимном ресурсе, с которого в результате сниффинга (контроля) трафика могут быть извлечены учетные данные.

Нередко уязвимые IoT-устройства позволяют преодолевать физические механизмы безопасности (сигнализации, умные замки, двери, окна, ворота), а также выполнять вполне физические деструктивные действия (сбой в пожарной сигнализации, вызванный атакой на его систему управления, повлечет срабатывание механизмов тушения).

Оценивая перспективы внедрения IoT-устройств и возможности их использования в противоправной деятельности, следует ожидать расширения сферы их применения. Уже сегодня набирает обороты внедрение IoT-устройств в промышленности, «умные» устройства в недалеком будущем будут использоваться во все большем количестве промышленных процессов и получать большую автономию, сокращая прямую зависимость от ручного контроля. С ростом количества таких процессов и их «критичности», безусловно, возрастет и интерес преступности к атакам на такие устройства.

Помимо IIoT, «умные» устройства с доступом к информационно-телекоммуникационным сетям также внедряются в другие системы и механизмы, в частности, в автомобильный транспорт – начиная от датчиков, заканчивая системами управления автомобилем (например, автопилот «Tesla»); воздушные и морские суда; беспилотные летательные аппараты и зонды; логистические системы и т. д. В таких случаях получение злоумышленниками несанкционированного доступа к устройствам IoT может нести не только угрозу информационной безопасности субъектов, а также и физическую угрозу жизни и здоровью людей.

Для минимизации рассмотренных рисков и сценариев неправомерных действий, на наш взгляд, разумно *руководствоваться следующими принципами при внедрении, применении и эксплуатации IoT-устройств:*

1. Развитие механизмов информационной безопасности устройств параллельно развитию основного функционала устройств. Данным принципом должны руководствоваться разработчики таких устройств при их создании. Зачастую аспектами информационной безопасности пренебрегают при разработке устройства, концентрируя внимание лишь на конечной функции устройства.

2. Применение комплекса методов контроля и ограничения доступа к таким устройствам. В данном случае принцип применим при внедрении или интеграции IoT-устройств. В применяемые методы могут входить: запрет на доступ к устройству из внешних сетей (при наличии возможности); white lists на административные панели и панели управления устройствами; разграничение прав доступа пользователей и иные методы контроля доступа.

3. Минимизация количества контролируемых такими устройствами процессов, объема доступной им информации, установление прав доступа на минимально необходимые. Суть этой рекомендации состоит в том, чтобы IoT-устройство имело возможность взаимодействия лишь с теми процессами (с той информацией), которые(ая) необходимы для его нормального функционирования, при этом исключая излишние возможности.

4. Изменение подхода к первичному конфигурированию и последующему администрированию устройств. Данная рекомендация состоит в том, что необходимо уделять внимание надлежащей настройке и администрированию не только основных компьютерных систем, а также и устройств IoT как в корпоративных структурах, так и в частных. Надлежащая первичная настройка и своев-

ременное обновление программного обеспечения IoT-устройств уменьшат риск быть атакованным.

5. Внедрение решений по мониторингу и предотвращению атак на IoT-устройства.

6. Применение политики «Нулевого доверия». В данном случае подразумевается необходимость иметь дополнительные «барьеры», обеспечивающие безопасность в случае компрометации IoT-устройства.

7. Проактивный подход к обнаружению уязвимых устройств. В данном случае подчеркивается важность предупреждения возможных инцидентов и ликвидация уязвимостей до обращения на них внимания злоумышленников. Принцип предполагает развитие подхода Threat Hunting, проведения независимых исследований, взаимодействие как независимых исследователей, так и организаций.

Одной из уязвимостей таких сетей является возможность получения контроля над выходными нодами – финальными прокси-серверами в сетях с «луковичной маршрутизацией», которые отвечают за обращения к запрашиваемым ресурсам, получение и последующую передачу контента пользователю по цепочке прокси-серверов в обратном направлении. Группы так называемых «плохих нод» – нод, функционирующих в противоправных целях, регулярно появляются в децентрализованных сетях, что позволяет злоумышленникам осуществлять контроль трафика отдельных пользователей с целью перехвата учетных данных пользователей, данных платежных сервисов и т. д. Для исключения использования SSL-шифрования применяются атаки типа SSLStripping или noHTTPS, при которых соединения выполняются с использованиями незашифрованных протоколов передачи данных. В таких сценариях, как правило, перехват данных производится незаметно для пользователя. При этом для сокрытия нелегитимных действий владельца выходной ноды перехват происходит только с определенных ресурсов, таких как криптовалютные биржи, криптокошельки, аккаунты на форумах и соцсетях и т. д.

Исходя из того, что анонимные децентрализованные компьютерные сети не имеют надежных процедур проверки и контроля операторов «нод», а также эффективных механизмов по противодействию подобным сценариям, вопрос безопасности таких сетей встает особенно остро. Учитывая рост числа пользователей данных сетей, привлекательность такого рода атак для злоумышленников будет только возрастать.

Минимизировать данные риски можно за счет установления запрета либо контроля на использование таких сетей: запрет доступа к IP-адресам узлам анонимных сетей; фильтрация как входящего, так и исходящего трафика, использование средств мониторинга сетевого периметра и предотвращения вторжений; установление иных ограничений на использование корпоративной сети. При этом рост популярности таких сетей, отмечаемый в настоящее время и способствующий росту числа выходных нод, контролируемых злоумышленниками, в перспективе может привести к массовому подрыву доверия пользователей к подобным сетям.

Учитывая, что существующие механизмы обеспечения анонимности и безопасности пользователей децентрализованных анонимных сетей не позволяют в полной мере гарантировать декларируемую анонимность и безопасность их использования, возможны в перспективе изменения в организации построения данных сетей и появление принципиально новых компьютерных сетей, функционирующих по иным правилам.

4. Прогноз развития тенденций криминальной деятельности с использованием цифровых технологий и предложения по их нейтрализации

Как было отмечено во втором разделе настоящей работы, в период распространения новой коронавирусной инфекции COVID-19 стала отчетливо проявляться сложившаяся на протяжении прошедших 10–15 лет зависимость государственного управления, экономики, жизнедеятельности отдельных граждан и организаций от бесперебойного функционирования цифровой инфраструктуры и электронных сервисов. В этих условиях особенно чувствительны негативные последствия противоправных посягательств на цифровые данные граждан и организаций, а также процессы их создания, обработки, хранения. Соответственно, приоритетной задачей является создание таких правовых механизмов функционирования цифровой экономики и развития информационно-телекоммуникационных технологий, при которых обеспечение информационной безопасности не сводило бы на нет неоспоримые достоинства цифровой трансформации в виде повышения производительности труда и не создавало бы излишних ограничений для осуществления деятельности в цифровом пространстве.

Прогнозируя дальнейшее развитие структуры и динамики преступлений, совершенных с использованием информационно-телекоммуникационных технологий, представляется необходимым отметить следующее:

1. Несмотря на сокращение объема ограничений и запретов, вызванных мерами по ограничению распространения коронавирусной инфекции COVID-19, значительная доля работников продолжает выполнять свои трудовые функции в дистанционном режиме. Существует высокая вероятность увеличения их числа в случае ухудшения санитарно-эпидемиологической обстановки вследствие второй волны COVID-19. Соответственно, с марта 2020 г. существенно возросла нагрузка на телекоммуникационную инфраструктуру, что значительно облегчает возможность организации критических нагрузок и DDOS-атак. Работа в дистанционном режиме приводит к увеличению спроса на использование сервисов видеоконференций, онлайн-обучения, мобильных приложений для доставки еды и т. д., что дает основания прогнозировать рост числа мошеннических сайтов-«клонов» в данном сегменте рынка. Наконец, использование в дистанционной работе личной электронной почты и оборудования повышает уязвимость информационных

систем организаций и упрощает распространение вредоносного программного обеспечения.

2. Развитие интернет-торговли, рост числа онлайн-транзакций и популярности банковских онлайн-приложений повлечет увеличение объема фишинговых рассылок предложений дистанционной продажи товаров, заказов выполнения работ, оказания услуг. В этих условиях следует ожидать также увеличение числа предложений легкого заработка, например, за счет получения налоговых вычетов, получения государственных мер социальной поддержки с предварительным перечислением определенной суммы за подробные инструкции.

3. Осложнение финансово-экономической ситуации способно повлечь рост числа нарушений договорных и финансовых обязательств, что в свою очередь вызовет увеличение фиктивных предложений, связанных с урегулированием взысканий, отсрочкой по выплате кредитов или помощи в проведении упрощенной процедуры банкротства.

4. Развитие технологий «Интернета вещей» и рост популярности «умных устройств» повлечет увеличение количества инцидентов, связанных со сбором подробностей частной жизни и иной личной информации пользователей с целью дальнейшего шантажа. Домашние «IP-камеры» позволяющие наблюдать за пользователями в реальном времени; роботы-пылесосы, оснащенные различными датчиками, сканирующими помещения, камерой; видеоняни и иные подробные устройства могут быть использованы в противоправных целях. Представляется, что в дальнейшем популярность и уровень внедрения таких устройств будет продолжать расти с увеличением при этом степени автономности IoT-устройств в таких системах, а также степени важности подконтрольных устройству процессов будет возрастать и интерес злоумышленников к проведению атак на подобные устройства.

5. Развитие анонимных децентрализованных сетей, а также виртуальных валют в условиях отсутствия механизмов их государственного контроля приведет к резкому скачку числа преступлений, связанных с дистанционным сбытом объектов, изъятых из гражданского оборота, в первую очередь, наркотических средств и психотропных веществ.

6. Совершенствование технологий искусственного интеллекта несет риски их использования в противоправных целях, в частности, при формировании и распространении фальшивых новостей (включая контент социальных сетей, «фейковых» видеосюжетов и т. п.), манипулировании массовым сознанием, прочей фальсифи-

кации данных. Кроме того, они способны повысить эффективность фишинговых атак, обеспечить автоматическое обнаружение уязвимостей в информационных системах.

В целях минимизации негативных последствий перечисленных выше прогнозных явлений предлагается следующий *комплекс мероприятий:*

1. Мероприятия по предупреждению и профилактике преступлений, совершенных с использованием информационно-телекоммуникационных технологий:

а) продолжение ведения органами внутренних дел, финансово-кредитными организациями, органами государственной власти субъектов Российской Федерации и местного самоуправления разъяснительной работы в средствах массовой информации, социальных сетях, телевизионных и Telegram-каналах по новым способам мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий;

б) повышение активности виктимологической профилактики киберпреступлений с использованием в этой работе потенциала коммерческих организаций, осуществляющих деятельность в сфере обеспечения кибербезопасности, а также образовательных организаций путем проведения вебинаров, размещения в социальных сетях актуальной информации о киберрисках и способах их снижения;

в) включение в образовательные программы по учебной дисциплине «Основы безопасности жизнедеятельности» для высших, средне-профессиональных и общеобразовательных учреждений тем, связанных с основами цифровой безопасности, правил использования персональных данных в сети Интернет, способов защиты информации на электронных носителях, и т. п.

2. Мероприятия по материально-техническому и кадровому обеспечению деятельности правоохранительных органов:

а) обеспечение недопустимости технологического отставания правоохранительных органов от современного уровня развития информационно-телекоммуникационных технологий и искусственного интеллекта, осуществление постоянного мониторинга технологических достижений и оценки рисков их противоправного использования с целью выработки научно обоснованных рекомендаций по выявлению, раскрытию и расследованию преступлений, совершенных с их использованием;

б) создание при Министерстве цифрового развития Экспертного совета по вопросам предупреждения угроз противоправного использования информационно-телекоммуникационных технологий с участием представителей МВД России, профильных научных

и образовательных организаций, специалистов негосударственных организаций, имеющих признанные компетенции в сфере информационно-телекоммуникационных технологий, для постоянного обмена информацией и выработки совместных решений в сфере противодействия IT-преступности;

в) повышение квалификации руководителей и сотрудников подразделений по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий, а также профессорско-преподавательского состава образовательных организаций системы МВД России в профильных образовательных организациях, чьи компетенции являются признанными в данной сфере.

3. Внесение изменений в законодательство по следующим направлениям:

а) в условиях роста числа мошенничеств, совершенных дистанционным способом, с использованием неправомерно полученных персональных данных, повышается степень общественной опасности преступлений, предусмотренных ст. 183 УК РФ (незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе). В этих условиях целесообразно усиление уголовной ответственности за совершение данного деяния;

б) в целях противодействия совершению противоправных действий в сети Интернет лицами, скрывающими свои подлинные персональные данные, предлагается:

– в условиях широкого использования в противоправной деятельности средств пользователей в сети Интернет (анонимайзеры, прокси-серверы, VPN-туннели, программное обеспечение TOR и др.), Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» следует дополнить нормой, возлагающей на интернет-провайдеров обязанности по блокированию доступа к информационным ресурсам, обеспечивающим сокрытие сведений о личности пользователя сети Интернет или используемом им оборудовании, программном обеспечении или действиях, совершенных в сети, в соответствии с перечнем, формируемым на основании предложений органов, осуществляющих оперативно-розыскную деятельность. В настоящее время подобный механизм уже реализован на законодательном уровне в отношении блокирования доступа к информационно-телекоммуникационным сетям и информационным ресурсам, посредством которых обеспечивается доступ к ранее заблокированным

ресурсам, содержащим информацию, распространение которой в Российской Федерации запрещено (порнографические изображения несовершеннолетних, способы изготовления наркотических средств, способы суицида и др.). Предлагается расширить сферу применения указанной нормы;

– ввести законодательное требование использования универсального порядка регистрации организаторами распространения информации в сети Интернет своих пользователей с использованием единой системы идентификации и аутентификации[1];

в) с целью повышения эффективности противодействия преступлениям, совершенным с использованием «социальной инженерии», представляется целесообразным:

– урегулировать правовое положение и особенности функционирования IP-телефонии как особого вида связи, предусмотрев механизм идентификации абонентов с подтверждением персональных данных, установив технологические требования к серверному оборудованию, регламентировать деятельность организаций, предоставляющих услуги связи в сфере IP-телефонии, ввести механизм лицензирования их деятельности и контроля соблюдения лицензионных требований[2];

– введение ограничений для передачи голосового трафика из сетей передачи данных в телефонную сеть связи общего пользования, допуская его только для достоверно установленных пользователей;

– установление уголовной ответственности за нарушения в области подмены номера и использование ресурса нумерации, не выделенной по договору об оказании услуг связи, как для лица, непосредственно причастного к подмене номера, так и для должностных лиц из числа представителей операторов связи, допустивших возможность осуществления «криминального» звонка, повлекшего причинение значительного материального ущерба;

– возложение на банки обязанности осуществлять подтверждение использования нового устройства и перевыпущенных сим-карт для работы в системах дистанционного банковского обслуживания только при личном визите клиента в офис банка или при гарантированной дистанционной идентификации банком личности клиента, а также установления ограничения на сумму проводимых операций по банковским счетам и вкладам клиента до подтверждения легитимности использования нового устройства или сим-карты;

---

[1] Письмо МВД по Республике Татарстан от 29 августа 2020 г. № 1/2045.

[2] Письмо УМВД России по Пензенской области от 31 августа 2020 г. № 2/2559.

– возложение на операторов связи обязанности по осуществлению блокировки трафика с абонентских номеров, внесенных в модуль ИБД-Ф «Дистанционное мошенничество» (в т. ч. мошеннических call-центров);

– возложение солидарной ответственности на компании-операторы сотовой связи за нарушения дилерами требований действующего законодательства в части идентификации личности абонента при заключении договора на оказание услуг связи;

г) с целью сокращения сроков расследования преступлений, совершенных с использованием средств подвижной (сотовой) связи, предлагается дополнить положения ст. 64 Федерального закона от 7 июля 2003 г. указанием на конкретные сроки предоставления операторами связи информации по запросам органов, осуществляющих оперативно-розыскную деятельность;

д) с целью недопущения совершения рейдерских захватов активов хозяйствующих субъектов с использованием фальсифицированной электронной подписи и поддельных документов предлагается внести изменения в Федеральный закон от 8 августа 2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей», аналогичные ранее внесенным изменениям в Федеральный закон 13 июля 2015 г. № 218-ФЗ «О государственной регистрации недвижимости», согласно которым при отсутствии в Едином государственном реестре недвижимости записи о возможности регистрации на основании документов, подписанных электронной подписью, заявление о государственной регистрации перехода, прекращения права собственности на соответствующий объект недвижимости, принадлежащий физическому лицу, возвращается без рассмотрения;

е) значительно увеличить размер штрафных санкций по ст. 19.7 КоАП РФ «Непредставление сведений (информации)»;

ж) принимая во внимание рост числа преступлений, связанных с незаконным оборотом оружия, совершенных с использованием информационно-телекоммуникационных технологий, представляется целесообразным дополнение уголовного законодательства Российской Федерации указанием на использование сети Интернет при совершении указанных преступлений как квалифицирующего признака, а также законодательства об информации возможностью блокировки сайтов, содержащих информацию об изготовлении оружия и самодельных взрывных устройств;

з) с целью пресечения распространения фишинговых рассылок, а также распространения иного вредоносного программного обеспечения, дополнить Федеральные законы «О связи» и «Об

информации, информационных технологиях и защите информации» положениями, возлагающими на операторов связи и организаторов распространения информации в сети Интернет, осуществляющих передачу электронных сообщений, осуществлять блокировку таких сообщений, а также СМС, ММС-сообщений, содержащих вредоносные вложения с установлением солидарной гражданско-правовой ответственности за вред, причиненный этим вложением, с отправителем и создателем данного вложения;

и) внедрение при проведении расчетных операций единого идентификатора, присваемого кредитно-финансовыми организациями и платежными системами для каждой транзакции, по которому банк-получатель или платежная система сможет идентифицировать данную операцию. Единый идентификатор финансовых транзакций позволит упростить процесс их анализа без ограничений, установленных законодательством о персональных данных или банковской тайне;

к) установление уголовной ответственности для лиц, участвующих в создании программного оборудования, используемого для сбыта наркотиков, интернет-сайтов и страниц в социальных сетях, на которых размещается информация о сбыте подконтрольных средств и веществ;

л) внести изменения в правила регистрации доменных имен, указав на необходимость личного документального подтверждения личности при обращении за оказанием данной услуги;

м) предусмотреть дополнительные основания для блокировки на территории Российской Федерации доступа к информационным ресурсам, расположенным в иностранных юрисдикциях, связанные с поступлением в органы внутренних дел заявлений по факту мошеннических действий с использованием данного информационного ресурса или его выявления в ходе мониторинга сети в рамках оперативно-розыскной деятельности[1];

н) с целью защиты несовершеннолетних от запрещенного контента обязать социальные сети, ведущие свою деятельность на территории России, обеспечить регистрацию страниц несовершеннолетних только после согласия и верификации родителями или опекунами, что позволит усилить контроль за деятельностью несовершеннолетних в сети;

---

[1] Письмо ГУ МВД России по Санкт-Петербургу и Ленинградской области от 28 августа 2020 г. № 54/3743; письмо УМВД России по Пензенской области от 31 августа 2020 г. № 2/2559.

о) внести изменения в постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе “Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено”», дополнив Правила создания, формирования и ведения вышеназванной автоматизированной информационной системы в части расширения полномочий Министерства внутренних дел Российской Федерации по принятию решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в сети Интернет, а также сетевых адресов в единый реестр, в отношении информации, размещенной в целях совершения мошенничества и хищения денежных средств со счетов банковских карт с использованием вредоносного программного обеспечения.

Предлагаются следующие критерии оценки информации для включения доменных имен и (или) указателей страниц сайтов в сети Интернет, а также сетевых адресов в единый реестр:

1) установленный факт совершения преступления, квалифицированного по ст. 158–159.6 УК РФ с использованием интернет-ресурса (постановление о возбуждении уголовного дела);

2) установленный факт использования интернет-ресурса в целях совершения хищения денежных средств с использованием программно-технических средств (по результатам судебной программно-технической экспертизы)[1].

4. Укрепление международного сотрудничества в сфере противодействия киберпреступности, имплементация инициатив Российской Федерации в области международной информационной безопасности[2].

Финансовое и организационное обеспечение реализации указанных мероприятий предлагается осуществить в рамках национального проекта «Цифровая экономика Российской Федерации»[3].

В заключение следует отметить, что рассмотренные выше правовые меры, направленные на снижение криминогенного потен-

[1] Письмо МВД по Республике Коми от 28 августа 2020 г. № 1/6865.

[2] URL: http://www.kremlin.ru/events/president/news/64086 (дата обращения: 15.06.2021).

[3] Утв. протоколом заседания Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

циала информационно-телекоммуникационной сферы, способны привести к ощутимым результатам в виде сокращения уровня высокотехнологичной преступности при условии изменения общественного сознания относительно приватности в интернет-пространстве. Интернет должен стать прозрачным и открытым пространством, в котором использование средств анонимизации представляет собой девиацию, требующую реакции со стороны надзорных органов, сравнимой с той, которая влечет появление в центре города человека в натянутой на лицо шапке с прорезями для глаз. Именно подобное отношение к использованию средств анонимизации как со стороны надзорных органов, так и со стороны общества в целом, способно переломить существующие негативные тенденции использования информационно-телекоммуникационных технологий в противоправных целях.

Список литературы

Нормативные акты

Конституция Российской Федерации [Электронный ресурс]: принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. Доступ из справ.-правовой системы «КонсультантПлюс».

Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма [Электронный ресурс]: заключена в г. Варшаве 16 мая 2005 г., ратифицирована Федеральным законом Российской Федерации № 183 от 26 июля 2017 г. Доступ из информ.-правового портала «Гарант».

Уголовный кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 13 июня 1996 г. № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ (ред. от 1 июля 2021 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

О полиции [Электронный ресурс]: Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс».

О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма [Электронный ресурс]: Федеральный закон от 7 августа 2001 г. № 115-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Вопросы Федеральной службы по финансовому мониторингу (вместе с «Положением о Федеральной службе по финансовому мониторингу») [Электронный ресурс]: указ Президента Российской Федерации от 13 июня 2012 г. № 808. Доступ из информ.-правового портала «Гарант».

О развитии искусственного интеллекта в Российской Федерации [Электронный ресурс]: указ Президента Российской Федерации от 10 октября 2019 г. № 490. Доступ из справ.-правовой системы «КонсультантПлюс».

Паспорт национального проекта «Национальная программа “Цифровая экономика Российской Федерации”» [Электронный ресурс]: утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным про-

ектам, протокол от 4 июня 2019 г. № 7. Доступ из справ.-правовой системы «КонсультантПлюс».

Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2 [Электронный ресурс]: утв. Президиумом Верховного Суда Российской Федерации 30 апреля 2020 г. Доступ из информ.-правового портала «Гарант».

О совершенствовании деятельности по раскрытию и расследованию преступлений, совершенных с использованием информационных технологий [Электронный ресурс]: решение коллегии МВД России от 22 мая 2014 г. № 2км/2. Доступ из справ.-правовой системы СТРАС «Юрист».

О мерах по совершенствованию организации раскрытия и расследования мошенничеств [Электронный ресурс]: решение коллегии МВД России от 24 октября 2017 г. № 3км. Доступ из справ.-правовой системы СТРАС «Юрист».

О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий [Электронный ресурс]: решение коллегии МВД России от 1 ноября 2019 г. № 3км. Доступ из справ.-правовой системы СТРАС «Юрист».

Литература

Абдрахманова Г.И. и др. Цифровая экономика: 2020 : краткий статистический сборник. Москва: НИУ ВШЭ, 2020.

Аналитический обзор «Комплексный анализ состояния преступности в Российской Федерации по итогам 2020 года и ожидаемые тенденции ее развития». Москва: ФГКУ «ВНИИ МВД России», 2021.

Балашова А.А. и др. Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании: учебное пособие / под ред. Ю. В. Гаврилина и А. В. Победкина. Москва: Академия управления МВД России, 2021.

Буснюк Н.Н., Мельянец Г.И. Системы мобильной связи. Минск: БГТУ, 2018.

Гаврилин Ю.В. Криминалистика: угрозы и вызовы современности // Криминалистика и новые вызовы современности (58-е криминалистические чтения). Сборник статей Всероссийской

научно-практической конференции. Москва: Академия управления МВД России, 2018.

Гаврилин Ю.В. Противодействие цифровой трансформации наркопреступности (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 4 (56).

Гаврилин Ю.В., Гаспарян Г.З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: учебное пособие. Москва: Проспект, 2021.

Гаврилин Ю.В., Парадников А.Г. Совершенствование выявления, раскрытия и расследования хищений, совершенных с использованием информационных банковских технологий (по итогам всероссийского онлайн-семинара) // Труды Академии управления МВД России. № 2 (54). 2020.

Гаврилин Ю.В., Шурухнов В.А. О правовых предпосылках применения отдельных способов сокрытия преступлений, совершенных с использованием информационно-коммуникационных технологий // Академическая мысль. 2017. № 1. URL: https://mvd.ru/upload/site120/folder_page/010/368/829/Akademicheskaya_mysl_1-2017.pdf

Коробеев А.И., Дремлюга Р.И., Кучина Я.О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. № 3.

Чернец В., Базлова Т., Иванова Э. Влияние через социальные сети / под общ. ред. Е. Г. Алексеевой. Москва: Фонд «ФОКУС-МЕДИА», 2010.

Gavrilin Yu.V., Pavlichenko N.V., Vasilieva M.A. The Remote Approach of Distribution of Objects Withdrawn from Circulation: Means, Legislation Issues, Solutions // Studies in Systems, Decision and Control. Vol. 181. Big Data-driven World: Legislation Issues and Control Technologies. Chapter 8. С. 85–93.

Интернет-источники

URL: http://www.kremlin.ru/events/president/news/64086.

URL: http://kremlin.ru/events/president/news/65090.

URL: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

URL: https://br-analytics.ru/blog/social-media-russia-2019/.

URL: https://cyberpolygon.com/ru/.

URL: https://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf.

URL: http://glagol-book.info/.
URL: https://www.group-ib.ru/media/double-cheating/.
URL: https://www.interfax.ru/russia/708250.
URL: https://issek.hse.ru/digec2020.
URL: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.
URL: https://www.kaspersky.ru/about/press-releases/2020.
URL: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-79-rossiyan-ne-poluchali-rekomendatsii.
URL: https://www.kaspersky.ru/blog/ginp-trojan-coronavirus-finder/27762/.
URL: https://www.kommersant.ru/doc/4337079.
URL: https://www.mos.ru/news/item/73933073/.
URL: https://www.rbc.ru/finances/27/08/2020/5f468fa59a7947858f2c197e.
URL: https://www.rbc.ru/rbcfreenews/5ed5ca639a7947a832ce9916.
URL: https://www.rbc.ru/society/20/05/2020/5ec4ae819a79476af7b97228.
URL: https://www.rbc.ru/technology_and_media/31/03/2020/5e81fa5e9a7947c6b6442bac.
URL: https://ria.ru/20200512/1571325897.html.
URL: https://tass.ru/ekonomika/7621137.
URL: https://unctad.org/en/PublicationsLibrary/der2019_overview_ru.pdf.

Учебное издание

Гаврилин Юрий Викторович

О НАУЧНЫХ ПОДХОДАХ К ПРОБЛЕМЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕСТУПНЫХ ЦЕЛЯХ

Учебное пособие

Редактор *В. А. Яровая*
Верстка *А. А. Мельникова*

Подписано в печать 24.09.2021. Формат 60x84 $^{1}/_{16}$.
Усл. печ. л. 4,2. Уч.-изд. л. 3,9. Тираж 64 экз. Заказ № у.

Отделение полиграфической и оперативной печати РИО
Академии управления МВД России.
125993, Москва ул. Зои и Александра Космодемьянских, д. 8

ISBN 978-5-907187-86-3