Предупреждение девиаций в цифровом мире уголовно-правовыми средствами

Ю.В. Грачева

профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), доктор юридических наук. Адрес: 125993, Российская Федерация, Москва, Садовая-Кудринская ул., 9. E-mail: uvgracheva@mail.ru

С.В. Маликов

старший преподаватель кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук. Адрес: 125993, Российская Федерация, Москва, Садовая-Кудринская ул., 9. E-mail: s.v.malikov@yandex.ru

А.И. Чучаев

профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), доктор юридических наук. Адрес: 125993, Российская Федерация, Москва, Садовая-Кудринская ул., 9. E-mail: moksha1@rambler.ru

Аннотация

Любой прогресс оказывает как положительное влияние на развитие общества, так и порождает риски причинения вреда общественным отношениям, часть из которых являются криминальными. Предметом исследования выступают новые технологии, которые могут быть использованы для причинения вреда охраняемым уголовным законом общественным отношениям. Целями работы являются определение механизма нарушения общественных отношений путем применения новых технологий и разработка адекватных уголовно-правовых мер по предотвращению девиаций в цифровом мире. Применены общенаучные (диалектический, логический, системный) и специально-юридические (сравнительно-правовой, формально-юридический, юридического моделирования) методы. Одной из популярных техник социальной инженерии выступает фишинг, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Совершение хищения чужого имущества с использованием полученной конфиденциальной информации влечет уголовную ответственности по п. «г» ч. 3 ст. 158 УК РФ. Фишинговые письма, как правило, содержат различного рода программы (трояны). Эти программы используются виновным, во-первых, при хищении денежных средств, например путем предоставления через удаленный доступ к управлению банковским счетом потерпевшего и т.д. Во-вторых, указанные программы применяются при вымогательстве имущества потерпевшего под угрозой уничтожения информации, хранящейся на компьютере. Подобные деяния могут быть квалифицированы только по совокупности ст. 272 и 273 УК РФ. Статью 163 УК РФ необходимо дополнить указанием на такой способ совершения преступления,

как угроза уничтожения информации. Схожими по общественно опасным последствиям для потерпевшего являются DoS-атаки. Рассмотрены пять самых известных кибератак, определен механизм причинения вреда объектам уголовно-правовой охраны, который показал необходимость уточнения редакций ст. 272 и 273 УК РФ. Рассмотрены также технология блокчейн и созданная на ее основе криптовалюта, искусственный интеллект и робототехника, определены уголовно-правовые риски и предложены оценки вреда в случае его причинения. Изменение гражданско-правового регулирования общественных отношений, возникающих в связи с рассмотренными новыми технологиями, может привести и к изменению уголовно-правовой оценки преступления, совершаемого с их использованием.

Ключевые слова

девиации, цифровой мир, уголовно-правовые риски, социальная инженерия, Dos-атаки, мошенничество, искусственный интеллект, роботизация, уголовная ответственность, блокчейн.

Благодарности: Публикация подготовлена при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16158.

Для цитирования: Грачева Ю.В., Маликов С.В., Чучаев А.И. Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право. Журнал Высшей школы экономики. 2020. № 1. С. 188–210.

УДК: 343 DOI: 10.17323/2072-8166.2020.1.188.210

Введение

Очередная промышленная революция не только способствует прогрессу, создавая обществу и государству новые возможности, но и порождает ранее не существовавшие способы и инструменты для совершения преступлений, ведет к возникновению новых видов девиаций в цифровом мире. Одним из средств предупреждения подобного поведения являются уголовно-правовые нормы. Внесению соответствующих запретов в Уголовный кодекс Российской Федерации (далее — УК РФ) или изменению уже имеющихся норм должно предшествовать выявление угроз охраняемым уголовным законом общественным отношениям, определение механизма причинения им вреда, оценка степени общественной опасности последнего. Если деяние по характеру и степени общественной опасности соответствует преступлению, то вначале необходимо проанализировать Особенную часть УК РФ на наличие соответствующего запрета и актуальности (адекватности) его изложения в уголовном законе, и только при отсутствии нормы дополнить УК РФ новым составом преступления.

Такое исследование возможно лишь на основе общенаучного и специально юридического методов исследования.

1. Метод социальной инженерии: криминальные риски

Значительная часть киберугроз экономике основана на методе *социальной инженерии*, позволяющем получить конфиденциальную информацию для противоправного завладения чужим имуществом. «Все техники социальной инженерии основаны на когнитивных искажениях. Эти ошибки в поведении используются социальными инженерами для создания атак, направленных на получение конфиденциальной информации, часто с согласия самой жертвы.

Одной из популярных техник социальной инженерии выступает *фишинг*, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Наиболее традиционным примером фишинговой атаки может служить сообщение, отправленное потерпевшему по электронной почте и подделанное под официальное письмо, например, банка или иной платежной системы, требующие проверки определенной информации или совершения определенных действий; крупной и (или) известной компании, например с поздравлением с победой в каком-либо конкурсе, проводимом компанией, в связи с чем срочно требуется изменить учетные данные или пароль. Все эти письма обычно содержат ссылку на фальшивую веб-страницу, в точности похожую на официальную и содержащую форму, требующую ввести конфиденциальную информацию (номер банковской карты, PIN-код и т.д.)»[1].

Совершение хищения чужого имущества с использованием таким образом полученной конфиденциальной информации влечет уголовную ответственности за кражу с банковского счета (или кражу, совершенную в отношении электронных денежных средств) по п. «г» ч. 3 ст. 158 УК РФ.

Фишинговые письма могут содержать различного рода программы (трояны), которые загружаются на компьютеры, смартфоны и другие технические устройства жертвы без ее согласия в случае прочтения письма и перехода по указанным в нем ссылкам. Распространенная разновидность такой программы — троян, шпионящий за потерпевшим. Он собирает необходимые сведения и может: а) дать виновному возможность ручного перевода средств с чужого банковского счета (или электронных денежных средств) через удаленный доступ; б) осуществить автозалив (программа, позволяющая во вре-

[1] Available at: https://www.consumer.ftc.gov/articles/howrecognize-and-avoid-phishing-scams (дата обращения: 1.07.2019)

мя формирования платежного поручения владельцем счета незаметно для него подставить другие реквизиты для перевода денежных средств).

Ответственность за такое хищение будет наступать согласно разъяснениям, содержащимся в Постановлении Пленума Верховного Суда Российской Федерации от 30. 11. 2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[2], по соответствующим частям ст. 159[6] и ст. 272 УК РФ.

Эта рекомендация Пленума небезупречна. Статья 159[6] УК РФ называется «Мошенничество в сфере компьютерной информации», начало диспозиции нормы повторяет название статьи. Вместе с тем из последней следует, что деяние, изложенное в ней, совершается путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Таким образом, в ней предусмотрен иной способ хищения, не совпадающий с мошенничеством, т.е. предусмотрена форма хищения, которая мошенничеством называться не может. Пленум Верховного Суда также не относит сформулированное в ст. 159[6] УК РФ преступление к мошенничеству, о чем свидетельствует п. 1 названного Постановления. В этом пункте перечислены статьи, в которых предусмотрена ответственность за мошенничество (ст. 158[1]–159[5] УК РФ), среди них нет ст. 159[6] УК РФ. Пленум безусловно прав, так как представить обман или злоупотребление доверием, осуществленный посредством вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, в результате которого потерпевший «добровольно» передает свое имущество, невозможно.

Отчасти можно согласиться с учеными [Болсуновская Л.М., 2016: 15–20]; [Лопашенко Н.А., 2015: 507], которые считают, что в ст. 159[6] УК РФ сформулирован самостоятельный состав хищения, деяние совершается способом, не присущим ни для одной из форм хищения. Но нужно иметь в виду, что статья называется мошенничеством в сфере компьютерной информации. Поэтому считать это преступление самостоятельной формой хищения нельзя, впрочем, как и квалифицировать какое-либо деяние по этой норме невозможно, поскольку таких преступлений нет и быть не может.

Все деяния, которые Пленумом Верховного Суда РФ рекомендовано квалифицировать по ст. 159[6] УК РФ, должны быть оценены по п. «г» ч. 3 ст. 158 УК РФ как кража с банковского счета или совершенная в отношении электронных денежных средств, и по соответствующей части ст. 272 УК РФ. Такая квалификация, с одной стороны, будет соответствовать букве и духу

[2] Бюллетень Верховного Суда РФ. 2018. № 2.

закону, так как имущество изымается тайно, а, с другой стороны, прекратит развернувшуюся после принятия Постановления Пленума Верховного Суда ненужную полемику, во-первых, относительно того, какое преступление изложено в ст. 159[6] УК РФ; во-вторых, по поводу правильности рекомендации о необходимости квалификации мошенничества в сфере компьютерной информации по совокупности с неправомерным доступом к компьютерной информации (ст. 159[6] и 272 УК РФ) [Кибальник А., 2018: 67].

Фишинг используется не только для хищения имущества у клиентов банков и иных частных лиц, но и у самих банков посредством атак на систему межбанковских переводов, карточный процессинг, управление банкоматами, интернет-банкинг, платежные шлюзы и т.д. Сбербанк оценивает ежегодные убытки от кибератак в России в размере около 600 млрд. руб., а во всем мире эта сумма приближается к 1 трлн. долл. США3. Типовые схемы подобных атак состоят из пяти этапов:

1) разведка и подготовка: программного обеспечения, фишинговых писем, инфраструктуры, в том числе для отмывания денег и их обналичивания и т.д.;

2) проникновение во внутреннюю сеть банка (эффективным и распространенным методом является фишинговая рассылка электронных писем сотрудникам банка, которая осуществляется как на рабочие, так и на личные адреса);

3) развитие атаки и закрепление в Сети (получив доступ к локальной сети банка, виновным необходимо получить полномочия локального администратора на компьютерах сотрудников и серверах для дальнейшего развития атаки. Успешность последней, как правило, обусловлена недостаточным уровнем защищенности систем от внутреннего нарушения);

4) компрометация банковских систем и хищение денег (основными способами хищений выступают перевод средств на подставные счета через системы межбанковских платежей, перевод денежных средств на криптовалютные кошельки, управление банковскими картами и счетами, управление выдачей наличных средств в банкоматах);

5) сокрытие следов (с целью затруднить расследование принимаются меры для уничтожения следов пребывания в системе. Некоторые виновные, понимая, что следы пребывания в системе все равно остаются, предпочитают полностью выводить из строя узлы Сети. Волна атак вирусов-шифровальщиков, с которой мир столкнулся в 2017 г., была примером того, как легко могут быть уничтожены данные крупной компании. В арсенале хакеров есть модифицированные вирусы, которые распространяются по рабочим станциям Сети и шифруют содержимое жестких дисков. Восстановить

[3] Available at: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Banks-attacks-2018-rus.pdf (дата обращения: 29 — 06 — 019)

зашифрованные данные в большинстве случаев невозможно, в связи с чем банк несет ущерб, вызванный вынужденным простоем бизнес-процессов, который может оказаться гораздо значительнее ущерба непосредственно от хищения денежных средств)[4].

Подобные действия соответствуют признакам преступления, предусмотренного ст. 158 УК РФ[5] (скорее всего, п. «б» ч. 4 — в особо крупном размере). Кроме того, ответственность должна наступать по ст. 272, 273 УК РФ. Если речь идет о Центробанке, Сбербанке и других крупных банках, то вместо ст. 272 и 273 УК РФ будет вменяться ст. 274[1] УК РФ, так как банки согласно п. 8 ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[6] относятся к субъектам критической инфраструктуры.

Другой разновидностью компьютерной программы (трояна), содержащейся в фишинговых письмах, могут быть программы-вымогатели. Эта программа блокирует работу компьютера и требует за восстановление функционирования системы перечислить определенную денежную сумму на счет по указанным реквизитам, например на электронный кошелек. В случае невыполнения требования она угрожает уничтожить информацию, хранящуюся на компьютере. Программы-шифровальщики направлены не на повреждение самих компьютеров или их частей, а на уничтожение находящейся в них информации. Деяния влекут ответственность по совокупности: ч. 2 ст. 272 УК РФ (исходя из корыстной заинтересованности) или ч. 4 ст. 272 УК РФ, если наступили тяжкие последствия либо возникла угроза для их наступления; по соответствующей части ст. 273 УК РФ УК РФ, поскольку создание и использование вредоносных программ не охватывается ст. 272 УК РФ. Ответственность по ст. 273 УК РФ должна наступать независимо от того, само виновное лицо написало вредоносную программу или приобрело уже готовую, поскольку общественно опасное деяние в ст. 273 УК РФ выражено альтернативными действиями: создание, распространение и использование. Изложенная позиция находит подтверждение в судебной практике[7].

Само требование перечислить денежные средства под угрозой уничтожения информации (базы данных) не может быть квалифицировано по ст. 163 УК РФ, несмотря на то, что оно направлено на завладение чужим имуществом. Вымогательством признается требование передачи чужого имуще-

---

[4] Ibid.

[5] Согласно Постановлению Пленума Верховного Суда РФ от 30.11.2017 № 48 по соответствующей части ст. 159[6] УК РФ и по статье, предусматривающей ответственность за компьютерное преступление.

[6] СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

[7] См., напр.: Апелляционное постановление Московского городского суда от 27.11.2017 по делу № 10-16199/ 2015 // СПС КонсультантПлюс.

ства под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно распространения сведений, позорящих потерпевшего, и т.д. Согласно ст. 128 ГК РФ, определяющей объекты вещных прав, к которым относится имущество [Данилов Д., 2018: 37–42], информация и базы данных не относятся к имуществу, но могут в некоторых случаях быть объектом гражданских прав. Отсутствие в ст. 163 УК РФ такого способа совершения преступления, как угроза уничтожения информации, не позволяет дать адекватную уголовно-правовую оценку подобным деяниям и является пробелом, который необходимо устранить путем дополнения ч. 1 ст. 163 УК РФ указанием на эту угрозу.

2. DoS или DDoS-атаки (Denial of Service «отказ в обслуживании»): криминальные риски

Схожими по общественно опасным последствиям являются *DoS-атаки (*Denial of Service — «отказ в обслуживании») — «хакерские атаки на вычислительную систему, приводящие к отказу в обслуживании, т.е. создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к системным ресурсам (серверам), либо этот доступ существенно затрудняется. Если атака выполняется одновременно с большого числа компьютеров, то это DDoS-атака. Она проводится, если требуется вызвать отказ в обслуживании хорошо защищенной компьютерной системы крупной компании или правительственной организации. С помощью DDoS-атак с высокой мощностью можно не только отключить один или несколько сайтов, но и нарушить работу всего сегмента Сети или даже отключить Интернет в малой стране»[8].

Цели атаки, как правило: установление контроля над системой, поскольку в нештатной ситуации она может выдать критическую информацию (например, версию, часть программного кода и т.д.); блокировка работы системы, обеспечивающей функционирование сервиса (службы), приносящей высокий доход. Мотивы атак: личная неприязнь, развлечение, политический протест, недобросовестная конкуренция, вымогательство или шпионаж[9].

С уголовно-правовой оценкой подобных действий уже сталкивается судебная практика. Так, группа лиц по предварительному сговору с целью устранения конкурента организовали и провели DDoS-атаку (типа «отказ в обслуживании»), на ее проведение были выделены денежные средства, подготовлена

[8] Available at: URL: https://losst.ru/chto-takoe-ddos-ataka-sut-i-proishozhdenie (дата обращения: 03-07-2019)

[9] Available at: URL: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0 (дата обращения: 03-07-2019)

бот-сеть, написана и использована вредоносная программа. Действия участников группы были квалифицированы по ч. 2 ст. 272 и ст. 273 УК РФ[10].

В этом деле заслуживают внимания разъяснения апелляционной инстанции на жалобу виновных об отсутствии в их действиях состава преступления, предусмотренного ст. 272 УК РФ, так как в результате DDoS-атаки на информационные ресурсы доступ к защищенной законом информации получить не удалось. Московский городской суд пришел к выводу, что доводы в жалобе несостоятельны. «В соответствии с требованиями ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" доступ к информации понимается как возможность ее получения и использования, а поскольку ... в результате ... DDoS-атаки, повлекшей блокирование (то есть невозможность законного доступа к сведениям при их сохранности) работы системы ЭВМ, осужденными была получена возможность неправомерного, несанкционированного доступа к защищенной законом компьютерной информации, о чем свидетельствует то, что в ходе атаки была использована бот-сеть, вредоносная программа, нормальный ход работы ООО «А» был нарушен, а система ЭВМ блокирована, то есть блокированы информационные ресурсы и система ЭВМ, объединенные в единую платежную систему, что судом правильно установлено как неправомерный доступ к компьютерной информации»[11].

Позиция апелляционной коллегии Мосгорсуда небесспорна. Трудно согласиться, что неправомерным доступом к компьютерной информации охватывается невозможность доступа к ней. Этот пример судебной практики свидетельствует, что редакция ст. 272 УК РФ нуждается в уточнении.

Самыми известными кибератаками последнего десятилетия, по данным лаборатории Касперского[12], являются:

1) WannaCry — масштабная атака, основанная на программе-шифровальщике, способной быстро распространяться по Интернету и локальным сетям. За четыре дня она вывела из строя более 200 000 компьютеров в 150 странах мира, в том числе и ряд объектов критической инфраструктуры (так, в некоторых больницах были зашифрованы все устройства, включая медицинское оборудование). Ущерб от атаки по разным данным составил от 4 до 8 млрд. долл.;

2) NotPetya/ExPetr — атака, ущерб от которой оценивается примерно в 10 млрд. долл. Как и в предыдущем случае, использовалась программа-

---

[10] См.: Апелляционное постановление Московского городского суда от 25.11. 2013 по делу № 10-11502/2013 // СПС КонсультантПлюс.

[11] Апелляционное постановление Московского городского суда от 25.11.2013 по делу № 10-11502/2013.

[12] См.: 5 самых легендарных кибератак. Available at: URL: https://www.kaspersky.ru/blog/five-most-notorious-cyberattacks/21607/ (дата обращения: 04-07-2019)

шифровальщик, но последствия оказались менее масштабными; основным ее адресатом стал бизнес — программа была заложена в финансовое программное обеспечение;

3) Stuxnet — атака, которая вывела из строя центрифуги обогащения урана в Иране, замедлив выполнение иранской ядерной программы на несколько лет. После этой атаки начали говорить об использовании кибероружия против промышленных систем. «Ничего более сложного и хитроумного в то время не существовало — червь умел незаметно распространяться через USB-флешки, проникая даже в те компьютеры, которые не были подключены к Интернету или локальной сети»[13]. Вредоносная программа распространилась по всему миру, была опасна для компьютеров, управляемых программируемыми котроллерами и софтом Siemens. Она стала причиной физического разрушения центрифуг для обогащения урана; червь, перепрограммируя контроллеры, задавал слишком большие скорости их вращения;

4) Dark Hotel — программа-шпион, которая внедрялась через публичные сети Wi-Fi в сеть отеля и предлагала его гостям установить на первый взгляд легальное обновление популярного программного обеспечения. Как только это делалось, устройства заражались шпионской программой. Она считывала нажатия клавиш, позволяла организовывать целевые фишинговые атаки. Программа была направлена была на получение конфиденциальной информации топ-менеджеров и высокопоставленных чиновников;

5) Mirai — вредоносная троянская программа, использованная для «Интернета вещей», позволившая получить контроль над ними и объединить в единую сеть (ботнет[14]), которой можно управлять удаленно. С ее помощью 21 октября 2016 г. была осуществлена DDoS-атака на DNS-провайдера Dyn. Последний такой массированной атаки не выдержал. Вместе с ним в США перестали работать PayPal, Twitter, Netfix, Spotify, онлайн-сервис PlayStatition и др.[15]

Обзор DDoS-атак показал, что:

а) средства вычислительной техники, как правило, защищены достаточно, уязвимыми для киберугроз они становятся в результате действий самих потерпевших (прочтения фишинговых писем, доверчивости, использование непроверенных USB-флешок и небезопасных Wi-Fi сетей);

б) уголовно-правовые средства противодействия нуждаются в корректировке. Так, ч. 1 ст. 272 УК РФ следует дополнить указанием на «неправо-

[13] Там же.

[14] Слово Botnet (ботнет) образовано от слов «robot» (робот) и «network» (сеть). Киберпреступники используют специальные троянские программы, чтобы обойти систему защиты компьютеров, получить контроль над ними и объединить их в единую сеть (ботнет), которой можно управлять удаленно. Available at: URL: https://www.kaspersky.ru/resource-center/threats/botnet-attacks (дата обращения: 04-07-2019)

[15] См.: 5 самых легендарных кибератак …

мерное воздействие на информационную систему или информационно-телекоммуникационная сеть, если это деяние повлекло нарушение, прекращение работы этих систем (сетей))», а в ч. 1 ст. 273 УК РФ после слов «компьютерной информации» добавить слова «, несанкционированного воздействия на информационную систему или информационно-телекоммуникационную сеть».

3. POS-терминалам (Point of Sale — устройство для приема платежных карт): криминальные риски

Следует отметить, что совершенствуются не только программы для неправомерного доступа к информации, но и средства для защиты от кибератак. В связи с этим получить доступ к *POS-терминалам* (Point of Sale — устройство для приема платежных карт) становится гораздо проще, чем к процессинговому центру, а результат, тем не менее, может быть внушительным. Например, в декабре 2013 г. из одной американской сети были похищены данные около 70 млн. карт [Овчинский В.С., 2018: 121].

В настоящее время на хакерском рынке существует большое количество разных программ, которые можно использовать для заражения POS-терминалов, а также поддельные POS-терминалы. В этом случае все данные карт, проходящих через зараженный терминал, становятся известными преступникам. На черном рынке продают не только сами вредоносные программы, но и отдельно доступ к терминалам, на которые эти программы можно установить.

Путем установки поддельных устройств или их заражения вредоносными программами осуществляется обман потерпевших, который облегчает доступ к чужому имуществу, при этом способ завладения последним остается тайным. В связи с этим деяние должно быть квалифицировано по п. «г» ч. 3 ст. 158 УК РФ как кража с банковского счета либо совершенная в отношении электронных денежных средств и по ст. 272 УК РФ. В случае использования вредоносной компьютерной программы для заражения терминала уголовная ответственность должна дополнительно (к п. «г» ч. 3 ст. 158 УК РФ) наступать по ст. 272 и 273 УК РФ. Поэтому трудно согласиться с рекомендацией Пленума Верховного Суда, содержащейся в его приведенном выше Постановлении от 30.11.2017 № 48, квалифицировать такие деяния по ст. 159[6] УК РФ.

4. Блокчейн, криптовалюта: криминальные риски

Появившаяся в конце XX в. технология *блокчейн* получила распространение в логистике, медицине, патентовании, кибербезопасности, голосова-

нии, торговле акциями, банковской сфере и т.п. [Арямов А.А, Иванов С.А., 2019: 13–16]. На ее основе были созданы виртуальные финансовые активы, в том числе криптовалюта (цифровая запись со своим криптографическим кодом в определенной информационной системе) [Арямов А.А., 2019: 12–13, 108–116]. Криптовалюта имеет децентрализованный характер, не эмитирована государством, обладает рядом преимуществ по сравнению с фиатными (символическими) деньгами: анонимность, минимальный процент по транзакциям, неподконтрольность публичной власти и т.д. Эти свойства, во-первых, обусловливают риски использования криптовалюты для анонимного финансирования терроризма, незаконного оборота наркотических средств (психотропных веществ), оружия, порнографических материалов, легализации имущества [Уфимцева В.А., 2019: 140–141] и т.д. Обладая высокой инвестиционной привлекательностью, она также создает угрозу неправомерного завладения ею. Во-вторых, именно из-за этих свойств криптовалюты информация о ней, размещенная в сети Интернет, повлекла обращения прокуратуры в суд с требованием признать данные сведения запрещенной информацией, которые в некоторых случаях удовлетворялись[16].

В судебной практике не вызывает трудностей квалификация преступлений, в которых криптовалюта является средством их совершения. Проблемы появляются, когда она выступает предметом преступления. Это обусловлено тем, что в российском законодательстве до сих пор не определена юридическая природа криптовалюты. В теории уголовного права предлагаются варианты уголовно-правовой оценки подобных деяний, ни один из которых не основан на буквальном толковании уголовного закона[17].

Попытку помочь правоприменителю предпринял Пленум Верховного Суда, приняв Постановление от 26.02.2019 № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7.07. 2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем»»[18]. Пункт 1 Постановления был дополнен абзацем 3, в котором Пленум указал, что согласно ст. 1 Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма (2005) и с учетом Рекомендации 15 ФАТФ (2012) предметом

[16] См., напр.: Апелляционное определение Санкт-Петербургского городского суда от 13.02. 2017 № 33-2537/2017 по делу № 2-10119/2016 // СПС КонсультантПлюс; Решением Мокшанского районного суда Пензенской области от 20.11. 2017 по делу № 2-443/2017~М-451/2017 требование о признании информации запрещенной к распространению в РФ удовлетворено // СПС КонсультантПлюс.

[17] Там же. С. 145–146.

[18] См.: Бюллетень Верховного Суда РФ. 2019. № 4.

преступлений, предусмотренных ст. 174 и 174[1] УК РФ, могут выступать, в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления.

Это разъяснение является попыткой устранить имеющийся пробел в правовом регулировании путем дополнения перечня предметов преступлений, изложенного в ст. 174 и 174[1] УК РФ, указанием на денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления. Однако в Постановлении не разрешен вопрос — как быть, если криптовалюта не была конвертирована в денежные средства? Пленум, с одной стороны, не урегулировал рассмотренную проблему, а с другой стороны вышел за пределы своих полномочий, рекомендовав к предмету преступлений, изложенных в ст. 174 и 174[1] УК РФ, относить еще и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления.

В оценке этой позиции Пленума можно согласиться с Ю.С. Харитоновой, отмечающей, что попытка Пленума Верховного Суда в этой ситуации дать разъяснения демонстрирует острую потребность в регулирования обращения криптовалюты [Харитонова Ю.С., 2019: 31–36].

Федеральный закон «О цифровых финансовых активах», который в том числе должен был определить правовой статус криптовалюты в России, пока не принят[19]. Однако первый шаг на пути к определению правового статуса криптовалюты уже сделан. Федеральным законом от 18.03.2019 № 34-ФЗ внесены изменения в ст. 128 (объекты гражданских прав) Гражданского кодекса Российской Федерации (далее — ГК РФ)[20]. Согласно этому закону «к объектам гражданских прав относятся вещи (включая наличные деньги и документарные ценные бумаги), иное имущество, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права) …». Таким образом, новая редакция статьи устранила ошибку в определении предусмотренных ст. 128 ГК РФ объектов гражданских прав [Василевская Л.Ю., 2019: 112], а права, относящиеся к имуществу, дополнила цифровыми правами.

Понятие последних дается в ст. 141[1] ГК РФ «Цифровые права». Под ними «признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или

[19] См.: Законопроект № 419059-7. Available at: URL: https://sozd.duma.gov.ru/bill/419059-7 (дата обращения: 09-07-2019)

[20] СЗ РФ. 2019. № 12. Ст. 1224.

ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу».

Некоторые цивилисты негативно оценивают отнесение цифровых прав к имущественным правам. «Сложно понять, как цифровой код может быть отнесен к категории имущественного права, не являясь по своей сути правовым требованием, которое могло бы обращаться в гражданском обороте как разновидность прав» [Вайпан В.А., Фролова М.А. 2018]; [Гузнов А., Михеева Л., Новоселова Л. [и др.], 2018: 16–30]. Ученые отмечают, что такие изменения влекут за собой и необходимость пересмотра понимания обязательственных отношений, содержания сделки и т.п. [Василевская Л.Ю., 2019: 118].

Но, несмотря на это, к предмету преступления будут относиться и цифровые права, а неправомерные действия в отношении криптовалюты будут охватываться теми составами преступлений, в которых имущество закреплено в качестве предмета преступления.

Кроме того, в отношении криптовалюты может быть применена конфискация имущества (гл. 15[1] УК РФ). Считается, что ее конфискация «впервые была осуществлена правоохранительными органами в ходе пресечения деятельности крупнейшего анонимного цифрового рынка продажи наркотических средств Silk Road, активы которого были проданы на четырех аукционах по действовавшему на тот период курсу биткоина на общую сумму 30 млн долларов США» [Долгиева М.М., 2018: 45–49]. После реализации биткоинов, принадлежащих Silk Road, продажа конфискованной криптовалюты в США происходит часто[21].

Работа по борьбе с криптопреступлениями и конфискации криптовалюты успешно ведется не только в США, но и в Великобритании[22], Китае[23], Испании[24] и многих других странах» [Долгиева М.М., 2018: 45–49]. Эта уголовно-правовая мера действительно может оказаться средством в борьбе с незаконными действиями, совершаемыми с ней.

Исследователи отмечают, что именно блокчейн во многом способствует раскрытию преступлений, в которых задействована криптовалюта в качестве средства совершения преступления или его предмета, установлению личности анонимных владельцев этих цифровых активов; операции с ней

[21] Available at: URL: https://bitjournal.media/27-06-2018/amerikanskie-pravoohraniteli-konfiskovali-17-mln-v-btc/; https://forklog.com/vlasti-ssha-konfiskovali-milliony-dollarov-v-kriptovalyute-prinadlezhavshie-byvshemu-vladeltsu-darknet-rynka-alphabay (дата обращения: 10-07-2019)

[22] Available at: https://www.surrey.police.uk/about-us/how-we-seized-converted-and-retained-12m-worth-of-bitcoin/ (дата обращения: 10-07-2019)

[23] Avasilable at: URL: https://forklog.com/politsiya-kitaya-izyala-u-organizatorov-futbolnyh-totalizatorov-1-4-mln-v-bitkoinah/ (дата обращения: 10-07 -2019)

[24] Available at: https://www.europol.europa.eu/newsroom/news/police-seize-more-eur-45-million-in-cryptocurrencies-in-europe's-biggest-ever-lsd-bust (дата обращения: 10-07-2019)

позволяют сделать любую скрытую финансовую операцию общедоступной. Кроме того, «повышение уровня компетенции сотрудников правоохранительных органов и финансовых разведок, технической оснащенности этих структур будет способствовать росту числа раскрытых подобных преступлений и предупреждению совершения новых» [Кунев Д.А., 2019: 76–80].

5. Искусственный интеллект и робототехника: криминальные риски

Современное общество уже невозможно представить без *искусственного интеллекта и робототехники*. Искусственный интеллект — область научных знаний и технологий создания интеллектуальных машин и интеллектуального программного обеспечения. Кроме того, искусственным интеллектом называют свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека. Одной из ключевых их особенностей является способность приобретать знания посредством обучения (самомодификации) и применять эти знания для решения проблем. Подобно тому, как человек использует свой мозг, чтобы учиться на новой информации, собранной органами чувств, искусственный интеллект учится на информации, передаваемой ему, например, в виде изображения или правил. «Данная информация не только обрабатывается в соответствии с тем, как она запрограммирована, но также изменяет сам алгоритм, с помощью которых ее обрабатывают. Процесс, при котором искусственный интеллект запрограммирован на автоматическое изменение собственного алгоритма, называется машинным обучением» [Арямов А.А., Иванов С.А., 2019: 4].

Искусственный интеллект и робототехника образуют наиболее перспективную комбинацию для автоматизации задач, не входящих в первичные заводские настройки роботов. В последние годы он все больше распространяется в роботизированных решениях, обеспечивая гибкость и возможность обучения там, где раньше применялись неизменяемые производственные настройки. Роботизированные системы с искусственным интеллектом управления используются не только на производстве, но и при совершении преступлений, а также создают риски причинения вреда охраняемым уголовным законом общественным отношениям.

Так, последние возникают в связи с использованием беспилотных транспортных средств, оснащенных искусственным интеллектом. Понятием «беспилотные транспортные средства», как правило, охватываются две группы автомобилей: высокоавтоматизированные автомобили с водителем (0–3 уровень автономности вождения[25]) и высокоавтоматизированные ав-

[25] См.: Стандарт SAE J3016.Available at: https://www.sae.org/binaries/content/assets/cm/ cotent/news/pressreleases/pathway-to-autonomy/automated_driving.pdf (дата обращения: 10 -07 -2019)

томобили без водителя (4–5 уровень автономности вождения[26]). Отметим, что термин «беспилотное транспортное средство» (беспилотники) больше подходит ко второй группе автомобилей, но устоявшейся терминологии ни в России, ни за рубежом пока нет [Незнамов А.В., 2018: 175–182].

Риски использования беспилотников обусловлены тем, что:

1) управление осуществляется через или с использованием информационно-телекоммуникационной сети, что создает возможность ее взлома и вмешательства в программу управления транспортным средством;

2) функционирование транспортного средства невозможно без источника питания, которое намеренно может быть отключено или повреждено;

3) транспортные средства, использующие спутниковую навигацию и электронные блоки для обработки GPS-сигнала, могут быть поражены сильной магнитной бурей;

4) программное обеспечение рассчитано на функционирование транспортного средства в стандартных (типовых) условиях. Проблема возникает, если система управления не сможет распознать нестандартную обстановку, которая в том числе может быть обусловлена плохими погодными условиями: сильный дождь, снегопад, туман и т.д. [Коробеев А.И. (а), 2019: 9–28, 64, 65]; [Коробеев А.И. (б), 2019: 64, 65].

Все это порождает угрозу причинения вреда личности, общественной безопасности и собственности.

Перечисленные риски будут актуальны, если беспилотники будут использоваться на дорогах общего пользования. На сегодняшний день ни международное[27], ни национальное законодательство России[28] не предусматривает нахождения беспилотных транспортных средств (высокоавтоматизированные автомобили без находящегося внутри водителя) на дорогах общего пользования. Отсутствует и соответствующая инфраструктура. Вместе с тем предложения об ответственности за причиненный вред в теории уголовного права уже делаются. Так, предлагается ответственность за вред (возникающий вследствие обстоятельств, изложенных ранее в п. 3 и 4), причиненный беспилотным транспортным средством (4–5 уровень автономности вождения), возложить на разработчика программно-аппаратных средств и собственника транспортного средства.

---

[26] Там же.

[27] См.: Конвенция о дорожном движении (Вена, 1968) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. XXXIII. М., 1979. С. 385–435.

[28] Постановление Правительства РФ от 23.10.1993 № 1090 «О Правилах дорожного движения» // Собрание актов Президента и Правительства РФ. 1993. № 47. Ст. 4531; Федеральный закон от 10.12.1995 № 196-ФЗ «О безопасности дорожного движения» // СЗ РФ. 1995. № 50. Ст. 4873; Федеральный закон от 8.11.2007 № 259-ФЗ «Устав автомобильного транспорта и городского наземного электрического транспорта» // СЗ РФ. 2007. № 46. Ст. 5555.

Если наступили общественно опасные последствия в результате целенаправленных действий по неправомерному вмешательству в систему управления транспортным средством или отключения (повреждения) его источника питания, то виновное лицо должно подлежать уголовной ответственности в соответствии с теми последствиями, которые наступили, как за преступления против личности или собственности.

Требует самостоятельного исследования вопрос о необходимости криминализации неправомерного вмешательства в системы управления транспортным средством или информационно-телекоммуникационные сети, обеспечивающие их работу, как компоненты транспортной безопасности.

Основа любого искусственного интеллекта и робототехники — это программное обеспечение, которое создает риски неправомерного доступа к нему с помощью вредоносных программ. Так, в 2016 г. было совершено одно из первых целенаправленных убийств «с использованием робота. В палате интенсивной терапии больной умер от подачи в капельницу смертоносного состава вместо предписанного лекарства. Полицейские не смогли бы обнаружить это преступление, если бы не случайность. Программист, которого банда наняла, чтобы взломать программу, управляющую автоматической раздачей лекарств, поделился информацией в одном из закрытых чатов. В нем присутствовал осведомитель городской полиции. Благодаря ему программист был задержан» [Овчинский В.С., 2018: 153].

На конференциях ФБР отмечалось, что «в течение 2015–2016 гг. агенты под прикрытием и осведомители неоднократно сообщали, что преступные синдикаты серьезно обсуждали различные варианты убийств, используя насыщенные электроникой автомобили, умные дома, медицинские комплексы», Интернет вещей (IoT) и т.п. Правоохранительные органы по всему миру всерьез готовятся к появлению преступных организованных групп, «специализирующихся на заказных высокотехнологичных убийствах, замаскированных под технические инциденты различного рода. Принимая во внимание объем рынка заказных убийств в Соединенных Штатах, составляющий около 2 млрд. долл. в год, ожидается появление» таких сетевых синдикатов.

Главным инструментом подобных преступных сообществ могут стать не хакерские программы сами по себе, а искусственный интеллект. Различного рода автоматизированные автономные системы в подавляющем большинстве управляются из единого вычислительного центра, функционирующего как искусственный интеллект (роевое обучение). Соответственно, подключиться и заместить команды одного искусственного интеллекта может только другой. Программисту это не под силу. Он будет распознан из-за большей медлительности и меньшей алгоритмичности действий и операций. Кроме

того, только искусственному интеллекту под силу замаскировать неправомерное отключение или выполнение несанкционированных действий техническим отказом. Характерной чертой современных вирусных программ является то, что они сами по себе обладают некоторыми признаками искусственного интеллекта, к которым относятся адаптивное поведение, самовоспроизведение с мутациями, мимикрия, возможность использования самообучающихся алгоритмов для распространения и заражения новых компьютеров и т.п. [Тирранен В.А., 2019: 137]

В ближайшее время данная преступная деятельность может стать реальностью. Для предотвращения и раскрытия этих преступлений необходимо иметь в правоохранительных органах специалистов, разбирающихся в тонкостях нейронных сетей, глубокого обучения и активного тестирования.

Изложенное подчеркивает необходимость:

1) оценки риска неправомерного вмешательства в программное обеспечение устройств или информационно-телекоммуникационных сетей, обеспечивающих их работу;

2) разработки, с одной стороны, производителями адекватных мер защиты программного обеспечения от неправомерного доступа, включая средства идентификации устройств, оснащенных искусственным интеллектом, а, с другой стороны, мер ответственности для производителей, не соблюдающих это требование.

Актуальность последнего предложения иллюстрирует отчет компании Trend Micro (май 2017 г.)29, согласно которому в мире насчитывается свыше 83 тыс. доступных через Сеть промышленных роботов, и в 5 тыс. из них отсутствуют механизмы аутентификации пользователей. Исследователи обнаружили в роботах 65 уязвимостей, в том числе позволяющих обойти механизмы аутентификации, модифицировать ключевые настройки и изменить режим работы устройства.

В подтверждение своих опасений исследователи осуществили показательную кибератаку на промышленного робота в лабораторных условиях. Эксперты продемонстрировали, как с помощью атаки можно незаметно изменить движение устройства. Программный код остается неизменным, а изменение движения невозможно уловить невооруженным взглядом. Вместе с тем малейшее отклонение в производственном процессе может привести к серьезным последствиям.

Одна из особенностей искусственного интеллекта — это его способность к самообучению, результаты которого не всегда под силу предсказать разработчикам, что также может порождать риски причинения вреда охраняемым

[29] Available at: URL: https://www.trendmicro.com/ru_ru/about/awards.html (дата обращения: 23.07.2019)

законом общественным отношениям. Проиллюстрируем эту особенность известной программой-роботом Tay (компания «Майкрософт»), созданной для общения с людьми в Интернете. За сутки робот стал расистом и научился ругаться. Компания-создатель пояснила, что чат-бот Tay с искусственным интеллектом — это обучаемый проект. Недопустимые ответы, которые он дает, свидетельствуют о взаимодействиях в процессе обучения[30]. В связи с этим возникает вопрос — кто подлежит ответственности за оскорбительные сообщения, сделанные этой программой?

Проблема характерна для всех роботов с искусственным интеллектом. Ее можно подразделить на две группы. Первая связана с неправомерным внесением изменений в программное обеспечение. На предотвращение подобного поведения в цифровом мире рассчитаны сделанные нами предложения по изменению редакции ст. 272 и 273 УК РФ. Вторая — с ответственностью за вред, причиненный искусственным интеллектом. В.А. Лаптев считает, что искусственный интеллект обладает «отдельными элементами субъективного права» и одновременно выступает объектом права [Лаптев В.А., 2019: 88]. В связи с этим он полагает, что в ближайшее время ответственности за работу искусственного интеллекта будут нести создатель (производитель) и владелец (оператор), по аналогии с ответственностью за причинение вреда источником повышенной опасности. Следующим шагом будет признание за такими роботами правосубъектности и способности нести самостоятельную юридическую ответственность. Заключительный этап — «правосубъектность будет существовать у искусственного интеллекта уже в виртуальном (цифровом) пространстве в отрыве от материального мира» [Лаптев В.А., 2019: 99].

Еще один риск, порождаемый искусственным интеллектом, — это возможность его использования для совершения преступления, например, дронов в качестве наркокурьеров, для совершения террористических актов и т.д.

Сегодня достигнуты большие успехи в миниатюризации роботов. Государственные и коммерческие структуры могут приобрести робота размером с большого жука, оснащенного видеокамерой, способной снимать как днем, так и ночью, микрофоном, устройством дистанционной передачи на расстояние до 5 км звука и изображения и, естественно, устройствами для передвижения. В американские спецподразделения поступили роботы-шмели, способные действовать в наиболее агрессивных средах, быть незаметными, проникать в здания, оснащенные пуленепробиваемыми стеклами, внутри не только фотографировать, но и поражать живые «мишени».

---

[30] См.: «Я всех ненавижу»: чат-бот от Microsoft всего за сутки стал расистом и мизантропом. Available at: URL: https://russian.rt.com/article/155810 (дата обращения: 11-07-2019)

В 2013–2014 гг. произошел подлинный прорыв в робототехнике, когда стало возможным создание роев боевых и гражданских роботов. Рой имитирует поведение пчел, муравьев, стаи птиц. Используя передовые решения в области «облачной» коллективной памяти, распределенной вычислительной мощности и модульных конструкций, системы могут не только координировать деятельность и самообучаться друг у друга, но и собираться из маленьких устройств в крупные единые комплексы. Военный потенциал этих технологий на первом этапе будет использоваться для сбора разведданных и массовых диверсий на территории противника, в последующем они могут стать одним из вариантов армии. Подобные силиконовые конструкции разных форм со смертоносным оборудованием будут способны на самостоятельное принятие тактических решений.

Л. Дель Монте — известный ученый-физик, бывший руководитель разработок микроэлектроники в IBM, автор книги «Нанооружие: растущая угроза человечеству», прогнозирует, что к концу 2020-х гг. «террористы смогут получить доступ к нанооружию и будут способны использовать наноботов (нанороботов) для совершения террористических атак, например для заражения систем водоснабжения крупных городов или отравления людей инъекциями. Нанодроны также могут стать инструментами биологической войны»[31].

В указанных случаях робот выступает в качестве орудия или средства совершения преступления. Уголовной ответственности подлежит лицо, использовавшее его для совершения преступления. Вместе с тем требует самостоятельного исследования вопрос о том, повышает ли степень общественной опасности преступление, совершенное с использованием робота (искусственного интеллекта)? Если речь идет о террористическом акте, то вряд ли, а если совершено убийство, то скорее всего да. Можно предположить, что это должно быть квалифицированное убийство, в связи с чем потребуется дополнение ч. 2 ст. 105 УК РФ соответствующим признаком.

Заключение

Появление новых технологий создает угрозу вреда всем сферам общественных отношений, но прежде всего — личности, экономике и общественной безопасности.

Одной из распространенных киберугроз в сфере экономики, способной причинять вред и имущественным интересам личности, выступает метод социальной инженерии. Имущественный ущерб, причиненный с использо-

[31] Available at: URL: https://inosmi.ru/science/20170321/238918900.html (дата посещения: 23-03-2019)

ванием этого метода, следует оценивать по п. «г» ч. 3 ст. 158 УК РФ как кража с банковского счета или совершенная в отношении электронных денежных средств, и соответственно по ст. 272, 273, 274^1 УК РФ. Кроме того, необходимо: а) исключение ст. 159^6 из УК РФ; б) дополнение ст. 163 УК РФ таким признаком, как угроза уничтожения информации. Отсутствие в этой статье такого вида угрозы является пробелом, не позволяющим уголовно-правовыми средствами бороться с виновными, использующими программы-вымогатели для завладения чужим имуществом.

Исследование DoS-атак выявило несовершенство уголовно-правовых норм, устранить которое возможно путем дополнения:

а) части 1 ст. 272 УК РФ указанием на «неправомерное воздействие на информационную систему или информационно-телекоммуникационная сеть, если это деяние повлекло нарушение, прекращение работы этих систем (сетей))»;

б) части 1 ст. 273 УК РФ после слов «компьютерной информации» словами: «несанкционированного воздействия на информационную систему или информационно-телекоммуникационную сеть».

Завладение чужим имуществом с использованием поддельных или зараженных вредоносными программами POS-терминалов должно быть квалифицировано по п. «г» ч. 3 ст. 158 УК РФ как кража с банковского счета и по ст. 272 УК РФ, поскольку способ изъятия имущества остается тайным, а с помощью обмана происходит завладение конфиденциальной информацией (номер платежной карты, ПИН-код и др.), который облегчает доступ к чужому имуществу. За использование вредоносной компьютерной программы для заражения терминала уголовная ответственность дополнительно (к п. «г» ч. 3 ст. 158) должна наступать по ст. 272 и 273.

Появление виртуальных финансовых активов, в том числе криптовалюты, стало возможным благодаря технологии блокчейн. Ее существование обусловливает риски использования криптовалюты для анонимного финансирования терроризма, незаконного оборота наркотических средств (психотропных веществ), оружия, порнографических материалов, легализации имущества, а также создает угрозу неправоверного завладения ею. Статьи 128 и 141^1 ГК РФ позволяют криптовалюту относить к имуществу и тем самым снимают проблему квалификации деяний, в которых она выступает предметом преступления.

Эволюция искусственного интеллекта и робототехники обозначила проблему ответственности за причиняемый ими вред, которая активно обсуждается как учеными, так и практиками. На сегодняшний день заслуживающим внимание выглядит предложение относить искусственный интеллект к источникам повышенной опасности. Основания и условия ответственности за вред, причиненный такими источниками, хорошо разработаны в

гражданском праве. В связи с тем, что искусственный интеллект способен к самообучению и вследствие этого принятию самостоятельных решений, обсуждаются варианты признания его субъектом права, «роботом-агентом», т.е. рассматриваются вопросы его самостоятельной и (или) субсидиарной ответственности.

Библиография

Арямов А.А. Цифровизация: уголовно-правовые риски в сфере экономики // Актуальные проблемы российского права. 2019. N 6. С. 108–116.

Арямов А.А., Иванов С.А. Девиации в цифровом мире: уголовно-правовое измерение. М.: Контракт, 2019. 130 с.

Болсуновская Л.М. Криминализация мошенничества в сфере компьютерной информации в российском праве // Библиотека криминалиста. 2016. N 3. С. 15–20.

Василевская Л.Ю. Токен как новый объект гражданских прав: проблемы юридической квалификации цифрового права // Актуальные проблемы российского права. 2019. N 5. С. 111–119.

Гузнов А., Михеева Л., Новоселова Л. и др. Цифровые активы в системе объектов гражданских прав // Закон. 2018. N 5. С. 16–30.

Данилов Д. Квалификация DDos-АТАК, совершенных из корыстной заинтересованности // Уголовное право. 2018. N 6. С. 37–42.

Долгиева М.М. Конфискация криптовалюты // Законность. 2018. N 11. С. 45–49.

Кибальник А. Квалификация мошенничества в новом постановлении Пленума Верховного Суда РФ // Уголовное право. 2018. N 1. С. 61–67.

Кунев Д.А. Современные угрозы использования криптовалют в преступных целях / Уголовное право: стратегия развития в XXI веке: материалы XVI международной конференции. М.: РГ-Пресс, 2019. С. 76–80.

Лаптев В.А. Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. N 2. 2019. С. 79–102.

Лопашенко Н.А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Криминологический журнал Байкальского государственного университета экономики и права. 2015. № 3. С. 504–513.

Незнамов А.В. Правила беспилотного вождения: об изменениях Венской конвенции о дорожном движении // Закон. 2018. № 1. С. 175–182.

Овчинский В.С. Криминология цифрового мира. М.: Норма, 2018. 352 с.

Вайпан В.А., Егорова М.А. и др. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики. М.: Юстицинформ, 2018. 376 с.

Тирранен В.А. Искусственный интеллект и нейронные сети как инструменты современной киберпреступности / Уголовное право: стратегия развития в XXI веке: материалы конференции. М.: РГ-Пресс, 2019. С. 135-140.

Уфимцева В.А. Уголовно-правовые риски использования криптовалюты / Уголовное право: стратегия развития в XXI веке. М.: РГ-Пресс, 2019. С. 140–147.

Харитонова Ю.С. Криптовалюта в правоприменительной практике // Предпринимательское право. 2019. N 2. С. 31–36.

Pravo. Zhurnal Vysshey Shkoly Ekonomiki. 2020. No 1

Preventing Deviations in the Digital World by Criminal Law Means

Yulia Gracheva

Professor, Department of Criminal Law, Kutafin Moscow State Law University. Address: 9 Sadovo-Kudrinskaya Str., Moscow 125593, Russia. E-mail: uvgracheva@mail.ru

Sergey Malikov

Senior Lecturer, Department of Criminal Law, Kutafin Moscow State Law University, Candidate of Juridical Sciences. Address: 9 Sadovo-Kudrinskaya Str., Moscow 125593, Russia. E-mail: s.v.malikov@yandex.ru

Alexander Chuchaev

Professor, Department of Criminal Law, Kutafin Moscow State Law University, Doctor of Juridical Sciences. Address: 9 Sadovo-Kudrinskaya Street, Moscow 125593, Russia. E-mail: moksha1@rambler.ru

Abstract

Any progress causes both positive influence on society and produces new risks of causing harm to public relations some of which may be criminal. The subject matter of the research is new technologies which may be used to bring harm to public relations protected by criminal law. The purpose of the article is to examine the tool of breaching public relations by applying new technologies and developing adequate criminal law measures to evade deviations in the digital world. The general scholar and social legal methods are implemented in the article. A popular technique of social engineering is fishing aimed at obtaining access to confidential data of the users, logins and passwords. The theft of property of another by means of getting confidential information causes criminal liability under article 3 of the Russian Criminal Code. Fishing letters contain various programs (Trojans). The programs are applied by the guilty when stealing money by providing access to the bank account of the victim etc. Such programs are applied to extort the property of the victim threatening to delete computer information. These actions may be qualified under articles 272 and 273 of the Criminal Code. In authors opinion, Article 163 of the Code should be added with the way of committing the crime, i.e. the threat of deleting information. Similar negative consequences may be caused by DoS attacks. The research studies five most famous cyber attacks, specifies the mechanism of causing harm to the objects of criminal law protection, which needs specification in article 272 and 273 of the Criminal Code. The paper studies the blockchain technology and cryptocurrency, artificial intelligence and robots. The changes in the civil law regulation of public relations arising due to the technologies in question may cause changes in the criminal law assessment of modern era crimes.

Keywords

deviations in the digital world, criminal risks, method of social engineering, Dos attacks, fraud in the field of computer information, unauthorized access, artificial intelligence and robotics, criminal liability, cryptocurrency, blockchain.

Acknowledgments: The work was supported by the Russian Foundation for Basic Research (research project № 18-29-16158).

For citation: Gracheva Y.V., Malikov S.V., Chuchaev A.I. (2020) Preventing Deviations in the Digital World by Criminal Law Means. *Pravo. Zhurnal Vysshey shkoly ekonomiki,* no 1, pp. 188–210 (in Russian)

DOI: 10.17323/2072-8166.2020.1.188.210

References

Aryamov A.A. (2019) Digitalization and criminal risks in economy. *Aktual'nye problemy rossijskogo prava,* no 6, pp. 108–116 (in Russian)

Aryamov A. A., Ivanov S.A. (2019) *Deviations in the digital area: criminal law dimension.* Moscow: Kontract, 130 p. (in Russian)

Bolsunovskaya L.M. (2016) Criminalization of fraud in computer information in Russian law. *Biblioteka kriminalista*, no 3, pp. 15–20 (in Russian)

Danilov D. (2018) Qualification of DDs-attacks for mercenary motives. *Ugolovnoe pravo,* no 6, pp. 37–42 (in Russian)

Dolgieva M.M. (2018) Confiscation of the crypto currency. *Zakonnost'*, no 11, pp. 45–49 (in Russian)

Guznov A., Miheeva L., Novoselova L. (2018) Digital assets in the system of the civil law. *Zakon*, no 5, pp. 16–30 (in Russian)

Haritonova Yu. S. (2019) Crypto currency in legal practice. *Predprinimatel'skoe pravo,* no 2, pp. 31–36 (in Russian)

Kibal'nik A. (2018) Qualification of fraud in recent resolution of the Russian Supreme Court. *Ugolovnoe pravo*, no 1, pp. 61–67 (in Russian)

Kunev D.A. (2019) Current threats of using crypto currency for criminal aims. *Ugolovnoe pravo: strategiya razvitiya v XXI veke.* Papers of a conference. Moscow: Prospect, pp. 76–80 (in Russian)

Laptev V.A. (2019) Artificial intelligence and liability for its work. *Pravo. Zhurnal Vysshej shkoly ekonomiki,* no 2, pp. 79–102 (in Russian)

Lopashenko N.A. (2015) Fraud reform: questions and answers. *Kriminologicheskij zhurnal Baikalskogo gosudarstvennogo universiteta ekonomiki i prava,* no 3, pp. 504–513 (in Russian)

Neznamov A.V. (2018) Rules of non-pilot driving and changing Vienna Traffic Convention. *Zakon*, no 1, pp. 175–182 (in Russian)

Ovchinskyi V.S. (2018) *Criminology of digital world.* Moscow: Norma, 352 p. (in Russian)

Tirranen V.A. (2019) Artificial intellect and neuron cells as means of modern cyber crime. *Ugolovnoe pravo: strategiya razvitiya v XXI veke*, pp. 135–140 (in Russian)

Ufimceva V.A. (2019) Criminal risks of using crypto currency. *Ugolovnoe pravo: strategiya razvitiya v XXI veke,* pp. 140–147 (in Russian)

Vaipan V.A. (ed.) (2019) *Legal regulation of digital economy.* Moscow: Yustitcinform, 376 p. (in Russian)

Vasilevskaya L. Yu. (2019) Token as a new object of civilian rights: qualification of digital rights. *Aktual'nye problemy rossijskogo prava,* no 5, pp. 111–119 (in Russian)