УГОЛОВНОЕ ПРАВО

А. А. Арямов*,
Ю. В. Грачева**

Цифровизация: уголовно-правовые риски в сфере экономики[1]

Аннотация. *Любая промышленная революция не только открывает новые возможности для общества и государства, но и наделяет преступников не существовавшими ранее способами и инструментами для совершения преступлений. Четвертая промышленная революция характеризуется автоматизацией и роботизацией производства, искусственным интеллектом, 3D-печатью, созданием новых материалов и технологий (биотехнологий и информационных технологий) и т.д.*

Одним из объектов уголовно-правовой охраны, угроза причинения вреда которому создается в результате цифровизации, выступает экономика (общественные отношения, возникающие в связи с обеспечением нормального функционирования экономики как единого народно-хозяйственного комплекса). В настоящее время можно выделить такие киберугрозы для экономики, как атаки на банки, на брокера, на расчетную систему, хищения через интернет-банкинг и некоторые другие действия, совершаемые посредством использования вредоносных программ. Их основной целью выступает неправомерное завладение чужим имуществом. Наиболее распространенными способами совершения хищения являются ручной перевод средств с компьютера владельца счета через удаленный доступ, автозалив, метод социального инжиниринга, применение программы-вымогателя, неправомерное использование бренда и др.

В условиях цифровизации перед наукой уголовного права стоит задача разработки модели системного обновления отечественного уголовного законодательства, выработки общих правил и четких критериев его осуществления, а не спонтанного ответа на сиюминутные потребности правоприменителя путем конструирования специальных составов киберпреступлений.

Ключевые слова: *цифровизация, киберпреступления, уголовно-правовые риски, криптовалюта, блокчейн, четвертая промышленная революция, информационные технологии; программы-вымогатели, атаки на банки.*

DOI: 10.17803/1994-1471.2019.103.6.108-116

[1] Работа выполнена при финансовой поддержке РФФИ по договору № 18-29-16158/18.

© Арямов А. А., Грачева Ю. В., 2019

* *Арямов Андрей Анатольевич*, доктор юридических наук, профессор, профессор кафедры уголовного права Российского государственного университета правосудия
aaryamov65@yandex.ru
117418, Россия, г. Москва, ул. Новочеремушкинская, д. 69

** *Грачева Юлия Викторовна*, доктор юридических наук, профессор, профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
uvgracheva@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

ВМЕСТО ВВЕДЕНИЯ

Четвертая промышленная революция обусловила появление:

1) автоматизации и роботизации производства, армии и всех сторон общественной жизни. При этом под робототехникой понимаются программируемые машины, которые могут автономно или автоматически выполнять те или иные действия; надо иметь в виду, что робототехника не является синонимом искусственного интеллекта. Последний предназначен для выполнения задач, которые могут быть решены без участия интеллекта человека;
2) 3D-печати. В ее основе лежит технология Additive Manufacturing, т.е. аддитивное[2] изготовление;
3) «производства новых материалов, включая материалы с заранее спроектированными свойствами, композитные материалы и т.п. Необходимость появления широчайшей гаммы новых материалов обусловлено, с одной стороны, требованиями широкого внедрения экономичной, эффективной 3D-печати, а с другой — развитием микроэлектроники, биотехнологий и т. п.»[3];
4) биотехнологий, в том числе:

— индустрии индивидуализированных лекарств;
— регенеративной медицины, использующей возможности 3D-печати для производства донорских органов;
— биоинформатики;

5) информационных технологий, включающих:

— большие данные (big data). Большие данные — «это сбор, хранение, оцифровка, обработка и предоставление в удобном для пользователя виде в любое время и в любой точке всей совокупности сведений о тех или иных событиях, процессах, явлениях и т.п. Ключевым в больших данных является то, что они позволяют работать именно со всей информацией в режиме онлайн. Определяющим здесь выступает слово «всей». Сами по себе большие данные являются важнейшим государственным и корпоративным активом, который при должном использовании обеспечивает их владельцам интеллектуальное превосходство и деловое доминирование»[4];
— когнитивные вычисления и экспертные системы. Как отмечается в науке, «в основу когнитивных вычислений заложены программы, моделирующие и имитирующие некоторые известные психофизиологические процессы человека. За счет этого созданы программы, обладающие возможностями совершенствования, и умеющие учитывать при решении тех или иных задач ошибки»[5];
— «облачные» и распределенные вычисления, т.е. информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети Интернет к общему набору конфигурируемых вычислительных ресурсов («облаку»), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера[6];

---

[2] Аддитивное производство — группа технологических методов производства изделий и прототипов, основанная на поэтапном добавлении материала на основу в виде плоской платформы или осевой заготовки (см.: URL: https://ru.wikipedia.org/wiki/%D0%90%D0% B4%D0%B4%D0%B8%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE (дата обращения: 15.03.2019).

[3] *Ларина Е., Овчинский В.* Русское чудо XXI века // URL: http://zavtra.ru/blogs/russkoe-chudo-xxi-veka (дата обращения: 15.03.2019).

[4] *Ларина Е., Овчинский В.* Указ. соч.

[5] *Ларина Е., Овчинский В.* Указ. соч.

[6] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

— блокчейн — компьютерная технология, построенная на особой системе шифрования, по существу — информационная база данных, в которой записи группируются в блоки, где каждый блок связан со следующим с помощью использования криптографической подписи. Блокчейн позволяет эффективно сохранять данные, но сам по себе не обеспечивает их достоверность, поскольку они самостоятельно вводятся пользователями. Последние создают записи, а особые субъекты, майнеры[7], проверяют их и группируют в блоки, после чего посредством своих мощностей пытаются рассчитать ключ к данному блоку. Справившийся с этой задачей майнер включает полученную информацию в блок, тем самым гарантирует ее достоверность. Выделяют: открытый публичный блокчейн[8]; консорциумный (комбинированный) блокчейн; закрытый частный блокчейн. Основные чертами технологии блокчейн являются: децентрализованность, анонимность, автономность, использование криптографии, присвоение каждой транзакции особых меток времени. Блокчейн-приложения разделяются на три категории в зависимости от уровня разработки: 1.0 — криптовалюта; 2.0 — модели умных контрактов; 3.0 — практически автономные смарт-контракты[9].

КИБЕРУГРОЗЫ И УГОЛОВНО-ПРАВОВЫЕ ПРОБЛЕМЫ

Чем выше технологический уровень государства и общества, чем глубже информационно-коммуникационные технологии проникли во все сферы жизни общества, тем более уязвимыми они становятся для организованной преступности и террористов[10]. Каждая высокая технология имеет тройное применение: гражданское, военное и криминальное. В связи с этим любая промышленная революция не только открывает новые возможности для общества и государства, но и наделяет преступников не существовавшими ранее способами и инструментами для совершения преступлений, порождает новые угрозы объектам уголовно-правовой охраны.

Киберугрозы затрагивают все общество в целом, и их невозможно ликвидировать полностью в связи с тем, что цифровые технологии успешно работают в силу своей открытости, а это сопряжено с риском. Однако уголовному праву под силу выявить эти угрозы и разработать уголовно-правовой механизм по их минимизации.

Одним из объектов уголовно-правовой охраны, которому может быть создана угроза причинения вреда в результате цифровизации, выступает экономика (общественные отношения, характеризующие нормальное функционирование экономики как единого народно-хозяйственного комплекса). В настоящее время выявлены следующие виды киберугроз:

1) *атаки на банки*. Главной мишенью киберпреступников в этой сфере были небольшие региональные банки. Целенаправленные атаки на них, как правило, происходят с использованием методов социального инжиниринга.

Начиная с 2013 г. несколько разных групп русскоговорящих хакеров атакуют банки и платежные системы. Делают это они очень успешно. Общая сумма хищений, к которым причастны эти мошенники, составляет более 1 млрд

[7] Лицо, подтверждающее транзакцию, получающее вознаграждение и комиссию.

[8] Публичный блокчейн не требует идентификации: любое лицо может вписать данные без разрешения и любое лицо может прочитать эти данные. Кроме того, эта платформа не имеет фиксированного перечня майнеров, им может быть любое лицо. Частный блокчейн предъявляет требования как к идентификации, так и к майнерам.

[9] См.: *Новгородская В. Б.* Новые технологии (блокчейн / искусственный интеллект) на службе права : научно-методическое пособие / под ред. Л. А. Новоселовой. М., 2019. С. 7, 9, 11, 13, 14, 18.

[10] См.: Национальная стратегия кибербезопасности 2016—2021 гг. (Великобритания) // URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016.pdf (дата обращения: 17.03.2019).

руб. (по состоянию на вторую половину 2014 г.). В конце 2015 г. и начале 2016 г. группа Buhtrap похитила у 13 банков 1,8 млрд руб. Средняя сумма хищения составила 143 млн руб.[11];

2) *атаки на брокера.* В 2015 г. была проведена первая успешная атака на брокера, которая вызвала большой резонанс среди участников финансового рынка. Для этой атаки «использовался троян Corkow (также известный как Metel). Он предоставляет удаленный доступ к системе, что позволяет злоумышленнику запускать программы, управлять клавиатурой и мышкой параллельно с оператором системы. В результате несанкционированного доступа к терминалу торговой системы было выставлено пять заявок на покупку 437 млн долл.»[12] и две заявки на продажу 97 млн долл. Однако была исполнена только часть заявок, в результате было куплено 158,536 тыс. и продано 93,925 тыс. долл. США. Указанные действия вызвали очень большую волатильность в течение 6 мин, что привело к причинению ущерба банку в размере 300 млн руб. Через 14 мин после первой заявки хакер дал команду Corkow на удаление своих следов и вывод системы из строя[13];
3) *атаки на расчетную систему*. Так, 16 августа 2015 г. произошел инцидент, в результате которого через банкоматы было похищено около 500 млн руб. Он затронул около 15 крупных банков — участников одной из российских расчетных систем, которая объединяет около 250 банков[14]. Были использованы вредоносные программы, хорошо известные антивирусным компаниям, которые очень сложно вовремя обнаружить стандартными средствами антивирусной защиты. Эти вредоносные программы предоставляли удаленный доступ к нужным системам внутризащищенных сетей и давали атакующим все возможности, доступные сотрудникам финансовых учреждений;
4) *хищения через интернет-банкинг.* Практически все стандартные меры безопасности, применяемые банками, — защищенные токены (ключи для авторизации пользователя), отслеживание смены оборудования и мест отправки платежных поручений, СМС-подтверждение и т.п. — можно обойти. Наиболее распространенными способами подобных хищений выступают:

— ручной перевод посредством удаленного доступа с компьютера владельца счета денежных средств. Для того чтобы обойти защиту электронных цифровых подписей (ЭЦП), хранимых на защищенных токенах, а также систему обнаружения смены компьютера владельца счета, используется удаленное подключение к компьютеру владельца счета, с которого совершается мошеннический перевод средств. Процесс формирования платежного поручения начинается после того, как владелец счета подключил к ЭВМ токен с ЭЦП. При удаленном подключении преступника работа владельца компьютера не нарушается и может проходить одновременно. Удаленный доступ будет предоставлен атакующему, даже если все входящие соединения к компьютеру владельца счета будут запрещены. Это обеспечивается за счет того, что средства удаленного доступа сами устанавливают исходящее соединение с сервером преступника, а злоумышленник, используя исходящее соединение, подключается к компьютеру владельца счета. Исходящие соединения с компьютером владельца счета, как правило, разрешены для обеспечения нормальной работы в сети «Интернет»;
— автоматический перевод (автозалив). Данный вариант совершения платежа является наиболее совершенным. Автозалив можно сделать двумя способами. Первый — непосредственно перед подписанием платежного поручения владельцем счета вредоносная

[11] См.: *Овчинский В. С.* Криминология цифрового мира. М. : Норма: Инфра-М, 2018. С. 114—115.

[12] *Черных Е.* Киберпреступность и наши телефоны // URL: http://crimescience.ru/?p=9980 (дата обращения: 17.03.2019).

[13] См.: *Черных Е.* Указ. соч.

[14] См.: *Овчинский В. С.* Указ. соч. С. 115.

программа заменит реквизиты платежа, при этом на экране будут отображаться данные, внесенные владельцем счета. В результате владелец счета подпишет уже измененное платежное поручение и отправит его в банк. Второй способ — вредоносная программа дождется подключения токена с ЭЦП, сама запустит систему интернет-банкинга, войдет с использованием логина (пароля) владельца счета, сформирует платежное поручение и отправит его в банк. Для того чтобы троянская программа в автоматическом режиме перевела денежные средства, преступник должен подготовить специальный файл настроек с указанием реквизитов для перевода. Данный файл настроек будет скачан вредоносной программой по команде с сервера управления ботнета[15];

— метод социального инжиниринга предполагает использование троянской программы для перенаправления пользовательских запросов к банковским сайтам на мошеннический сайт со страницами, внешне копирующими настоящий сайт банка. Фишинговый сайт используется для получения конфиденциальных данных пользователей: логина (пароля), номера телефона владельца счета. Переводы денежных средств необходимо подтверждать одноразовым кодом, который может быть получен владельцем счета по СМС, со скрэтч-карты или иным способом. Для получения кода подтверждения мошенник показывает фишинговые страницы, требующие ввести код подтверждения под разными предлогами, например для отмены мошеннической операции. При нажатии на любую из кнопок (аннулировать или подтвердить) код подтверждения будет отправлен преступнику, и он сможет завершить перевод денежных средств. Если пользователь не вводит полученный код подтверждения, то преступник, используя номер телефона, который будет указан пользователем на фишинговом сайте, осуществит звонок владельцу счета от имени банка. Цель звонка — уговорить пользователя ввести код подтверждения перевода денежных средств на фишинговом сайте либо продиктовать код по телефону;

— программы-вымогатели. В России эта угроза стала серьезной проблемой для бизнеса относительно недавно. Основной задачей таких программ является шифрование файлов надежным методом, чтобы расшифровать их можно было только при наличии специального секретного ключа, находящегося у вымогателя. Главное — это «зашифровать не просто файлы, а базы данных, рабочие документы, резервные копии и т.д.»[16] После того как файлы зашифрованы, приходит уведомление, в котором сообщается, сколько и куда необходимо перевести денег, чтобы получить ключ расшифровки. Как правило, оплата производится в биткоинах. Больше всего компании страдают, когда злоумышленники шифруют базы 1С:Бухгалтерии, общие файловые серверы, данные резервных копий. Как отмечает И. Сачков, «основной

[15] Ботнет (от слов robot и network) — компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании (DoS- и DDoS-атаки). Боты как таковые не являются вирусами. Они представляют собой набор программного обеспечения, который может состоять из вирусов, брандмауэров, программ для удаленного управления компьютером, а также инструментов для скрытия от операционной системы (см.: URL: https://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82 (дата обращения: 17.03.2019)).

[16] *Сачков И.* Зашифрованный мир: как работает WannaCry и что умеют программы-вымогатели? // URL: https://www.forbes.ru/tehnologii/344285-zashifrovannyy-mir-kak-rabotaet-wannacry-i-chto-umeyut-programmy-vymogateli (дата обращения: 17.03.2019).

способ распространения таких программ — рассылки по электронной почте вложений под видом банковских выписок, счетов, уведомлений о вызове в суд и т.п.»[17];

— неправомерное использование бренда. Наиболее яркий пример — использование бренда для проведения фишинговых атак на клиентов, партнеров или даже внутренних сотрудников компании. Сейчас многие компании — банки, онлайн-магазины, такси, рестораны и т.д. — выходят на рынок со своими мобильными приложениями. Мошенники используют этот тренд, создавая фейковые мобильные приложения, которые пользователи устанавливают, среагировав на хорошо узнаваемые бренды и символику. Как правило, все они становятся жертвами мошеннических или вредоносных программ. Это не только наносит вред пользователям, скачавшим подобные приложения, но и подрывает доверие к компаниям, которые не уделяют должного внимания защите своих брендов.

В связи с развитием информационных технологий на мировом финансовом рынке появились виртуальные финансовые активы, созданные на основе технологии блокчейн, — криптовалюты, т.е. цифровые записи со своим криптографическим кодом в определенной информационной системе, существующей только в виртуальном пространстве. Криптовалюта имеет децентрализованный характер, не эмитирована государством, обладает рядом преимуществ по сравнению с фиатными деньгами: анонимность, минимальный процент по транзакциям, неподконтрольность публичной власти и т.д. Эти преимущества обусловливают уголовно-правовые риски использования криптовалюты для анонимного финансирования терроризма, незаконного оборота наркотических средств (психотропных веществ), оружия, порнографических материалов, легализации имущества[18].

В судебной практике не вызывает сложностей квалификация преступлений, в которых криптовалюта является средством их совершения, сложности появляются тогда, когда она выступает предметом преступления. Это обусловлено тем, что в российском законодательстве до сих пор не определена юридическая природа криптовалюты, поэтому в теории уголовного права предлагаются разные варианты уголовно-правовой оценки подобных деяний, ни один из которых не основан на буквальном толковании уголовного закона[19].

Федеральный закон «О цифровых финансовых активах», который в том числе должен был определить правовой статус криптовалюты, пока не принят (идет обсуждение проекта, однако примечательно, что Центробанк предложил исключить из него всякое упоминание о криптовалютах). Между тем депутаты Государственной Думы РФ только планируют в течение 2019 г. принять отдельный закон о криптовалютах[20]. В ГК РФ уже внесены изменения — ст. 128 ГК РФ дополнена цифровыми правами[21], а в ст. 141.1[22]

---

[17] *Сачков И.* Указ. соч.

[18] См.: *Уфимцева В. А.* Уголовно-правовые риски использования криптовалюты // Уголовное право: стратегия развития в XXI веке : материалы XVI Междунар. науч.-практ. конференции. М., 2019. С. 140—141.

[19] См.: *Уфимцева В. А.* Указ. соч. С. 145—146.

[20] URL: https://fomag.ru/news-streem/gosduma_rf_otlozhila_vtoroe_chtenie zakonoproekta o tsifrovykh aktivakh / (дата обращения: 24.03.2019).

[21] Некоторые ученые негативно оценивают отнесение цифровых прав к имущественным правам в связи с тем, что, по их мнению, «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» (Правовое регулирование экономических отношений в современных условиях развития цифровой экономики. М. : Юстицинформ, 2019. 376 с.).

[22] Цифровыми правами 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

эти цифровые права разъясняются. Изменения вступят в силу с 1 октября 2019 г.[23] С этого момента неправомерные действия в отношении цифровых прав будут охватываться теми составами преступлений, в которых имущество закреплено в качестве предмета.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Приведен далеко не полный перечень киберугроз в финансовой сфере, основной целью которых является неправомерное завладение чужим имуществом или конфиденциальной информацией посредством использования вредоносных программ. В этой связи некоторые ученые полагают, что, с одной стороны, подобный способ не получил должного отражения в УК РФ, несмотря на наличие, например, п. «г» ч. 3 ст. 158, 159.3, ст. 159.6. С другой стороны, нет единства в оценке неправомерного доступа к чужой информационной системе кредитных учреждений (частных лиц) с намерением завладения чужим имуществом[24], в частности образуется ли совокупность преступлений, предусмотренных ст. 159.6 и ст. 272 УК РФ?[25] Кроме того, в теории уголовного права предлагается дополнить УК РФ самостоятельной «формой хищения с новым способом его совершения — использованием компьютерных технологий»[26]. Не ставя целью проанализировать это предложение, отметим следующее. В условиях цифровизации перед доктриной уголовного права стоит задача скорейшей разработки модели системного обновления отечественного уголовного законодательства, выработки общих правил и четких критериев его осуществления, а не спонтанного ответа на актуальные потребности правоприменителя путем конструирования специальных составов киберпреступлений[27].

БИБЛИОГРАФИЯ

1. *Иногамова-Хегай Л. В.* Квалификация преступлений с использованием компьютерных технологий // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции. — М., 2019.
2. *Ларина Е., Овчинский В.* Русское чудо XXI века // URL: http://zavtra.ru/blogs/russkoe-chudo-xxi-veka.
3. *Новгородская В. Б.* Новые технологии (блокчейн / искусственный интеллект) на службе права: научно-методическое пособие / под ред. Л. А. Новоселовой. — М., 2019.
4. *Овчинский В. С.* Криминология цифрового мира : учебник для магистратуры. — М. : Норма: Инфра-М, 2018.

числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу (ч. 1 ст. 141.1 ГК РФ).

[23] Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // СЗ РФ. 2019. № 12. Ст. 1224.

[24] См.: *Иногамова-Хегай Л. В.* Квалификация преступлений с использованием компьютерных технологий // Уголовное право: стратегия развития в XXI веке. С. 52—55.

[25] Пленум Верховного Суда РФ считает, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ (п. 20 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

[26] *Иногамова-Хегай Л. В.* Указ. соч. С. 54—55.

[27] См.: *Русскевич Е. А.* О концепции «минималистической цифровизации» Особенной части УК РФ // Уголовное право: стратегия развития в XXI веке. С. 110—116.

5. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики : монография / отв. ред. В. А. Вайпан, М. А. Егорова. — М. : Юстицинформ, 2019.
6. *Русскевич Е. А.* О концепции «минималистической цифровизации» особенной части УК РФ // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции. — М., 2019.
7. *Сачков И.* Зашифрованный мир: как работает WannaCry и что умеют программы-вымогатели? // URL: https://www.forbes.ru/tehnologii/344285-zashifrovannyy-mir-kak-rabotaet-wannacry-i-chto-umeyut-programmy-vymogateli.
8. *Уфимцева В. А.* Уголовно-правовые риски использования криптовалюты // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции. — М., 2019.
9. *Черных Е.* Киберпреступность и наши телефоны // URL: http://crimescience.ru/?p=9980.

Материал поступил в редакцию 6 мая 2019 г.

DIGITALIZATION: CRIMINAL LAW RISKS IN THE ECONOMY[28]

ARYAMOV Andrey Anatolievich, Doctor of Law, Professor, Professor of the Department of Criminal Law of the Russian State University of Justice
aaryamov65@yandex.ru
117418, Russia, Moscow, ul. Novocheriomushkinskaya, d. 69

GRACHEVA Yulia Viktorovna, Doctor of Law, Professor, Professor of the Department of Criminal Law of the Kutafin Moscow State Law University (MSAL)
uvgracheva@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *Any industrial revolution not only opens up new opportunities for society and the state, but also endows criminals with previously non-existing methods and tools for committing crimes. Automation and production robotization, artificial intelligence, 3D printing, the creation of new materials and technologies (biotechnologies and information technologies), etc characterize the fourth industrial revolution.*
One of the objects of the criminal law protection under threat of harm due to digitalization is the economy (public relations arising from ensuring the normal functioning of the economy as a single national economic complex). At present, it is possible to distinguish such cyber threats for the economy as attacks on banks, on a broker, on a settlement system, embezzlement through Internet banking and some other actions carried out through the use of malicious programs. Their main purpose is misappropriation of other people's property. The most common methods of embezzlement are the manual transfer of funds from the computer of the account owner through the remote access, automatic software upload, social engineering method, the use of an ransomware program, illegal use of the brand, etc.
In the conditions of digitalization, the science of criminal law faces the task of developing a model for systematic updating of domestic criminal legislation, developing general rules and clear criteria for its implementation, rather than a spontaneous response to the immediate needs of a law enforcer by designing special cybercrime compounds.

Keywords: *digitalization, cybercrime, criminal law risks, cryptocurrency, blockchain, fourth industrial revolution, information technology; extortion programs, attacks on banks.*

[28] The work is carried out with the financial support of the Russian Foundation for Basic Research, Contract No. 18-29-16158 / 18.

REFERENCES (TRANSLITERATION)

1. Inogamova-Hegaj L. V. Kvalifikaciya prestuplenij s ispol'zovaniem komp'yuternyh tekhnologij // Ugolovnoe pravo: strategiya razvitiya v XXI veke : materialy XVI Mezhdunarodnoj nauchno-prakticheskoj konferencii. — M., 2019.
2. Larina E., Ovchinskij V. Russkoe chudo XXI veka // URL: http://zavtra.ru/blogs/russkoe-chudo-xxi-veka.
3. Novgorodskaya V. B. Novye tekhnologii (blokchejn / iskusstvennyj intellekt) na sluzhbe prava: nauchno-metodicheskoe posobie / pod red. L. A. Novoselovoj. — M., 2019.
4. Ovchinskij V. S. Kriminologiya cifrovogo mira : uchebnik dlya magistratury. — M. : Norma: Infra-M, 2018.
5. Pravovoe regulirovanie ekonomicheskih otnoshenij v sovremennyh usloviyah razvitiya cifrovoj ekonomiki : monografiya / otv. red. V. A. Vajpan, M. A. Egorova. — M. : Yusticinform, 2019.
6. Russkevich E. A. O koncepcii «minimalisticheskoj cifrovizacii» osobennoj chasti UK RF // Ugolovnoe pravo: strategiya razvitiya v XXI veke : materialy XVI Mezhdunarodnoj nauchno-prakticheskoj konferencii. — M., 2019.
7. Sachkov I. Zashifrovannyj mir: kak rabotaet WannaCry i chto umeyut programmy-vymogateli? // URL: https://www.forbes.ru/tehnologii/344285-zashifrovannyy-mir-kak-rabotaet-wannacry-i-chto-umeyut-programmy-vymogateli.
8. Ufimceva V. A. Ugolovno-pravovye riski ispol'zovaniya kriptovalyuty // Ugolovnoe pravo: strategiya razvitiya v XXI veke : materialy XVI Mezhdunarodnoj nauchno-prakticheskoj konferencii. — M., 2019.
9. Chernyh E. Kiberprestupnost' i nashi telefony // URL: http://crimescience.ru/?p=9980.