Научная статья
УДК 343
EDN NZNOMN
DOI 10.17150/2411-6262.2022.13(1).22

О.С. Капинус
Университет прокуратуры Российской Федерации, г. Москва, Российская Федерация,
rector@agprf.org

ЦИФРОВИЗАЦИЯ ПРЕСТУПНОСТИ И УГОЛОВНОЕ ПРАВО

АННОТАЦИЯ. Вступление России в эпоху информационного общества повлекло существенную трансформацию экономики, способов коммуникации людей, характера социальных связей, что не могло не затронуть преступность. Представители криминального сообщества быстро взяли на вооружение новые информационно-коммуникационные технологии и переместили значительную часть своей противоправной деятельности в онлайн-пространство, вследствие чего преступность приобрела качественно новые характеристики.

Цифровизация изменила не только качественные параметры, но и масштабы преступности. Преступления в сфере компьютерной информации по своим объемам многократно (на насколько порядков) превышают все остальные виды преступлений, взятые вместе.

Процессы цифровизации оказали существенное влияние на традиционные сегменты преступности, в том числе, корыстную преступность. Предметом корыстных посягательств в большинстве случаев становятся уже не вещи (включая наличные деньги), а безналичные денежные средства. А по мере развития, усложнения и диверсификации цифрового финансового и квазифинансового оборота предметом хищения все чаще становятся новые виды «бестелесных» активов – криптовалюта, бонусы потребительской лояльности, виртуальные объекты, используемые игроками в многопользовательских онлайн-играх. В соответствии с этим неизбежно трансформируются и способы хищения. Для хищения безналичных денег и нематериальных финансовых активов используются неправомерный доступ к охраняемой законом компьютерной информации, вредоносные компьютерные программы, методы социальной инженерии.

Таким образом, цифровизация глобальной экономики и российского общества кардинально изменили криминальный ландшафт, масштабы, структуру и качественные характеристики преступности. По идее, уголовное право должно оперативно реагировать на происходящие трансформации, надлежащим образом учитывать новую криминальную реальность, подстраиваться под нее, создавать новые и адаптировать существующие инструменты противодействия противоправной деятельности. Однако действующее уголовное законодательство явно отстает от современных тенденций преступности, что снижает его превентивный и охранительный потенциал.

Автор приходит к неутешительному выводу о том, что адаптация уголовного законодательства и правоприменительной практики для противодействия цифровой преступности осуществляется медленно, непоследовательно и противоречиво, показывая соответствующие проблемы на конкретных примерах.

С точки зрения автора, современная криминологическая реальность требует смены векторов уголовной политики, трансформации базовых уголовно-правовых положений и институтов, уточнения существующих уголовно-правовых запретов и криминализации новых общественно опасных деяний, т.е. полномасштабной реформы уголовного права.

КЛЮЧЕВЫЕ СЛОВА. Цифровая преступность, цифровизация преступности, информационно-коммуникационная преступность, уголовное право, криптоактивы, хищение.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 27 февраля 2022 г.; дата принятия к печати 21 марта 2022 г.; дата онлайн-размещения 30 апреля 2022 г.

Original article

O.S. Kapinus
University of Prosecutor's Office of the Russian Federation, Moscow, Russian Federation,
rector@agprf.org

DIGITALIZATION OF CRIME AND CRIMINAL LAW

ABSTRACT. Russia's entry into the era of the information society entailed a significant transformation of the economy, the ways people communicate, the nature of social ties, which could not but affect crime. Representatives of the criminal community adopted quickly new information and communication technologies and moved a significant part of their illegal activities to the online space, as a result of which crime acquired qualitatively new characteristics.

Digitalization has changed not only the qualitative parameters, but also the scale of crime. Crimes in the field of computer information in their volumes are many times higher (by how many orders of magnitude) than all other types of crimes taken together. Digitalization processes have had a significant impact on traditional segments of crime, including mercenary crime. In most cases, the object of mercenary encroachments is no longer things (including cash), but non-cash funds. And with the development, complexity and diversification of digital financial and quasi-financial turnover, new types of "disembodied" assets are becoming increasingly the subject of theft - cryptocurrency, consumer loyalty bonuses, virtual objects used by players in multiplayer online games. In accordance with this, the methods of theft are transformed inevitably. Illegal access to legally-protected computer information, malicious computer programs, and social engineering methods are used to steal non-cash money and intangible financial assets.

Thus, the digitalization of the global economy and Russian society has changed radically the criminal landscape, the scale, structure and qualitative characteristics of crime. In fact, the criminal law should respond promptly to the ongoing transformations, properly take into account the new criminal reality, adapt to it, create new and adapt existing tools to counter illegal activities. However, the current criminal legislation clearly lags behind modern crime trends, which reduces its preventive and protective potential.

The author comes to the disappointing conclusion that the adaptation of criminal legislation and law enforcement practice to counteract digital crime is slow, inconclusive and contradictory, showing the relevant problems on exact examples.

From the author's point of view, modern criminological reality requires a change in the vectors of criminal policy, transformation of basic criminal law provisions and institutions, clarification of existing criminal law prohibitions and criminalization of new socially dangerous acts, i.e. a full-scale reform of criminal law.

KEYWORDS. Digital crime, digitalization of crime, information and communication crime, criminal law, crypto assets, theft.

ARTICLE INFO. Received February 27, 2022; accepted March 21, 2022; available online April 30, 2022.

Вступление России в эпоху информационного общества повлекло трансформацию практически всех сфер жизни. Стремительное развитие цифровых технологий до неузнаваемости изменило экономику, способы коммуникации людей, характер социальных связей, государственное управление, да и все социальное пространство, перевело значительную его часть в виртуальную плоскость. Эти процессы, конечно же, не могли не затронуть и преступность.

Представители криминального сообщества быстро взяли на вооружение новые информационно-коммуникационные технологии и переместили значительную часть своей противоправной деятельности в онлайн-пространство, вследствие чего преступность приобрела качественно новые характеристики — экстерритори-

альность, виртуальность, гипертаргетированность, мультипликативность (способность к самовоспроизводству), сверхизменчивость [1, с. 12–14].

Цифровизация изменила не только качественные параметры, но и масштабы преступности. В 2021 г. официально зарегистрировано 2 004 404 преступлений. При этом удельный вес преступлений, совершенных с использованием информационно-коммуникационных технологий или в сфере компьютерной информации (обозначим их собирательным понятием цифровая или информационно-коммуникационная преступность), составил 25,8 % от всех зарегистрированных преступлений (в 2020 г. — 25,0 %, в 2019 г. — 14,5 %).

Официальная статистика фиксирует некоторую стабилизацию показателей регистрации цифровой преступности. Темпы их прироста в 2021 г. сильно замедлились: по сравнению с 2020 г. их количество возросло на 1,4 % — с 510 396 до 517 722, тогда как в 2020 г. — на 73,4 %, в 2019 г. — на 68,5 %.

Однако приведенные показатели не отражают истинные масштабы информационно-коммуникационной преступности. По оценкам специалистов, 85–97 % компьютерных преступлений остаются латентными [2, с. 35]. Причем имеются все основания считать эти оценки заниженными. В 2021 г. по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» зарегистрировано всего 6 392, а по ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» — 317 преступлений. При этом в том же 2021 г. программные решения «Лаборатории Касперского» обнаруживали в среднем 380 тыс. новых вредоносных файлов в день (!)[1]. И это данные лишь одного игрока на рынке антивирусной компьютерной защиты. На этом фоне официальные показатели регистрации преступлений в сфере компьютерной информации, предусмотренных гл. 28 УК РФ, выглядят как капля в море. Правоохранительные органы регистрируют лишь мизерную часть совершаемых преступлений в сфере компьютерной информации, хотя по своим объемам они многократно (на несколько порядков) превышают все остальные виды преступлений, взятые вместе.

За рамками официального статистического учета остается огромный массив преступных посягательств на безналичные денежные средства граждан, совершенных с использованием информационно-коммуникационных технологий. По оценкам Сбербанка, в 2020 г. совершено не менее 15 млн телефонных звонков с целью хищения денежных средств, находящихся на банковских счетах[2]. В 2021 г. представители Сбербанка заявили, что «кибермошенники совершают около 100 тысяч звонков в день, каждый 10-й звонок любому абоненту в России — это звонок преступника. Девять из 10 владельцев мобильных телефонов сталкивались с телефонным мошенничеством и принимали такого рода звонки»[3].

При этом в 2020 г. официально зарегистрировано всего 218 739 преступлений, совершенных с использованием или применением средств мобильной связи, а в 2021 г. их число составило 217 552, что конечно же не соответствует реальным масштабам соответствующего вида криминальной деятельности.

Цифровизация экономической деятельности и гражданского оборота не только породила новые криминальные вызовы и угрозы, но и оказала существенное влияние на традиционные сегменты преступности, в том числе, корыстную преступность.

---

[1] В 2021 году решения «Лаборатории Касперского» в среднем обнаруживали ежедневно 380 тысяч вредоносных файлов. URL: https://www.kaspersky.ru/about/press-releases/2021_v-2021-godu-resheniya-laboratorii-kasperskogo-v-srednem-obnaruzhivali-ezhednevno-380-tysyach-vredonosnyh-fajlov.

[2] Сбербанк оценил число мошеннических звонков в России за год. URL: https://www.rbc.ru/society/12/12/2020/5fd446c49a7947746aba6e19.

[3] Сбербанк назвал телефонное мошенничество национальным бедствием. URL: https://ria.ru/20210707/moshennichestvo-1740256569.html.

По данным Центрального Банка России, доля безналичных платежей в розничном платежном обороте с 2013 по 2020 гг. выросла почти в 5 раз и на 01.01.2021 г. превысила 70 %. На 01.01.2021 г. общее количество выпущенных российскими кредитными организациями платежных карт составило 305,6 млн. единиц. В России 93,7 % взрослого населения пользуются банковским счетом, при этом 74,8 % пользуются интенсивно (три и более операции в месяц). Доля взрослого населения, использующего дистанционный доступ к банковским счетам для осуществления перевода денежных средств (Интернет и/или мобильный банкинг), составляет около 75,4 % [4].

Происходящие структурные изменения форм сохранения сбережений и способов управления финансовыми активами закономерным образом изменили вектор корыстных преступных посягательств. Их предметом в большинстве случаев становятся уже не вещи (включая наличные деньги), а безналичные денежные средства. А по мере развития, усложнения и диверсификации цифрового финансового и квазифинансового оборота предметом хищения все чаще становятся новые виды «бестелесных» активов — криптовалюта, бонусы потребительской лояльности, виртуальные объекты, используемые игроками в многопользовательских онлайн-играх, и т.п.

В соответствии с этим неизбежно трансформируются и способы хищения. Для хищения безналичных денег и нематериальных финансовых активов используются неправомерный доступ к охраняемой законом компьютерной информации, вредоносные компьютерные программы, методы социальной инженерии. При этом насильственные и иные «контактные» корыстные посягательства (карманные и квартирные кражи) постепенно уходят в прошлое. Официальная статистика фиксирует ежегодное сокращение доли грабежей, разбоев, вымогательств. Суммарный удельный вес корыстно-насильственных преступлений в общем количестве зарегистрированных преступлений составил в 2021 г. 2,1 %, тогда как в 2015 г. он находился на уровне 3,8 %, в 2010 г. — 7,4 %, а в 2005 г. — 11,9 %.

Итак, цифровизация глобальной экономики и российского общества кардинально изменили криминальный ландшафт, масштабы, структуру и качественные характеристики преступности. По идее, уголовное право должно оперативно реагировать на происходящие трансформации, надлежащим образом учитывать новую криминальную реальность, подстраиваться под нее, создавать новые и адаптировать существующие инструменты противодействия противоправной деятельности. Однако действующее уголовное законодательство явно отстает от современных тенденций преступности, что снижает его превентивный и охранительный потенциал.

Адаптация уголовного законодательства и правоприменительной практики для противодействия цифровой преступности осуществляется медленно, непоследовательно и противоречиво. Весьма показательной в этом отношении можно считать ситуацию с реформированием уголовно-правовых норм об ответственности за хищение.

С одной стороны, необходимо признать, что правоприменительная практика, а вслед за ней и законодатель довольно оперативно отреагировали на изменение вектора корыстных посягательств. В 2017 г. Пленум Верховный Суд Российской Федерации признал безналичные денежные средства предметом хищения, т.е. имуществом в уголовно-правовом смысле (см. п. 5 постановления Пленума от 30.11.2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»). Такое решение нельзя считать безупречным, ведь с позиции гражданского права безналичные денежные средства представляют собой имущественное право обязательственного характера (право требования клиента к банку) (см.

[4] Аналитическая справка об индикаторах финансовой доступности за 2020 год (по результатам замера 2021 года). URL: https://cbr.ru/Content/Document/File/124646/acc_indicators_29072021.pdf.

постановление Конституционного Суда Российской Федерации от 10.12.2014 г. № 31-П). Тем не менее, с точки зрения инструментальных правоприменительных соображений позицию Пленума следует признать полностью оправданной. Впоследствии этот подход был реализован на законодательном уровне. Федеральным законом от 23.04.2018 г. № 111-ФЗ ч. 3 ст. 158 УК РФ была дополнена п. «г», предусматривающим ответственность за кражу с банковского счета, а равно в отношении электронных денежных средств. Таким образом законодатель признал, что безналичные и электронные денежные средства являются предметом хищения, т.е. имуществом, хотя соответствующие финансовые активы имеют не вещную, а обязательственную природу.

Расширительная трактовка имущества позволила правоприменительным органам обеспечить надлежащую уголовно-правовую оценку корыстных посягательств на криптовалюту, причем охранительный потенциал уголовного закона был реализован даже в условиях неопределенности позитивного регулирования [3, с. 74–85; 4, с. 59–69].

С другой стороны, нужно понимать, что подобное расширение уголовно-правового понятия «имущество» неизбежно вступает в противоречие с существующей конструкцией хищения, регламентированной в п. 1 примечаний к ст. 158 УК РФ. Дело в том, что «новый» предмет хищения (точнее, его новая расширительная трактовка) не укладывается в рамки его «старой» объективной стороны, которая определяется в законе как изъятие и (или) обращение чужого имущества в пользу виновного или других лиц. В юридической литературе справедливо отмечается, что такое понимание объективной стороны хищения непригодно для противоправных корыстных посягательств на криптоактивы. Что же касается цифровых финансовых активов и безналичных денег, то корыстное посягательство на них вообще не может описываться в терминах «изъятие» и «обращение в пользу виновного». Эти понятия представляют собой уголовно-правовую проекцию вещно-правовой терминологии, тогда как цифровые финансовые активы и безналичные деньги имеют обязательственно-правовую природу. Имущественное обязательство не может быть объектом владения (да и права собственности в целом), а потому его изъятие из правомерного владения невозможно. Посредством противоправных действий можно лишь заменить кредитора, т.е. осуществить незаконный «перевод» имущественного права требования одного лица (потерпевшего) к другому (виновному) [5, с. 71–87].

Поэтому адаптация предписаний гл. 21 УК РФ «Преступления против собственности» к потребностям противодействия цифровой преступности не должна ограничиваться лишь расширением трактовки предмета хищения. Необходимо системное изменение подхода к регламентации ответственности за хищения, которое должно осуществляться с учетом специфики посягательств на цифровые активы.

Нельзя не обратить внимание и на противоречия в части дифференциации уголовной ответственности за информационно-коммуникационные преступления против собственности. Федеральный закон от 23.04.2018 г. № 111-ФЗ признал кражу с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ) тяжким преступлением и отнес ее к числу особо квалифицированных видов кражи. При этом в пояснительной записке к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств)» соответствующее законодательное решение объясняется следующим образом: «Высокая степень общественной опасности указанных противоправных деяний подтверждается спецификой преступлений,

совершить которые могут лишь лица, обладающие специальными знаниями и использующие технические средства, что приводит к нарушению не только права собственности, но и банковской тайны».

Однако практика применения п. «г» ч. 2 ст. 158 УК РФ пошла вразрез с идеями разработчиков соответствующего законопроекта. Эта новелла задумывалась как инструмент противодействия высокотехнологичным кражам с банковских счетов, которые совершаются посредством неправомерного доступа к компьютерной информации или с использованием методов социальной инженерии, а на деле ее чаще всего применяют для квалификации банальных хищений безналичных денежных средств с использованием найденных или похищенных банковских карт, оборудованных системой бесконтактных платежей. Типичная ситуация — злоумышленник нашел потерянную банковскую карту или завладел чужой банковской картой, после чего совершал покупки (как правило, неоднократные) товаров с использованием этой банковской карты на сумму, не превышающую лимит для бесконтактной оплаты (1000 руб.). Правоохранительные органы и суды квалифицируют такие хищения как тяжкое преступление по п. «г» ч. 3 ст. 158 УК РФ (соответствующие приговоры исчисляются тысячами), хотя для их совершения «большого ума» не нужно. Очевидно, что здесь нужна иная — более тонкая — дифференциация уголовной ответственности, основанная не на свойствах предмета хищения, а на специфике способа его совершения.

В заключение отметим, что эти и иные проблемы, обусловленные процессами цифровизации преступности, требуют системного научно обоснованного решения. Причем нужно понимать, что точечными поправками, вносимыми в УК РФ с целью подстроить его под очередную высокотехнологичную криминальную новацию, здесь обойтись не получится. Мы не сможет должным образом адаптировать российское уголовное право к новой преступности, изменяя УК РФ по принципу «стимул — реакция», «вызов — ответ», не имея при этом современной концепции уголовной политики, четких представлений о целях, задачах, принципах, пределах уголовно-правового противодействия преступности и его ожидаемых результатах [6, с. 37–46]. Современная криминологическая реальность требует смены векторов уголовной политики, трансформации базовых уголовно-правовых положений и институтов, уточнения существующих уголовно-правовых запретов и криминализации новых общественно опасных деяний, т.е. полномасштабной реформы уголовного права.

Список использованной литературы

1. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения / Е.А. Русскевич. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2022. — 227 с.

2. Противодействие киберпреступности в аспекте обеспечения национальной безопасности / П.В. Агапов, С.В. Борисов, Д.В. Вагурин [и др.]. — Москва : Юнити, 2014. — 512 с.

3. Ображиев К.В. Хищение цифровой валюты (криптовалюты): проблемы квалификации / К.В. Ображиев // Уголовный закон в эпоху искусственного интеллекта и цифровизации : материалы Всерос. науч.-практ. конф., Саратов, 9 июня 2021 г. / под общ. ред. А.Г. Блинова, Е.В. Кобзевой. — Саратов, 2021. — С. 74–85.

4. Пикуров Н.И. Проблемы определения юридической природы криптовалюты для квалификации преступлений против собственности / Н.И. Пикуров // Вестник Университета прокуратуры Российской Федерации. — 2021. — № 4 (84). — С. 59–69.

5. Ображиев К.В. Преступные посягательства на цифровые финансовые активы и цифровую валюту: проблемы квалификации и законодательной регламентации / К.В. Ображиев. — DOI 10.12737/jrl.2022.018 // Журнал российского права. — 2022. — № 2. — С. 71–87.

6. Капинус О. Криминализация и декриминализация деяний: поиск оптимального баланса / О. Капинус. — DOI 10.31857/S086904990000367-5 // Общественные науки и современность. — 2018. — № 4. — С. 37–46.

References

1. Russkevich E.A. *Criminal Law and Digital Crime: Problems and Solutions*. Moscow, Infra-M Publ., 2022. 227 p.

2. Agapov P.V., Borisov S.V., Vagurin D.V., Korenyuk A.L., Merkurev V.V. *Counteracting Cybercrime in the Light of Ensuring National Security*. Moscow, Yuniti Publ., 2014. 512 p.

3. Obrazhiev K.V. Theft of Digital Currency (Cryptocurrency): Qualification Problems. In Blinov A.G., Kobzeva E.V. (eds). *Criminal Law in the Era of Artificial Intelligence and Digitalization. Materials of All-Russian Research Conference, Saratov, June 9, 2021*. Saratov, 2021, pp. 74-85. (In Russian).

4. Pikurov N.I. Issues of Determining the Legal Nature of Cryptocurrency in the Qualification of Property Primes. *Universiteta prokuratury Rossiiskoi Federatsii = Bulletin of the University of the Prosecutors Office of the Russian Federation*, 2021, no. 4, pp. 59-69. (In Russian).

5. Obrazhiev K.V. Criminal Attacks on Digital Financial Assets and Digital Currency: Qualification and Legal Regulation Issues. *Zhurnal rossiyskogo prava = Russian Law Journal*, 2022, no. 2, pp. 71–87. (In Russian). DOI: 10.12737/jrl.2022.018.

6. Kapinus O. Criminalization and Decriminalization of Acts: Finding the Best Balance. *Obshchestvennye nauki i sovremennost' = Social Science and Modernity*, 2018, no. 4, pp. 37–46. (In Russian). DOI: 10.31857/S086904990000367-5.

Информация об авторе

Капинус Оксана Сергеевна — доктор юридических наук, профессор, ректор Университета прокуратуры Российской Федерации, г. Москва, Российская Федерация, rector@agprf.org, AuthorID РИНЦ: 508753, Scopus Author ID: 55867575200.

Author

Oksana S. Kapinus — D.Sc. in Law, Full Professor, Rector of the University of the Prosecutor's Office of the Russian Federation, Moscow, Russian Federation, rector@agprf.org, AuthorID RSCI: 508753, Scopus Author ID: 55867575200.

Для цитирования

Капинус О.С. Цифровизация преступности и уголовное право / О.С. Капинус. — DOI 10.17150/2411-6262.2022.13(1).22. — EDN NZNOMN // Baikal Research Journal. — 2022. — Т. 13, № 1.

For Citation

Kapinus O.S. Digitalization of Crime and Criminal Law. *Baikal Research Journal*, 2022, vol. 13, no. 1. (In Russian). EDN: NZNOMN. DOI: 10.17150/2411-6262.2022.13(1).22.