

УГОЛОВНО-ПРАВОВЫЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

М. А. Ефремова, crimlaw16@gmail.com
Казанский филиал Российского государственного университета правосудия,
г. Казань, Россия

Аннотация. В статье рассматриваются проблемы трансформации и противодействия преступности в условиях цифровизации. Переход к новому поколению Интернета и развитие его как децентрализованной онлайн-экосистемы, основанной на технологиях блокчейн, открывают широкие границы для новых форм преступности. Появление цифровой валюты и цифровых финансовых активов привело к расширительной трактовке предмета хищения и отнесению к таковому предметов, лишенных материальной или вещной формы. Не могут выступать предметом преступлений против собственности невзаимозаменяемые токены, бонусы в программах потребительской лояльности и виртуальное имущество в компьютерных играх. Оставляя цифровые следы в виртуальном пространстве, лицо формирует совокупность данных, именуемых цифровой личностью, которые могут стать предметом посягательства, некоторые из которых остаются за рамками действующего уголовного законодательства.

Ключевые слова: уголовное право, цифровизация, информационно-телекоммуникационные сети, хищение, преступление, метавселенная.

Для цитирования: Ефремова М. А. Уголовно-правовые средства противодействия преступности в условиях цифровизации // Вестник ЮУрГУ. Серия «Право». 2024. Т. 24. № 2. С. 21–26. DOI: 10.14529/law240204.

Original article
DOI: 10.14529/law240204

CRIMINAL LAW MEANS OF COMBATING CRIME IN THE CONTEXT OF DIGITALIZATION

М. А. Efremova, crimlaw16@gmail.com
Kazan Branch of the Russian State University of Justice, Kazan, Russia

Abstract. The article discusses the problems of transformation and combating crime in the context of digitalization. The transition to a new generation of the Internet and its development as a decentralized online ecosystem based on blockchain technologies opens wide boundaries for new forms of crime. The emergence of digital currency and digital financial assets has led to a broad interpretation of the subject of theft and the classification of objects that lack material or real form as such. Non-fungible tokens, bonuses in consumer loyalty programs and virtual assets in computer games cannot be the subject of crimes against property. By leaving digital traces in the virtual space, a person forms a set of data called a digital identity, which can become the subject of an attack, some of which remain outside the scope of the current criminal legislation.

Keywords: criminal law, digitalization, information and telecommunication networks, theft, crime, metaverse.

For citation: Efremova M. A. Criminal law means of combating crime in the context of digitalization. *Bulletin of the South Ural State University. Series "Law"*. 2024. vol. 24. no. 2. pp. 21–26. (in Russ.) DOI: 10.14529/law240204.

Согласно данным Международного союза электросвязи примерно 67 % населения мира, или 5,4 миллиарда человек, в настоящее вре-

мя подключены к Интернету. Данный показатель увеличился на 4,7 % с 2022 года. В Европе, Содружестве Независимых Государств

(СНГ) и Америке от 87 % до 91 % населения пользуется Интернетом [9]. Доступность Интернета обусловила переход преступности на «цифровые рельсы», то есть перемещение ее в режим «онлайн». Включение информационно-телекоммуникационных технологий в «традиционные» формы и способы противоправной деятельности, в конечном итоге, породило не просто новый вид преступности, а совершенно уникальное явление, которое отличается принципиально иным механизмом совершения преступления.

Переход к Интернету эпохи Web3, развитие технологий искусственного интеллекта, блокчейн актуализируют вопросы о способности современного уголовного права противостоять новым угрозам и о возможностях его адаптации к произошедшим переменам.

В последние несколько лет во всем мире была запущена интеграция Интернета в формате Web3, который предполагает наличие некой децентрализованной онлайн-экосистемы, основанной на технологиях блокчейн. С внедрением Web3 в новом направлении стала развиваться и виртуальная реальность, а также метавселенная. Метавселенная позволяет взаимодействовать людям, аватарам, робототехнике и Интернету так, будто они находятся не в виртуальном, а в реальном мире. С позиции уголовного права метавселенная в обозримом будущем будет представлять определенные риски. Отсутствие эффективного регулирования технологий блокчейн и Web3 будет способствовать тому, что метавселенная может стать своеобразной площадкой для преступной деятельности. На сегодняшний день основными видами противоправной деятельности в метавселенной являются мошенничество, кража виртуальных активов, легализация и отмывание преступных доходов, манипулирование рынком. Финансовые преступления – далеко не единственные формы противоправной деятельности в метавселенной. Возвращаясь к рискам, обусловленным появлением метавселенной, к их числу следует отнести прежде всего неконтролируемый поток передачи большого объема данных, что делает их уязвимыми и доступными для неправомерного использования. Метавселенной присуща иммерсия, то есть погружение, эффект которой достигается благодаря органам чувств. Ввиду этой особенности у пользователей отсутствует возможность получить физический вред. Однако в результате воздейст-

вия на их аватар со стороны других пользователей присутствует опасность вреда психического. Эффект присутствия может вызвать чувство страха, тревожности и причинить психологическую травму. Осмысление метавселенной через призму уголовного права еще предстоит, однако этому должно предшествовать решение вопроса о регулировании отношений в ней, что может произойти по самым различным сценариям. Один из них базируется на идее невмешательства реального права в виртуальные отношения. Чем больше стирается грань между реальным миром и виртуальным, тем больше очевидным становится вывод о том, что полностью воздержаться от подобного невмешательства едва ли возможно. Применение аналогии и распространения норм реального права на виртуальные отношения следует признать другой крайностью. Компромиссной видится перспектива урегулирования отношений в виртуальной среде посредством разработки своеобразных правил поведения, которые должны соблюдаться заинтересованными сторонами и точечным регулированием нормами права тех отношений, которые никак иначе урегулированы быть не могут.

Если вопросы противодействия преступности в метавселенной пока еще остаются вопросами будущего, то в настоящее время требует решения проблема квалификации посягательств на так называемое виртуальное имущество, то есть активы, лишенные традиционной вещной формы, – безналичные денежные средства, цифровые права, криптовалюту, NFT, «имущество» в компьютерных играх, бонусные баллы в программах потребительской лояльности. Для завладения новыми «бестелесными» активами используются бесконтактные или дистанционные способы. Ввиду их специфичности закономерно возникает вопрос о возможностях применения положений гл. 21 УК РФ в подобных ситуациях. Предусмотрев уголовную ответственность за кражу с банковского счета и электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), сам законодатель уже пошел по пути признания в качестве предмета хищения «бестелесных» активов. Высшие судебные инстанции в своих актах также относят безналичные и электронные денежные средства к имуществу и предмету хищения, а в п. 5 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48

«О судебной практике по делам о мошенничестве, присвоении и растрате» говорится, что безналичные, электронные денежные средства, бездокументарные ценные бумаги являются имуществом, а, следовательно, и предметом хищения.

В гражданском законодательстве безналичные денежные средства, бездокументарные ценные бумаги, цифровые права определяются как разновидность имущественных прав, которые в свою очередь отнесены к категории иного имущества. Немногочисленная правоприменительная практика, которая начала складываться еще в отсутствие позитивного регулирования оборота цифровых финансовых активов и цифровой валюты, преимущественно пошла по пути признания таковых в качестве предмета хищения. С одной стороны, подобный подход позволяет уголовному праву, как основному элементу механизма уголовно-правовой охраны, решать стоящие перед ним задачи. С другой стороны, усиливается рассогласованность между нормами гражданского и уголовного права, происходит «размывание» понятия хищения [5, с. 82]. Следует согласиться с мнением о том, что подобная расширительная трактовка имущества «не укладывается в рамки объективной стороны хищения, которая определяется в законе как изъятие и (или) обращение чужого имущества в пользу виновного или других лиц» [3].

Вовсе не урегулированным следует признать вопрос о правовом статусе других «бестелесных активов»: «имущества» в компьютерных играх, бонусных баллов в программах потребительской лояльности различных торговых сетей и иного виртуального имущества. И хотя виртуальные активы фактически не являются имуществом, а представляют собой информацию в виде компьютерного кода, оно может выступать предметом сделок уже за реальные денежные средства. Ввиду того, что виртуальное имущество не является цифровыми правами, оно не может выступать предметом преступлений против собственности [4, с. 5].

Специфическим предметом посягательства следует признать и NFT (non fungible token) или невзаимозаменяемый токен. Особенность NFT заключается в том, что он может быть цифровой копией объекта материального мира или другого нематериального объекта, а также выступать в качестве самостоятельного

виртуального объекта. NFT позволяет оцифровать все, что угодно. NFT может выступать, с одной стороны, как сертификат, удостоверяющий право собственности, и как самостоятельный объект, с другой. Пока статус виртуального имущества не определен, сложности видятся и в определении юридического признака таких активов, а именно в установлении собственника или владельца. Как отмечает В. В. Хилюта, разработчики компьютерных игр обладают исключительными правами на программу и иные ее составляющие, следовательно, именно им принадлежат виртуальные его объекты. Однако приобретая имущество в компьютерной игре, лицо становится собственником, но лишь в виртуальной реальности [7, с. 70]. Отношения между разработчиками и пользователями игр обычно регламентируются пользовательским соглашением, а отношения между пользователями внутри игры – правилами самой игры. Правила некоторых игр допускают и даже поощряют возможность кражи игрового имущества (например, в игре Ultima online). Поэтому неправомерное завладение чужим виртуальным имуществом возможно путем противоправного доступа к аккаунту пользователя. Ввиду изложенного применить к подобного рода посягательствам нормы гл. 21 УК РФ не представляется возможным. Из имеющегося арсенала уголовно-правовых средств противодействия неправомерному завладению виртуальным имуществом остается ч. 2 ст. 272 УК РФ, предусматривающая уголовную ответственность за неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершенный из корыстной заинтересованности. Вышеизложенное позволяет сделать вывод о том, что в контексте посягательств на «бестелесные» предметы адаптационные возможности положений гл. 21 УК РФ исчерпаны и необходим принципиально новый подход к регламентации ответственности за их хищение.

Один из таких подходов предложен В. В. Хилютой, который считает, что в рамках «теории имущественных преступлений следует развивать два самостоятельных направления, которые бы четко разграничивали между собой посягательства на телесное и бестелесное имущество ввиду специфичности способа деятельности, механизма причинения ущерба и предмета преступного посягательства» [8, с. 22]. Ученый полагает, что о хищении мож-

но говорить исключительно как о посягательстве на имущество, имеющее вещный признак. Во всех остальных случаях речь идет о посягательствах на объекты гражданских прав. Иной позиции придерживается А. В. Архипов, полагая необходимым отказаться «от разделения предмета преступлений против собственности на имущество и право на имущество», а «после отказа законодателя от обязательности физического (вещного) признака предмета хищения сохраняющееся в законе разделение предмета преступлений против собственности на имущество и право на имущество утратило смысл» [1, с. 23]. Представляется, что решение ряда вышеперечисленных проблем первично должно произойти в рамках гражданского законодательства, однако трансформация понятия хищения в обозримом будущем все же неизбежна.

Процессы цифровизации обусловили появление такого феномена, как «цифровая личность», а, следовательно, и потребность в совершенствовании механизма уголовно-правовой охраны в этом направлении. Цифровая личность представляет собой образ человека в цифровом пространстве и включает в себя все аспекты и данные, связанные с конкретным субъектом в виртуальной среде. Сюда можно отнести логины и пароли, персональные данные, информацию об аккаунтах в социальных сетях и многое другое. Следовательно, структура цифровой личности строится на основе тех данных, которые лицо само предоставляет или оставляет в сети. Иными словами, цифровая личность – это совокупность цифровых следов, оставленных владельцем о самом себе. Сегодня существует множество схем и способов завладения цифровыми личными данными: покупка их в Darknet, фишинговые атаки и рассылки вредоносного программного обеспечения. Получая доступ к цифровым данным о лице, злоумышленники могут совершить целый ряд преступлений. Неправомерное завладение данными о цифровом облике лица может осуществляться с целью последующих незаконных финансовых операций, создания «цифровых двойников», изменения данных о личности и т.д. Подобные действия образуют так называемую «кражу цифровой личности» (digital identity theft). В отдельных случаях подобным деяниям можно дать надлежащую правовую оценку, однако положения действующего уголовного законодательства не дают внятного ответа на вопрос

о квалификации использования технологий реконструкции лица другого человека в режиме реального времени [6, с. 590]. Сложности могут возникнуть и при квалификации деяний, совершенных при помощи синтетической идентификации с использованием неполных данных (synthetic identify), когда объединяется реальная и недостоверная информация для создания «новой» личности.

Подводя итог вышеизложенному, отметим, что современное уголовное право, столкнувшись с цифровой реальностью, не всегда способно выполнять свои базовые функции. Цифровизация механизма совершения преступлений привела не только к трансформации традиционной преступности, но и к кризису уголовного права [6, с. 590], которое запаздывает и не реагирует на стремительно меняющиеся реалии, а охранительно-предупредительные функции в подобных условиях в полной мере не реализуются. Незначительный запас прочности для противодействия преступности в условиях цифровизации у действующего уголовного законодательства еще присутствует, но и он стремительно исчерпывается под влиянием вышеназванных процессов. Однако предложить какой-либо определенный путь в устранении возникшего сбоя механизма уголовно-правовой охраны весьма затруднительно, потому как невозможно предсказать, как будут развиваться информационно-коммуникационные технологии. Социальная реальность такова, что виртуальное и реальное тесно переплетены между собой. Пользователи метавселенной и компьютерных игр, владельцы нематериальных активов являются реальными людьми. В свою очередь отношения, возникающие в связи вышесказанным, нельзя признать сугубо виртуальными. В англосаксонской правовой системе для решения вопроса о границах между реальным и виртуальным в игровой сфере разработана концепция «магического круга» (The Magic Circle Test) [2]. Суть концепции заключается в том, что все происходящее в виртуальном пространстве находится в рамках «магического круга», однако если виртуальные отношения влекут последствия для мира реального, то круг разрывается и они могут попасть под сферу действия права. Представляется, что данная концепция не утратила своей актуальности и по сей день. Для опережающего регулирования отношений, порожденных цифровизацией, необходимо объединение усилий

представителей юридической науки, поскольку только таким путем возможно выработать принципиальные теоретико-прикладные ре-

шения о границах действия права, от которых в свою очередь будет зависеть эволюционное развитие уголовного права.

Список источников

1. Архипов А. В. Цифровые объекты как предмет хищения // Уголовное право. 2020. № 6. С. 16–23.
2. Дюранске Б. Т., Кейн Ш. Ф. Виртуальные миры, реальные проблемы // Известия высших учебных заведений. Правоведение. 2013. № 2 (307). С. 115–134.
3. Капинус О. С. Цифровизация преступности и уголовное право // Baikal Research Journal. 2022. Т. 13. № 1.
4. Мочалкина И. С. Цифровые права и цифровая валюта как предмет преступлений в сфере экономики: дис. ... канд. юрид. наук. М., 2022. 240 с.
5. Ображиев К. В. Преступные посягательства на цифровые финансовые активы и цифровую валюту: проблемы квалификации и законодательной регламентации // Журнал российского права. 2022. Т. 26. № 2. С. 71–87.
6. Русскевич Е. А., Дмитренко А. П., Кадников Н. Г. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации // Вестник Санкт-Петербургского университета. 2022. № 3. С. 585–598.
7. Хилюта В. В. Дематериализация предмета хищения и вопросы квалификации посягательств на виртуальное имущество // Журнал российского права. 2021. № 5. С. 68–82.
8. Хилюта В. В. Цифровые права как предмет хищения // Вестник Университета прокуратуры Российской Федерации. 2020. № 5 (79). С. 15–22.
9. Measuring digital development. ICT development 2023. URL: <https://www.itu.int/itu-d/reports/statistics/idi2023/>.

References

1. Arkhipov A. V. [Digital objects as a subject of theft]. *Ugolovnoe pravo* [Criminal law], 2020, no. 6, pp. 16–23. (in Russ.)
2. Dyuranske B. T., Keyn Sh. F. [Virtual worlds, real problems]. *Izvestiya vysshikh uchebnykh zavedeniy. Pravovedenie* [Proceedings of Higher Educational Institutions. Pravovedenie], 2013, no. 2 (307), pp. 115–134. (in Russ.)
3. Kapinus O. S. [Digitalization of crime and criminal law]. *Baikal Research Journal* [Baikal Research Journal], 2022, Vol. 13, no.1. (in Russ.)
4. Mochalkina I. S. *Cifrovye prava i cifrovaya valjuta kak predmet prestupenij v sfere jekonomiki: dis. ... kand. jurid. nauk* [Digital rights and digital currency as a subject of crimes in the field of economics. Author's abstract]. Moscow, 2022, 240 p.
5. Obrazhiev K. V. [Criminal encroachments on digital financial assets and digital currency: problems of qualification and legislative regulation]. *Zhurnal rossiyskogo prava* [Journal of Russian Law], 2022, no. 2, pp. 71–87. (in Russ.)
6. Russkevich E. A., Dmitrenko A. P., Kadnikov N. G. [Crisis and palingenesis (rebirth) of criminal law in the context of digitalization]. *Vestnik Sankt-Peterburgskogo universiteta. Pravo* [Vestnik of Saint Petersburg University. Law], 2022, no. 3, pp. 585–598. (in Russ.)
7. Khilyuta V. V. [Dematerializacija predmeta hishhenija i voprosy kvalifikacii posjagatel'stv na virtual'noe imushhestvo]. *Zhurnal rossiyskogo prava* [Journal of Russian Law], 2021, no. 5, pp. 68–82. (in Russ.)
8. Khilyuta V. V. [Cifrovye prava kak predmet hishhenija]. *Vestnik Uni-versiteta prokuratury Rossiyskoy Federatsii* [Bulletin of the University of the Prosecutor's Office of the Russian Federation], 2020, no. 5 (79), pp. 15–22. (in Russ.)

9. Measuring digital development. ICT development 2023. Available at: www.itu.int/itu-d/reports/statistics/idi2023/.

Информация об авторе

Ефремова Марина Александровна, доктор юридических наук, доцент, заведующий кафедрой уголовно-правовых дисциплин, Казанский филиал Российского государственного университета правосудия, г. Казань, Россия.

Information about the author

Marina A. Efremova, Doctor of Sciences (Law), Associate Professor, Head of the Department of Criminal Law Disciplines, Kazan Branch of the Russian State University of Justice, Kazan, Russia.

Поступила в редакцию 17 января 2024 г.

Received January 17, 2024.