
ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРАВА PROBLEMS OF INFORMATION LAW

Научная статья
УДК/UDC 343.97
DOI: 10.21779/2224-0241-2023-47-3-156-163

Использование IT-технологий при совершении преступлений – глобальная проблема государства

О.С. Поликарпова

Санкт-Петербургский университет МВД России, г. Санкт-Петербург, Российская Федерация,
zhuravlenok_os@mail.ru, <https://orcid.org/0000-0002-1324-6267>

Аннотация. В статье рассматривается проблема, порождаемая внедрением информационных и телекоммуникационных технологий в совершение общественно опасных деяний, как входящих в группу преступлений, отнесенных к компьютерной информации, так и выходящих за ее пределы, актуальность которой обусловлена стремительным ростом преступлений, совершаемых посредством применения информационных технологий и сети «Интернет». Отмечены принятые на государственном уровне нормативные правовые акты, направленные на защиту информации, регулирование отношений, связанных с выпуском и оборотом цифровых финансовых активов, внедренных в повседневную жизнь современного общества вследствие развития информационных технологий, в том числе обусловленные дополнением Уголовного закона Российской Федерации новыми квалифицированными признаками составов хищений, позволяющих расширить круг лиц, в действиях которых усматриваются признаки преступлений, совершаемых с применением таких технологий. Положительно отмечен и вклад научного сообщества в разработку пособий и рекомендаций, направленных на противостояние киберпреступности. По результатам исследования указано на необходимость внесения изменений в главу 14 Уголовно-процессуального кодекса Российской Федерации и разработку методических рекомендаций, направленных на разъяснение порядка наложения ареста на имущество, что может быть реализовано лишь в результате признания имуществом цифровых финансовых активов, включая криптовалюты.

Ключевые слова: информационные системы, IT-технологии, криптовалюта, цифровые финансовые активы, киберпреступность.

Для цитирования: Поликарпова О.С. Использование IT-технологий при совершении преступлений – глобальная проблема государства // Юридический вестник ДГУ. 2023. Т. 47, № 3 (67). С. 156–163. DOI: 10.21779/2224-0241-2023-47-3-156-163

Original article

The use of IT-technologies in the commission of crimes is a global problem of the state

Olga S. Polikarpova

St. Petersburg University of the Ministry of Internal Affairs of Russia, St. Petersburg, Russian Federation,
zhuravlenok_os@mail.ru, <https://orcid.org/0000-0002-1324-6267>

Abstract. The article deals with the problem generated by the introduction of information and telecommunication technologies in the commission of socially dangerous acts, both included in the group of crimes related to computer information and beyond its limits, the relevance of which is due to the rapid growth of crimes committed through the use of information technologies and the Internet. The adoption at the state level of normative legal acts aimed at protecting information, regulating relations related to the release and circulation of digital financial assets introduced into the daily life of modern society due to the development of information technology, including those caused by the addition of the Criminal Law of the Russian Federation with new qualified signs of theft, allowing to expand the circle of persons in the actions of which are signs of crimes committed with the use of such technologies. The contribution of the scientific community to the development of manuals and recommendations aimed at countering cybercrime was also positively noted. According to the results of the study, it is indicat-

ed that it is necessary to amend Chapter 14 of the Criminal Procedure Code of the Russian Federation and develop methodological recommendations aimed at clarifying the procedure for arresting property, which can be implemented only as a result of the recognition of digital financial assets, including cryptocurrencies, as property.

Key words: information systems, IT technologies, cryptocurrency, digital financial assets, cybercrime.

For citation: Polikarpova O.S. The use of IT-technologies in the commission of crimes is a global problem of the state. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2023, vol. 47, no. 3 (67), pp. 156–163. DOI: 10.21779/2224-0241-2023-47-3-156-163 (In Russ.).

Информационные и телекоммуникационные технологии применяются для хранения и распространения информации, в том числе посредством сети Интернет. В современном обществе, в условиях всеобщей информатизации и цифровизации, такие технологии получили наименование IT-технологии. Преступления, совершаемые с использованием вышеуказанных технологий, подразумевают неправомерный доступ к компьютерной информации, нарушение правил обработки или передачи такой информации, распространение вредоносных компьютерных программ, то есть в большинстве своем составляют деяния, подпадающие под признаки преступлений, включенных в главу 28 Уголовного кодекса Российской Федерации (далее – УК РФ), именуемую «Преступления в сфере компьютерной информации»¹.

Свое развитие преступления с использованием IT-технологий во многих развитых и развивающихся странах получили в начале 2000-х годов, что стало возможным в связи с повсеместным внедрением современных информационных технологий как в различные сферы трудовой деятельности, так и в повседневную жизнь каждого гражданина. Однако еще в 1996 году Б.В. Вехов исследовал способы совершения компьютерных преступлений и предлагал методику их расследования [2, с. 44], а в 1997 году Н.И. Шумилов, исследуя способы совершения информационных преступлений, обращал внимание на особенности организации их раскрытия и расследования, а также на прирост информационных преступлений в России до 10–15 % с 1985 года [8].

Вследствие того, что рассматриваемый вид преступлений получил международное распространение в ноябре 2001 года, в Будапеште была подписана Конвенция о преступности в сфере компьютерных технологий² (далее – Конвенция), предусматривающая как виды преступлений, со-

вершаемых с использованием компьютерных программ, данных и систем, так и обязательства подписавших ее государств принять законодательные меры, направленные на эффективное уголовное преследование лиц, причастных к совершению таких преступлений, и применение к ним соразмерных наказаний, предусматривающих, в том числе, денежные санкции и лишение свободы. Однако в России данная Конвенция не была ратифицирована.

Только в 2006 году в России, с целью защиты прав физических и юридических лиц в информационном пространстве, был принят Федеральный закон «Об информации, информационных технологиях и о защите информации»³, что позволило разработать и закрепить значимые для реализации такой защиты определения, принципы правового регулирования отношений, возникающих, в том числе, при использовании информационных технологий, а также обязанности и ответственность операторов информационных систем. Однако это не повлияло на снижение количества совершаемых в данной сфере преступлений, что побудило авторов Концепции развития законодательства РФ обратить внимание в процессе ее разработки на необходимость ратификации вышеуказанной Конвенции на период до 2012 года⁴ в целях повышения эффективности борьбы с преступлениями в сфере информационных технологий, особо акцентируя внимание на правовом регулировании вопросов онлайн-безопасности и ответственности за киберпреступления. Тем не менее, ратификации указанной Конвенции не последовало. Позднее на нормативную неурегулированность функционирования глобальной сети Интернет обратили внимание Ш.Б. Магомедов, А.Г. Саидов, Р.А. Абдусаламов и С.Н. Решетников [7, с. 28].

Исследованием способов предупреждения и расследования преступлений, совершаемых с использованием информационных технологий посвятили свои научные труды А.С. Егорышев, обративший внимание общественности на стремитель-

¹ Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (с изм. на 10.07.2023 г.) // Собр. Законодательства Российской Федерации. 17 июня. 1996. № 25, ст. 2954 (дата обращения 17.07.2023).

² Конвенция Совета Европы «О преступности в сфере компьютерных технологий» ETS № 185 от 23 ноября 2001 (с изм. от 28.01.2003). URL: <https://demo.garant.ru/#/basesearch/подписана%20Конвенция%20о%20преступно-сти%20в%20сфере%20компьютерных%20технологий/all:1> (далее по тексту рукописи – Конвенция).

³ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп. от 29.12.2022) // Российская газета. 2006. 29 июля. № 165.

⁴ Концепция развития законодательства РФ на период до 2012 года, утвержденная Торгово-промышленной палатой РФ в 2010 году. URL: <https://www.garant.ru/products/ipo/prime/doc/6636709/> (дата обращения: 07.07.2023).

ный рост преступлений, связанных с неправомерным доступом к компьютерной информации, которых в 2003 году было зарегистрировано 7053, и появление преступлений, направленных на распространение вредоносных компьютерных программ [5]. Ю.В. Гаврилин, указавший на стремительный повсеместный переход на финансовые расчеты с использованием информационных технологий, что явилось следствием появления нового вида общественно опасных деяний, совершаемых с использованием компьютерной информации и технологий, либо непосредственно направленных на такие технологии как на предмет преступления [3].

Наглядным примером служит создание в 2011 году двумя жителями г. Москвы одной из крупнейших в мире сетей по компрометации систем дистанционного банковского обслуживания, получившей название «Carberg». Лишь в марте 2012 года деятельность организованной преступной группы (далее – ОПГ) была пресечена благодаря проведенной межведомственной операции сотрудников МВД и ФСБ России, и в апреле 2014 года организаторы преступной группы были привлечены к уголовной ответственности с назначением наказания свыше 5 лет лишения свободы. Ущерб, причиненный действиями данной ОПГ гражданам и организациям, со счетов которых осуществлялось хищение денежных средств, составил свыше 150 млн. рублей¹. Но только в 2017 году в России был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»².

Вместе с тем, изощренность способов совершения преступлений с использованием IT-технологий продолжает нарастать, что способствует совершению многомиллионных хищений, в том числе посредством автоматического подключения заранее предустановленных вредоносных компьютерных программ в систему банковской сферы, подрывая ее стабильность, и больше того, ставит под угрозу безопасность общественной жизни, обороны и экономического развития всей страны. На масштабность таких угроз обратил внимание общественности Хуа Ли с приведением в своем научном труде статистических данных, насчитывающих на 2018 год более 4,3 млрд. кибератак на Россию. Хотя и значимость для «эффективного функционирования системы безопасности» положений Федерального закона № 187-ФЗ была положительно отмечена последним [9] и с его мнением

следует согласиться, поскольку с вступлением в силу данного Федерального закона прирост числа хакерских атак на объекты кредитно-финансовой сферы, здравоохранения, военные объекты и госструктуры не отмечен, их количество за 6 месяцев 2020 года составило более 1 млрд. случаев³, что существенно меньше показателей 2018 года. Но колоссальная опасность таких атак для общества и государства все же оставалась на очень высоком уровне, и уже к 2022 году был зафиксирован существенный прирост кибератак на компании и учреждения Российской Федерации, большинство из которых приводило к заражению вредоносным программным обеспечением, что по итогам 2022 года составило по сравнению с предшествующим годом практически двукратное увеличение событий, подрывающих информационную безопасность⁴.

Кроме того, заметим, что использование IT-технологий при совершении преступлений вышло далеко за пределы ограниченного круга преступлений, включенных в главу 28 УК РФ, и получило широкое распространение при совершении других видов общественно опасных деяний, что явилось следствием необходимости внесения изменений в УК РФ. Так, Федеральным законом № 111-ФЗ⁵ в 2018 году ч. 3 ст. 158 УК РФ была дополнена пунктом «г», относящим к предусматривающим уголовную ответственность деяниям тайное хищение, совершенное с банковского счета либо в отношении электронных денежных средств, а в ст. 159³ УК РФ формулировка «мошенничество с использованием платежных карт (поддельных либо принадлежащих другому лицу)» заменена более широким понятием «мошенничество с использованием электронных средств платежа», что позволило расширить круг деяний, отнесенных к общественно опасным.

Однако применение современных технологий не ограничилось составами хищений и преступлений в отношении компьютерной информации. Киберпреступления, разъяснения сущности которых проанализированы, систематизированы и аргументированы С.И. Буз [1], получили более ши-

¹ Официальный сайт Министерства внутренних дел Российской Федерации. URL: <https://мвд.рф/news/item/2155073/> (дата обращения 11.07.2023).

² Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. 2017. 31 июля. № 167.

³ Из интервью директора Департамента международной информационной безопасности МИД России Андрея Крутских журналу «Международная жизнь» от 29.06.2020. URL: <https://interaffairs.ru/news/show/26787> (дата обращения: 27.06.2023).

⁴ Отчет «Кибератаки на российские компании в 2022 году // Ростелеком Солар. Москва. 2023. [Электронный ресурс]. URL: <https://rt-solar.ru/upload/iblock/4a4/ghus61x9rd8cv5vczms5ig1svts4tlep/Otchet-o-kiberatakakh-na-rossiyskie-kompanii-v-2022-godu.pdf> (дата обращения: 21.07.2023).

⁵ Федеральный закон от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Российская газета. 2018. 25 апреля. № 88.

рокое распространение, обратившись в широко-масштабную проблему государства.

Примером совершения преступления, к сфере компьютерной информации и хищению отношения не имеющего, но тесно связанного с применением IT-технологий как при его организации, так и при финансировании, выступает ужасающее своей циничностью убийство, совершенное в октябре 2018 года в г. Москве, предусмотренное п.п. «ж, з» ч. 2 ст. 105 УК РФ, жертвой которого оказался старший следователь по особо важным делам следственной части следственного управления УМВД на транспорте по Центральному федеральному округу. В ходе организации указанного преступления доступные на сегодняшний день почти каждому гражданину технологии позволили извлечь из социальной сети «Facebook» фотографию будущей жертвы преступления и осуществлять непосредственное планирование преступления путем переписки заказчика с исполнителем в мессенджере «Telegram», с последующим виртуальным финансированием преступления. За подготовку и непосредственное убийство следователя организатор преступления расплатился с его исполнителем путем транзакции криптовалюты, в частности, bitcoins¹, на учетную запись последнего в сети «Интернет»².

А наибольшую распространенность применение IT-технологий получило при совершении незаконного распространения наркотических средств и психотропных веществ, поскольку за последние несколько лет способ совершения данного вида преступлений претерпел кардинальные изменения, существенно усложнившие порядок их раскрытия, установление причастных к совершению преступления лиц и процесс доказывания вины последних. Так, примером изложенного служит обвинительный приговор по делу № 1-778/2020³, согласно которому судом установлена вина Н.К.Г. в преступлениях, предусмотренных п.п. «а, б» ч. 3 ст. 228.1, п. «г» ч. 4 ст. 228.1 УК РФ, совершенных посредством незаконного приобретения с целью дальнейшего сбыта партии наркотического средства – производного N – метилэфедрона в значительном и крупном размерах и последующего сбыта через неустановленного оператора информационной системы в интернет-магазине «Pablo shop»,

предлагающем производить оплату приобретаемого наркотического средства в криптовалюте через электронный денежный обменник. Для последующего сообщения координат месторасположения тайников с предварительно заготовленной закладкой наркотического средства использовался мессенджер «Telegram», посредством которого информация направлялась оператору указанного интернет-магазина и далее перенаправлялась приобретателю запрещенного вещества. Такой способ совершения преступления позволил полностью исключить не только непосредственный контакт сбытчика с приобретателем наркотического средства, но и получение каких-либо данных друг о друге, что существенно затруднило процесс выявления совершенных эпизодов преступной деятельности и установления обстоятельств их совершения. И только заключение с обвиняемым досудебного соглашения о сотрудничестве по инициативе последнего позволило органам предварительного следствия установить детальную схему совершения вышеуказанных преступлений.

Подобный вид финансирования стал возможным именно ввиду развития IT-технологий, позволивших внедрить в оборот по всему миру виртуальные денежные средства, получившие общее наименование «криптовалюта», к основным из видов которой на сегодняшний день отнесены bitcoin и ethereum⁴, позволяющие избежать расчетов привычными нам денежными знаками в виде банкнот и монет.

В реалиях сложившейся в мире к 2020 году ситуации, связанной с бесконтрольным распространением криптовалют, с целью регулирования отношений, возникающих при обращении цифровых финансовых активов, а также защиты интересов физических и юридических лиц, имеющих отношение к обращению таких активов, в Российской Федерации был принят Федеральный закон № 259-ФЗ⁵, вступивший в силу с 1 января 2021 года, определяющий, в том числе, понятие цифровой валюты, порядок ее использования в качестве средства платежа и учета в информационных системах, зачастую осуществляющих функции финансовых бирж. И, что представляется наиболее важным для совершенствования способов раскрытия и расследования преступлений, связанных в той или иной степени с цифровыми финансовыми активами, ука-

¹ Bitcoins – децентрализованная цифровая криптовалюта, созданная в 2009 году. URL: <https://ru.wikipedia.org/wiki/Биткойн> (дата обращения 11.07.2023).

² Приговор Московского областного суда от 17.11.2020 в отношении А.А. Абдулазизова по делу № 2-34/2020. // Архив Московского областного суда, 2020.

³ Приговор Благовещенского городского суда Амурской области от 22.09.2020 г. в отношении Никифорова К.Г. по делу №1-778/2020. URL: <https://sudact.ru> (дата обращения 27.06.2023).

⁴ Ethereum – созданная и запущенная в 2015 году программистом В. Бутериным криптовалюта, эмиссия которой не ограничена. URL: <https://cryptonisation.com/ethereum-что-это-и-как-заработать/>

⁵ Федеральный закон от 31.07.2020 № 259-ФЗ (с изм. от 14.07.2022) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета 2020. 6 августа. № 173 (далее по тексту исследования, Федеральный закон № 259 -ФЗ).

занным Федеральным законом определено лицо, осуществляющее выпуск таких финансовых активов, выступающее в качестве оператора информационных систем, предназначенных для данного вида деятельности, порядок его регистрации в качестве такового, порядок учета пользователей информационной системы и предусмотрены требования, предъявляемые к зарегистрированным операторам информационных систем, в том числе включающие обязанность предоставления сведений о цифровых активах их обладателях на основании запросов уполномоченных сотрудников органов исполнительной власти, предварительного расследования либо на основании решения суда, в целях выявления, раскрытия и расследования преступлений, связанных в той или иной степени с цифровыми финансовыми активами.

Представляется, что положения Федерального закона № 259-ФЗ будут способствовать раскрытию преступлений, совершаемых с использованием IT-технологий, и позволят сократить период времени, затраченный на их расследование, в целях соблюдения принципа разумности сроков уголовного судопроизводства. Но для предотвращения столь широкого распространения и стремительного развития таких преступлений, сокращения процессуальных сроков недостаточно. Такой вывод следует из неутешительной статистики, насчитывающей за 2019 год 294, 4 тыс. рассматриваемого в статье вида преступлений¹. А за 2020 год, то есть включающий в себя основной период изоляции населения страны в связи с пандемией², число преступлений, совершенных с использованием информационно-телекоммуникационных технологий либо компьютерной информации существенно возросло и составило 510,4 тыс., что на 73,4% больше, чем за аналогичный период предшествующего года, из которых 300, 34 тыс. совершены посредством

сети Интернет и только 10 тыс. путем применения компьютерных программных средств³.

Столь стремительному росту количества преступлений, совершаемых с использованием IT-технологий и совершенствованию способов достижения преступного результата поспособствовала внезапно возникшая и стремительно распространявшаяся новая коронавирусная инфекция «COVID-19», позволившая злоумышленникам воспользоваться переходом значительной части населения как России, так и других стран на дистанционный формат осуществления трудовой деятельности, к отрицательным моментам которой следует отнести пренебрежение мерами безопасности при работе в сети Интернет, либо невозможностью их обеспечения на должном уровне ввиду удаленности от фактического места работы, где вопросами безопасности занимаются квалифицированные сотрудники организации, а равно повышение периода времяпрепровождения населения страны в «Интернет» – пространстве.

Только за январь 2021 года преступлений, совершаемых с применением IT-технологий зарегистрировано 37,2 тыс., что на 32,2 % больше, чем в январе 2020 года⁴ и лишь к концу 2021 года темпы роста такого вида преступлений замедлились, приведя в результате к незначительному приросту в сравнении с аналогичным периодом предшествующего года⁵. За весь период 2022 года снизилось количество хищений и криминальных деяний в сфере компьютерной информации в среднем на 26, 37 %, но увеличилось количество сбыта наркотических средств с использованием высоких информационных технологий на 20, 9 %⁶. И снова наблюдаем существенный прирост, зафиксированный по результатам I квартала 2023 года, ввиду чего официальными сведениями МВД России констатируется, что с использованием информационно-телекоммуникационных технологий совершается практически каждое третье преступление. Тем не менее следует отметить тот факт, что раскрывае-

¹ Статистические данные Генеральной прокуратуры Российской Федерации (Состояние преступности в России) за январь – декабрь 2019 года. URL: https://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf (дата обращения 17.07.2023).

² Указ Президента РФ от 25.03.2020 № 206 «Об объявлении в Российской Федерации нерабочих дней». URL: <http://www.kremlin.ru/events/president/news/63065> (дата обращения 11.07.2023); Указ Президента РФ от 02.04.2020 № 239 «О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19) // Российская газета. 2020. № 72(8126). 3 апреля; Указ Президента РФ от 28.04.2020 № 294 «О продлении действия мер по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19) // Собрание законодательства Российской Федерации. 2020. № 18, ст. 2875.

³ Официальный сайт МВД России «О состоянии преступности за январь–декабрь 2020 года». URL: <https://mvd.pf/reports/item/22678184/> (дата обращения 17.07.2023).

⁴ Официальный сайт МВД России «О состоянии преступности по итогам января 2021 года». URL: <https://mvd.pf/news/item/23238035/> (дата обращения 17.07.2023).

⁵ Официальный сайт МВД России «О состоянии преступности за январь–декабрь 2021 года». URL: <https://mvd.pf/reports/item/28021552/> (дата обращения 17.07.2023).

⁶ Официальный сайт МВД России «О состоянии преступности за январь–декабрь 2022 года». URL: <https://mvd.pf/reports/item/35396677/> (дата обращения 17.07.2023).

мость так называемых IT-преступлений возросла до 35,1 %¹.

Приведенная в статье динамика роста преступлений с применением IT-технологий требует от государства принятия мер, направленных на совершенствование способов их раскрытия и расследования.

На сегодняшний день наблюдается активность законодательных инициатив относительно разработки и принятия подзаконных и нормативных правовых актов, способных оказать влияние на снижение уровня преступности в сфере информационных технологий. К таковым, в том числе, относятся указы Президента «Об утверждении Доктрины информационной безопасности Российской Федерации»², «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»³, «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года»⁴, Приказ МВД России «Об утверждении Перечня должностных лиц органов внутренних дел Российской Федерации, правомочных получать у операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, на основании судебных решений, содержащуюся в записях информационной системы информацию о цифровых финансовых активах, принадлежащих их обладателю»⁵.

¹ Официальный сайт МВД России. Статистические сведения о состоянии преступности в январе-марте 2023 года. URL: <https://mvd.rf/news/item/37766256/> (дата обращения: 19.07.2023).

² Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 декабря 2016 года № 646 // Собр. законодательства РФ. 2016. № 50, ст. 7074.

³ О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 9 мая 2017 года №203 // Собр. законодательства РФ. 2017 № 20, ст. 2901.

⁴ Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 23 ноября 2020 г. № 733 // Собр. законодательства РФ. 2020. № 48, ст. 7710.

⁵ Приказ МВД России от 1 августа 2022 г. № 568 «Об утверждении Перечня должностных лиц органов внутренних дел Российской Федерации, правомочных получать у операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, на основании судебных решений содержащуюся в записях информационной системы информацию о цифровых финансовых активах, принадлежащих их обладателю» // Официальный интернет-портал правовой информации (pravo.gov.ru) 28 октября 2022 г. № 0001202210280025.

Вместе с тем, правоприменительной практике необходимы рекомендации по фактическому применению тех или иных нормативных правовых актов. В частности, Н.И. Долженко и И.А. Ярошук, исследуя возникающие при осуществлении расследования киберпреступлений сложности, указывают как на высокий уровень латентности таких преступлений и дистанционный способ их совершения, так и на дефицит в системе МВД России высококвалифицированных специалистов в сфере IT-технологий, чем обусловлена необходимость выработки эффективных методических рекомендаций в целях оптимизации раскрытия и расследования исследуемых в статье видов преступлений, а также подготовки квалифицированных кадров для правоохранительной системы России [4]. Аналогичной точки зрения придерживается и С.А. Нестерович, исследующий стоящие перед сотрудниками следственных органов проблемы расследования киберпреступлений [6]. И такие высказывания не остались без внимания. В данном направлении активизировались представители научного сообщества, предложив правоприменителям разработанные с учетом современных реалий учебные, практические пособия и методические рекомендации, раскрывающие способы установления владельцев криптокошельков, разъясняющие вопросы, связанные с механизмом использования криптовалют при совершении преступлений, выявлением и порядком документирования преступлений в сфере незаконного оборота наркотиков, совершенных с использованием новых информационных и финансовых технологий, а также использованием криптовалюты для финансирования преступлений либо осуществления расчетов за результат преступной деятельности и последующей легализации полученных преступным путем доходов, не все из которых общедоступны в связи с ограничением доступа к содержанию ряда практических пособий и рекомендаций ведомственной принадлежности, что оправдывается необходимостью успешного разрешения задач правоохранительных органов, направленных на борьбу с преступностью, и позволяет нам привести выходные данные только некоторых из них [10, 11, 12].

Однако считаем, что на сегодняшний день только разработки способов выявления и документирования вышеобозначенной преступной деятельности недостаточно. Назрела необходимость в детальной научной проработке вопроса, определяющего возможность и порядок наложения ареста на цифровые финансовые активы, принадлежащие лицам, подозреваемым (обвиняемым) в совершении общественно опасных деяний с применением информационных технологий, что должно повлечь за собой как внесение соответствующих дополнений в положения ст. 115 Уголовно-процессуального кодекса Российской Федерации, так и разработку соответствующих методических рекомендаций для последующего обеспечения воз-

возможности компенсации ущерба, причиненного потерпевшим в результате совершения хищений принадлежащих им денежных средств посредством применения IT-технологий и ущерба, причиненного вследствие удаленного использования вредоносных программ воздействия на компьютерные и мобильные сети, а в отношении преступлений, связанных с незаконным оборотом наркотических средств, данная мера, считаем, будет способствовать противостоянию государства с преступлениями против здоровья населения и общественной нравственности посредством наложения ареста и последующего обращения в доход государства в соответствии с положениями ст. 104¹ УК РФ дохода в виде цифровых финансовых активов, извле-

ченного от такого вида деятельности. Однако основным препятствием предложенного, как представляется, выступает отсутствие нормативно-правового акта, относящего цифровые финансовые активы, в том числе криптовалюты, как одного из видов таких активов, к имуществу, несмотря на то, что текст внесенного на рассмотрение Государственной Думы Российской Федерации еще в марте 2018 года законопроекта о цифровых финансовых активах, относил названные активы к имуществу в электронном виде, созданному с использованием криптографических средств¹, но уже к принятию Федерального закона № 259-ФЗ, данная формулировка была существенно скорректирована.

Список источников¹

1. Буз С. И. Киберпреступления: понятие, сущность и общая характеристика // Юрист-Правовед. 2019. № 4 (91). С. 78–82.
2. Вехов Б. В. Компьютерные преступления : Способы совершения, методика расследования / В. Б. Вехов; Ассоц. Рос. работников правоохранит. Органов. Москва : Право и закон, 1996. 179 с.
3. Гаврилин, Ю. В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы : дис. ... д-ра юрид. наук. Москва, 2009. 404 с.
4. Долженко Н. И., Ярошук И. А. Киберпреступность как одна из ключевых проблем современности. Правовая парадигма. 2020. Т. 19, № 1. С. 151–157.
5. Егорышев, А. С. Расследование и предупреждение неправомерного доступа к компьютерной информации : дис. ... канд. юрид. наук. Уфа, 2004. 230 с.
6. Нестерович С. А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и образования. 2018. № 8 (44). С. 46–49.
7. Магомедов Ш. Б., Саидов А. Г., Абдусаламов Р. А., Решетников С. Н. Обеспечение информационной безопасности Российской Федерации: конституционно-правовой аспект // Юридический вестник Дагестанского государственного университета. 2012. № 2. С. 25–28.
8. Шумилов Н. И. Криминалистические аспекты информационной безопасности : дис. ... канд. юрид. наук. СПб., 1997. 164 с.
9. Хуа Ли. Кибербезопасность в России в свете Доктрины информационной безопасности РФ 2016 года // Мир русскоговорящих стран - World of Russian-speaking countries : научный журнал. Ярославль : РИО ЯГПУ, 2019. № 2 (2). С. 13–22.
10. Земцова С. И., Галушин П. В., Карлов А. Л. и др. Криптовалюта в механизме совершения преступлений в сфере незаконного оборота наркотических средств и психотропных веществ : учебное пособие / Отчет о НИР от 28.10.2020. Министерство внутренних дел РФ. 2021.
11. Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учебное пособие. Москва : Академия управления МВД России, 2022. 76 с.
12. Документирование преступной деятельности лиц, причастных к легализации наркодоходов, в том числе с использованием интернет-бирж обмена криптовалюты: методические рекомендации // Академия управления МВД России. Москва, 2018. – URL: <https://мвд.рф/книги/научная-периодика/научные-работы-и-материалы-академии-упра/item/21375232/> (дата обращения 19.07.2023).

References

1. Buz S. I. Kiberprestupleniya: ponyatie, sushchnost' i obshchaya kharakteristika [Cybercrimes: concept, essence and general characteristics], *Yurist"-Pravoved"* [Jurist-Pravoved], 2019, no. 4 (91), pp. 78-82. (In Russ.)
2. Vekhov B. V. Komp'yuternye prestupleniya : Sposoby soversheniya, metodika rassledovaniya [Computer crimes: Methods of commission, methods of investigation], V. B. Vekhov; Assoc. of Russian law enforcement officers. Organs. Moscow : Pravo i zakon Publ., 1996, 179 p. (In Russ.).

¹ Законопроект № 419059-7 «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». URL: <https://sozd.duma.gov.ru/bill/419059-7> (дата обращения 10.07.2023).

3. Gavrilin Yu. V. Rassledovanie prestuplenii, posyagayushchikh na informatsionnyuyu bezopasnost' v sfere ekonomiki: teoreticheskie, organizatsionno-takticheskie i metodicheskie osnovy [Investigation of crimes encroaching on information security in the field of economics: theoretical, organizational, tactical and methodological foundations], Dr. Law. Sci. Dis. Moscow, 2009, 404 p. (In Russ.).
4. Dolzhenko, N. I., Yaroshchuk, I. A. Kiberprestupnost' kak odna iz klyuchevykh problem sovremennosti [Cybercrime as one of the key problems of our time]. *Pravovaya paradigma [The legal paradigm]*, 2020, vol. 19, no. 1, pp. 151-157. (In Russ.).
5. Egoryshev, A. S. Rassledovanie i preduprezhdenie nepravomernogo dostupa k komp'yuternoi informatsii [Investigation and prevention of unlawful access to computer information]: Cand. Law Sci. Dis. Ufa, 2004, 230 p. (In Russ.).
6. Nesterovich, S. A. Problemy rassledovaniya kiberprestuplenii, kotorye stoyat pered sotrudnikami sledstvennykh organov [Problems of investigation of cybercrimes faced by employees of investigative bodies], *Vestnik nauki i obrazovaniya [Bulletin of Science and Education]*, 2018, no. 8 (44), pp. 46-49. (In Russ.).
7. Magomedov, Sh. B., Saidov, A. G., Abdusalamov, R. A., Reshetnikov, S. N. Obespechenie informatsionnoi bezopasnosti Rossiiskoi Federatsii: konstitutsionno-pravovoi aspekt [Ensuring information security of the Russian Federation: constitutional and legal aspect], *Yuridicheskii vestnik Dagestanskogo gosudarstvennogo universiteta [Law Herald of Dagestan State University]*, 2012, no. 2, pp. 25-28. (In Russ.).
8. Shumilov, N. I. Kriminalisticheskie aspekty informatsionnoi bezopasnosti [Criminalistic aspects of information security]: Cand. Law Sci. Dis. St. Petersburg, 1997, 164 p. (In Russ.).
9. Hua, Li. Kiberbezopasnost' v Rossii v svete Doktriny informatsionnoi bezopasnosti RF 2016 goda [Cybersecurity in Russia in the light of the Information Security Doctrine of the Russian Federation in 2016], *Mir russkogovoryashchikh stran [World of Russian-speaking countries]: a scientific journal*, Yaroslavl : RIO YAGPU Publ., 2019, № 2 (2), pp. 13-22. (In Russ.).
10. Zemtsova S. I., Galushin P. V., Karlov A. L. et al. Kriptovalyuta v mekhanizme soversheniya prestuplenii v sfere nezakonno oborota narkoticheskikh sredstv i psikhotropnykh veshchestv [Cryptocurrency in the mechanism of committing crimes in the field of illicit trafficking of narcotic drugs and psychotropic substances] : textbook, Research report dated 28.10.2020. Ministry of Internal Affairs of the Russian Federation, 2021. (In Russ.).
11. Ustanovlenie vladel'tsev kriptovalyutnykh koshel'kov pri rassledovanii prestuplenii v sfere nezakonno oborota narkoticheskikh sredstv [Identification of owners of cryptocurrency wallets in the investigation of crimes in the field of illicit drug trafficking]: a textbook. Moscow : Academy of Management of the Ministry of Internal Affairs of Russia Publ., 2022, 76 p. (In Russ.).
12. Dokumentirovanie prestupnoi deyatel'nosti lits, prichastnykh k legalizatsii narkodokhodov, v tom chisle s ispol'zovaniem internet-birzh obmena kriptovalyuty [Documenting the criminal activities of persons involved in the legalization of drug proceeds, including using online cryptocurrency exchanges], Methodological recommendations, Academy of Management of the Ministry of Internal Affairs of Russia. Moscow, 2018. (In Russ.). Available at: <https://мвд.рф/книги/научная-периодика/научные-работы-и-материалы-академии-упра/item/21375232/> (accessed 19.07.2023).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Поликарпова Ольга Сергеевна, преподаватель кафедры административной деятельности органов внутренних дел Санкт-Петербургского университета МВД России, г. Санкт-Петербург, Российская Федерация. E-mail: zhuravlenok_os@mail.ru

INFORMATION ABOUT THE AUTHOR

Polikarpova Olga Sergeevna, Lecturer of the Department of Administrative Activity of Internal Affairs Bodies of the St. Petersburg University of the Ministry of Internal Affairs of Russia, St. Petersburg, Russian Federation. E-mail: zhuravlenok_os@mail.ru

Поступила в редакцию 24.07.2023 г.;
одобрена после рецензирования 25.08.2023 г.;
принята к публикации 01.09.2023 г.

Received 24.07.2023; approved after reviewing
25.08.2023; accepted for publication 01.09.2023