УДК 343.9
DOI: 10.26140/bgz3-2020-0902-0095

К ВОПРОСУ О ПОПУЛЯРНОСТИ КРИПТОВАЛЮТЫ В ПРЕСТУПНОЙ СРЕДЕ

Корчагин Анатолий Георгиевич, кандидат юридических наук, профессор, кафедра уголовно-правовых дисциплин
Владивостокский государственный университет экономики и сервиса
(690014, Россия, Владивосток, ул. Гоголя 41, e-mail: iakovenko.aa@students.dvfu.ru)
SPIN-код: 8003-0674
AuthorID: 1014170

Яковенко Андрей Александрович, ассистент, кафедра конкурентного и предпринимательского права,
Дальневосточный федеральный университет
(690091, Россия, Владивосток, ул. Суханова, 8, e-mail: iakovenko.aa@students.dvfu.ru)

Аннотация. В статье рассматривается феномен криптовалюты и технологии, на которой она основана. Описывается механизм её функционирования и возникающие проблемы правового характера, которые во взаимосвязи делают рассматриваемый феномен привлекательным в преступной среде. Глобальная цифровизация задает новые требования, в частности, сочетания юридических и технических регуляторов, без которых не получится добиться адекватного правового регулирования в цифровую эпоху. Предметом исследования является отечественная и зарубежная юридическая доктрина, раскрывающая сущность рассматриваемой технологии и механизмы защиты общественных отношений в процессе использования технологии. В работе используются следующие методы научного исследования: статистический; догматический; сравнительно-правовой; синергетический, а также логический, функциональный, системный. Новизна исследования обусловлена необходимостью сближения правовой и информационной системы и стремлением показать необходимость данного сближения в период стремительной цифровизации во всех сферах общества. Авторы приходят к выводу, что отсутствие правового регулирования и технические особенности делают новые цифровые решения особо привлекательными в преступной среде, что проблема носит комплексный характер и чем дольше не будут решаться вопросы правового регулирования, тем больше будут усугубляться риски использования криптовалюты.

Ключевые слова: цифровизация, интеграция, блокчейн, криптовалюта, правовое регулирование, преступность, даркнет, наркотики, хищение, отмывание.

ON THE QUESTION OF THE POPULARITY OF CRYPTOGRAPHIC CURRENCY IN THE CRIMINAL ENVIRONMENT

Korchagin Anatoly Georgiyevich, PhD in Law, Professor, Department of Criminal Law Disciplines
Vladivostok State University of Economics and Service
(690014, Russia, Vladivostok, 41 Gogol Street, e-mail: iakovenko.aa@students.dvfu.ru)
Yakovenko Andrey Alexandrovich, assistant, department of competition and business law
Far Eastern Federal University
(690091, Russia, Vladivostok, Sukhanov Street, 8, e-mail: iakovenko.aa@students.dvfu.ru)

Abstract. The phenomenon of cryptovolta and the technology on which it is based is considered in the article. The mechanism of its functioning and arising problems of legal character, which in interrelation make this phenomenon attractive in criminal environment, are described. Global digitalization sets new requirements, in particular, a combination of legal and technical regulators, without which it is impossible to achieve adequate legal regulation in the digital age. The subject of the study is the domestic and foreign legal doctrine revealing the essence of the technology in question and the mechanisms of protection of public relations in the process of technology use. In work the following methods of scientific research are used: statistical; dogmatic; comparative legal; synergetic, as well as logical, functional, system. The novelty of the research is caused by necessity of rapprochement of legal and information system and aspiration to show necessity of the given rapprochement during rapid digitalization in all spheres of a society. The authors come to the conclusion that the problem is complex and the longer the legal regulation issues are not solved, the more the risks of using cryptographic currency will be aggravated.

Keywords: digitalization, integration, blockchain, cryptocurrency, legal regulation, crime, darknet, drugs, theft, laundering.

ВВЕДЕНИЕ.

Более десяти лет назад в мире появился новый цифровой феномен, споры о юридической природе которого не утихают до сих пор. Речь идет о технологии блокчейн и криптовалютах.

Актуальность исследования обусловлена сложностью данных технологических решений, а цель необходимостью показать негативное проявление неспособности двух систем: цифровой и правовой к оперативной интеграции. Появление новых цифровых решений, направленных на улучшение качества жизни общества, начинает конкурировать с традиционными государственными институтами. Помимо такой конкуренции мы также наблюдаем неспособность создаваемых феноменов найти свое в место в существующей системе, следовательно, они практически не поддаются регулированию.

МЕТОДОЛОГИЯ.

Выбор методов предопределен поставленной целью исследования. В качестве методов исследования выбраны общенаучные и специальные методы: диалектический, системный, логический, формально-юридический и другие.

РЕЗУЛЬТАТЫ.

Отсутствие правового регулирования, является одним из факторов того, что полем активной преступной деятельности, все чаще становится виртуальное пространство.

На фоне этого, крайне важно учитывать основные черты, которые характеризуют «цифровую преступность» [1]. К ним относятся: 1) экстерриториальность - все больше компьютерных атак затрагивает одновременно две, три, десять и более стран. 2) виртуальность - физическую дистанцию от непосредственного потерпевшего, более того выступает значительным психоло-

гическим преимуществом правонарушителя. 3) гипертаргетированность - нацеленность сразу на многих потерпевших и способность вызывать целые цепи многоуровневых общественно опасных последствий. 4) мультипликативность - свойство компьютерной преступности, выражающееся в способности самовоспроизводства. 5) сверхизменчивость — появление новой IT-технологии на массовом рынке товаров или услуг практически незамедлительно оборачивается очередной «перезагрузкой» преступности. 6) системная латентность (гиперлатентность) — компьютерная преступность практически не поддается внятному количественному измерению. По оценкам специалистов, 85–97% компьютерных преступлений не обнаруживается [2].

Вышеперечисленное позволяет говорить о том, что мы являемся свидетелями активной трансформации рисков и угроз безопасности под влиянием новых информационно-коммуникационных технологий [3].

Технология блокчейн и основанная на ней криптовалюта является наглядным подтверждением сказанного. Полагаем, чтобы иметь более полное представление, к каким негативным последствиям приводит практически абсолютная несогласованность двух систем, стоит раскрыть механизм функционирования технологии блокчейн, на которой базируется криптовалюта и описать технологическую сущность самой криптовалюты.

Блокчейном, помимо самой технологии, называют непосредственную базу данных — тот самый «распределённый реестр». «Распределённый» означает, что у каждого участника хранится (и синхронизируется) полная копия базы или, как минимум, запись большого количества последних транзакций. Таким образом, блокчейн невозможно ликвидировать, отключив от сети отдельных участников: база сохранится у оставшихся. Хранение базы означает участие в системе и, соответственно, наличие уникального ключа, необходимого для адресации транзакций (адреса участника, или «кошелька»). Наличие или отсутствие какой-либо иной информации о пользователе в базе не влияет на работу системы – поэтому блокчейн может быть анонимным, то есть включать только адреса участников (их «кошельки»).

Объем базы криптовалюты биткойн – наиболее распространенной реализации технологии блокчейна – составляет около 180 Гб и постоянно растет. Децентрализованные базы данных неудобно использовать для непосредственного хранения файлов или объемных данных; это слишком дорого и в большинстве случаев неэффективно. Блокчейн эффективен не как доступное «облачное» хранилище данных, а как устойчивая и непротиворечивая история транзакций в сети, где ни один из участников не доверяет остальным [4].

База биткойна открыта для проверки: любой из участников может проверить транзакции, совершенные в ней другими участниками за любое время. Объем доступной информации может отличаться в разных блокчейнах, однако, чем более открыта сеть, более она защищена от взлома. В любом случае и в любой реализации блокчейна при совершении очередной транзакции проверяется ее возможность — например, имеется ли у участника достаточно криптовалюты для перевода. Таким образом исключается возникновение денежных средств из ниоткуда.

Блокчейн — совершенно новая технология, и, как и некоторые другие, направлен на технологическое решение ряда задач, которые ранее решало государственное регулирование. Проблема двойного расходования, идентификации владельца, исполнения смарт-контрактов – все они решаются технологическим, а не юридическим путем: действие становится невозможным в силу асимметричного шифрования и цепочки блоков, а не вследствие правового запрета и государственного надзора. Такой подход влечет меньше издержек, однако не учитывает пограничные ситуации и не обладает гибкостью, присущей правовому регулированию.

Блокчейн допускает трансграничный, глобальный обмен данными. Соответственно, для регулирования блокчейна актуальны те же проблемы, что и для регулирования глобальных сетей вообще – в первую очередь проблема экстерриториальности в трансграничных отношениях. Каждое государство имеет свой вектор движения в правовом регулировании информационных технологий, международное регулирование в этой сфере минимально. Отчасти регулирование криптовалют и блокчейна относится к валютному, финансовому законодательству и регулированию рынка ценных бумаг, который традиционно регулировался в рамках национальной юрисдикции. Единственная смежная сфера, в которой действует сильная международная кооперация (на базе ФАТФ) — это борьба с отмыванием денег, но на ее базе будет сложно достигнуть каких-либо международных соглашений по криптовалютам.

Таким образом, встает вопрос: а нужно ли вообще регулировать блокчейн и его реализации (криптовалюты) и почему, а также, к чему мы придем в случае отказа от регулирования или простого игнорирования данного вопроса?

Полагаем, что на поставленный вопрос можно ответить следующим образом.

Отсутствие регулирования. Регулятор будет наблюдать за (полагаем, что данная ситуация частично сложилась в правовой среде РФ) данным объектом; информировать о возможных негативных последствиях оборота криптовалюты (на примере РФ, различные информационные письма и подобного рода акты со стороны органов власти и Центробанка). При этом нет как законодательного запрета оборота данного феномена, так и норм, регулирующих оборот.

Положительные стороны – регулятор снимает с себя ответственность за риски, связанные с оборотом криптовалюты, связанные с высокой волатильностью.

Отрицательные стороны – невозможность мониторинга движения средств и контроля за операциями, а также идентификации в целях ПОД/ФТ. Рост числа мошеннических схем. Невозможность решения возникающих споров в правовом поле. Неконтролируемый рост оборота криптовалют.

Запрет регулирования. Полный запрет на обращение и использование криптовалют.

Положительные стороны – Угроза стабильности национальной валюты будет устранена; риски для потребителя минимизированы; сведены к минимуму риски, связанные с оттоком средств, отмыванием денег и финансированием терроризма.

Отрицательные стороны – увеличится теневой оборот криптоактивов; операции с криптовалютуой уйдет в другие юрисдикции; произойдет отток специалистов и предпринимателей связанных с блокчейн сферой в более благоприятные юрисдикции.

Регулирование. Регистрация (лицензирование) обменных площадок, идентификация пользователей в целях ПОД/ФТ, налогообложение участников оборота, предоставление отчетности по операциям площадками, требования к минимальному капиталу площадок, защита прав потребителей, ответственность за нарушение установленных требований.

Положительные стороны – статистика использовании криптовалют; контроль операций и идентификация в целях ПОД/ФТ; возможность введения ограничений на объемы и перечень операций; правовые способы защиты отношений в случаи нарушения прав сторон.

Отрицательные стороны - легализация криптовалют может повысить интерес граждан к вложениям в криптовалюты и потенциально увеличить риски потери ими средств; возможность использования недобросовестных и мошеннических схем и появления теневого оборота средств (в случае мер на уровне рекомендаций).

В правовом поле Российской Федерации можно наблюдать следующее: начиная с 2014 года начинается

период отрицания (неофициального запрета) и жесткой критики на уровне органов государственной власти, примером может послужить Письмо ЦБ РФ [5], более того на официальном портале общественных и экспертных обсуждений Regulation.gov.ru был выставлен текст законопроекта, подготовленный Минфином, который вносит изменения в КоАП РФ, а также в федеральные законы «о ЦБ РФ» (86-ФЗ) и «Об информации, информационных технологиях и о защите информации» (149-ФЗ), расширяющие толкование понятия денежных суррогатов и налагающие новые санкции за их выпуск/эмиссию, распространение, а также за информацию об этом, но после резкой волны критики в адрес опубликованного акта, страницу сайта поспешили удалить. Далее с перечня поручений президента [6] от 21.10.2017 г., в котором значится необходимость определения правового статуса новых цифровых технологий, начинается период, постепенной легализации.

25.01.18 г. появился известный проект «О цифровых финансовых активах» (далее — ФЗ об ЦФА), переживший несколько редакций: изначально под цифровыми финансовыми активами понималась криптовалюта и токен, которые отличались меж собой только эмитентом. Одним из главных недостатком проекта являлись положения о том, как токены на территории РФ нужно эмитировать: для этого следует получить разрешения (лицензии), а равно и использовать несколько площадок-посредников, то есть вся суть ICO/токенизации как таковой исчезла. Полагаем, единственными плюсами первоначальной редакции было выделение домашнего майнинга и промышленного (по потребляемой мощности: до 15 Квт и более) и введение термина «смарт-контракт» [7].

Необходимо отметить, что на конец 2018 года насчитывалось, примерно, 9 законопроектов, которые не могли обеспечить адекватного регулирования рынка криптовалюты.

Наконец, основным достижением стал Федеральный закон от 18.03.2019 N 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» [8], который закрепляет в Гражданском кодексе РФ понятие цифрового права.

Несмотря на то, что на сегодняшний день мы получили новый объект в виде цифровых прав, дальнейшее развитее регулирования криптовалюта получит только в Законе «О цифровых финансовых активах», принятие которого откладывали неоднократно, а также законе о краудфандинге.

В итоге, законопроекты, которые мы могли наблюдать продолжительное время, давали основания полагать, что создатели норм далеки от цифровой сферы. Частично сохраняющаяся на сегодняшний день правовая неопределенность является благоприятной средой для развития и укрепления рисков использования криптовалюты.

Самыми распространенными угрозами, связанными с оборотом криптовалюты, на сегодняшний день являются: незаконная продажа запрещенных товаров и услуг; отмывание преступных доходов; хищение криптовалюты и иные преступления против собственности.

Масштабы наркоторговли в Интернете с использованием криптовалюты продолжают увеличиваться примерно со скоростью 44 млн дол. в год [9]. Однако, полагаем, что данная цифра далека от объективности и связана это с тем, что на национальном уровне статистические данные разных источников, например, Касперского, МВД, Генпрокуратуры, различаются так как нет единого критерия оценки. Говоря о международном уровне, необходимо сказать, что здесь критериев так же нет, так как не совпадает система преступлений.

Купить запрещенные товары в сети становится все проще. Для этого через Tor браузер достаточно посетить определенный сайт, например, Hydra - крупнейшая российской торговой площадки по продаже наркотиков. При этом на сайте есть инструкции, как правильно создать криптокошелек и совершить оплату.

Государство неизбежно будет сталкиваться с проблемой технической возможности и законности своих действий по закрытию таких сайтов, до тех пор, пока данный вопрос не будет поставлен под международный контроль, как, например, банковские операции [10].

Вторым направлением использования криптовалюты в незаконных целях является отмывание преступных доходов. Причина, по которой криптовалюта популярна при отмывании преступных доходов это практически полное отсутствие правового регулирования.

Сегодня ни в России, ни в мире не ведется учет легализированных с использованием виртуальной валюты преступных доходов. Это, однако, не препятствует выявлению и анализу отдельных криминологических трендов.

На сегодняшний день, обналичить криптовалюту не так тяжело. Вот наиболее известные и надежные способы конвертации криптовалюты в фиатные деньги на территории СНГ.

Обменники. Выбирается надежный поставщик услуги с нужным направлением обмена, заполняется форма заявки и оплачивается. Преимущество обменников для обналичивания криптомонет: операции занимают несколько минут; среднее время исполнения поручения - 5-10 минут в зависимости от направления и скорости подтверждения операции в блокчейне; большое количество направлений - банки (Сбербанк, Тинькофф, АльфаБанк, Приват24 и другие), международные платежные системы Visa/Mastercard, электронные платежные системы (Qiwi, Яндекс, Пайер, Advcash, PerfectMoney, Капиталист). Недостатки: риск встретить мошенников, поэтому для обмена необходимо найти надежную биржу с достойной репутацией. Правила работы обменников регулируются «Пользовательским соглашением». Курс обмена устанавливается на определенное время, как правило, на 15 минут, в течение которых операция должна быть завершена в соответствии с инструкциями. В противном случае запрос может быть отменен или пересчитан по новому курсу. Для обналичивания пользователю понадобится только адрес электронной почты и номер кошелька или карты для получения денег. Большинство сервисов предлагают программу лояльности для постоянных клиентов.

Биржи криптовалют. Только самые популярные криптовалюты (Bitcoin, Ethereum, Litecoin, Ripple, Monero, Dash, Dogecoin, Zcash, Ethereum Classic) могут быть выведены через обменный пункт, в то время как биржи предлагают широкий спектр доступных криптоактивов для финансовых операций, включая токены ERC20. Биржи взимают небольшие торговые сборы, но они могут быть значительными при вводе или выводе фиатных денежных средств. Актуальная информация всегда представлена в разделах «Комиссии» (Fee). Однако, не все торговые платформы работают с фиатной валютой.

Электронные платежные системы (EPS): Advcash, Capitalist, Payeer, Epayments и другие. Такие сервисы предоставляют электронный кошелек в фиатной валюте. Он может быть пополнен с помощью криптовалюты, конвертация произойдет автоматически. После этого деньги можно вывести и обналичить доступными способами. Список решений большой: банковские карты и переводы, наличные, дебетовые карты и др.

Обмен с другими людьми. Как правило, такие люди находят друг друга на специализированных форумах, они договариваются об обмене и заключайте сделки. Таким образом, обналичивают криптовалюту и получают настоящие (фиат) деньги. Главное - не попасться мошеннику.

Также существуют нелегальные сервисы по конвертации криптовалюты. Самые большие объемы отмывае-

мых таким образом средств проходят через офшоры, где финансовый контроль за денежными потоками традиционно более слабый.

Новым и популярным способом легализации криминальных доходов является их отмывание через сайты азартных игр. Именно через эти сервисы отмывается около трех четвертей всех грязных виртуальных денег. Согласно данным Trend Micro, преступники все чаще стали использовать игровую валюту как способ сохранения стоимости криптовалюты. Для этого покупается валюта наиболее популярных виртуальных игр. Она продается за криптовалюту, а потом на специальных сервисах конвертации обменивается в фиатную валюту [9].

Третью группу преступлений с использованием криптовалюты составляют преступления, где виртуальная валюта является предметом преступного посягательства. В настоящее время в связи с отсутствием у криптовалюты правового статуса именно данная группа преступлений демонстрирует самые высокие показатели прироста. В первом квартале 2019 было похищено цифровых валют на сумму 356 млн долларов, в то время как убытки от незаконного присвоения средств составили 851 млн долларов, говорится в ежеквартальном отчете уважаемой американской компании CipherTrace [11,12]. Это объясняется рассмотренными выше технологическими особенностями.

Лица, похищающие криптовалюту, применяют следующие способы:

1. Фишинговые электронные кошельки. Поскольку никто не хочет вручную вводить длинные строки случайных буквенно-цифровых символов, которые также чувствительны к регистру, все используют функцию копирования / вставки, чтобы указать адреса, на которые пользователь отправляет криптовалюту. «Угонщики буфера обмена» (также известные как клиперы) являются вредоносными программами, которые обнаруживают использование буфера обмена для хранения адреса крипто-кошелька, а затем запускают сценарий, который заменяет правильный адрес на адрес злоумышленника. В результате чего, зачастую жертва не осознает, что произошло, цифровая валюта поступает на другой счет.

2. Создание фишинговых сайтов (или сайтов- копий) популярных ресурсов. Криптовалютные торговые платформы и биржи, по-видимому, являются областью криптосферы, наиболее уязвимой для хакерских атак, поскольку они являются кратчайшим путем к множеству централизованно хранимых цифровых активов.

3. Краудинвестинговые проекты. Развитие новой модели коллективного инвестирования (ICO, IPO и др.) привело к появлению мошеннических компаний, собирающих с потерпевших средства в криптовалюте, заведомо не имея цели заниматься предпринимательской деятельностью. По нашим данным, более трех четвертей всех организованных в 2017–2018 гг. краудфандинговых компаний являются мошенническими;

4. Создание инвестиционных фондов, работающих с использованием криптовалюты. Если учесть тот факт, что они создавались на фоне высокой волатильности криптовалюты и в условиях отсутствия правовых гарантий защиты вкладчиков, логично предположить, что более 40 % из них потенциально могут иметь криминальные цели. И, если принять во внимание, что в настоящее время криптовалюта не признается уголовно-правовой практикой объектом гражданских прав и, следовательно, предметом мошенничества, крайне сложно квалифицировать действия таких фондов как мошенничество [13].

Вышесказанное позволяет говорить о необходимости внесения изменений в механизм уголовно-правовой охраны. С учетом стремительной «цифровизации» общественных отношений отечественная юридическая доктрина отмечает дизруптивное воздействии информационно-коммуникационных технологий на механизм уголовно-правовой охраны (дизрупции уголовного права). Главной задачей для приспосабливания уголовно-парвового механизма к противодействию преступлениям «нового времени», является преодоление «нецифрового» видения уголовного права [1].

Проникновение кибернетических методов, а также инструментария цифровых технологий в механизм преступления приводит к необходимости переосмысления уголовного законодательства: а) необходимости определения оптимального количества составов преступлений направленных против информации и информационной безопасности; б) «оцифровка» классических составов, которые затрагивают информационные отношения; в) в тех случаях, где адаптация традиционных составов преступлений будет явно недостаточной или невозможной для эффективного противодействия современным криминальным угрозам в виртуальной среде, — разработка специальных норм.

Учитывая особенности технической стороны новых цифровых решений, потребуется единое международное регулирование, построенное на общих стандартах противодействия киберпреступности.

Международные достижения в сфере информационной безопасности уже сегодня требуют постоянного расширения правового сотрудничества в этой области, так как «вчерашние» достижения в этой сфере не дают основания говорить о наличии той международной правовой базы, которая может способствовать эффективному сотрудничеству в области информационной безопасности [10].

ЗАКЛЮЧЕНИЕ.

Таким образом, на основании вышеизложенного необходимо обозначить, что риски, связанные с оборотом криптовалюты, и причины, распространенного использования данных цифровых решений в преступной среде, носят комплексный характер. Именно техническая сложность порождает проблемы правового регулирования данного феномена. Отсутствие правового регулирования оборота будет только усугублять риски использования криптовалюты. Для криптопреступности характерно увеличение динамики, углубление специализации компаний и «опривычивание» криминального использования цифровой валюты. Несмотря на то, что основа в виде появления нового объекта права уже имеется, однако, законодателю предстоит еще большая работа: ввести требования об обязательной идентификации владельцев цифровых активов и иных лиц, участвующих в их обороте; установить режим конвертации цифровой криптовалюты в фиатную; введение уголовной и административной ответственности за нарушение стандартов оборота криптоинструментов; определение модели налогового администрирования криптовалюты; лицензирование профессиональной деятельности, связанной с созданием и оборотом новых цифровых активов.

СПИСОК ЛИТЕРАТУРЫ:

1. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения: монография / Москва: ИНФРА-М, 2019. 227 с.

2. Агапов П.В., Борисов С.В., Вагурин Д.В., Коренюк А.Л., Меркурьев В.В., Побегайло А.Э., Халиуллин А.И. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография. М., 2014. С. 35.

3. Кислый В. А. Юридические аспекты применения блокчейна и использования криптоактивов. // URL: https://goo.gl/tc2dZe.8. (дата обращения 18.01.2020 г.).

4. Булгаков И.Т. Правовые вопросы использования технологии блокчейн // Закон. 2016. No 12. С. 80–88.

5. Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн// Центральный банк Российской Федерации (Банк России) // https://www.cbr.ru/press/PR/?file=27012014_1825052.htm (дата обращения 18.01.2020 г.).

6. Перечень поручений по итогам совещания по вопросу использования цифровых технологий в финансовой сфере http://kremlin.ru/acts/assignments/orders/55899 (дата обращения 18.01.2020 г.).

7. О цифровых финансовых активах: Проект федерального закона // https://www.minfin.ru/ru/document/?id_4=121810-proekt_federalnogo_zakona_o_tsifrovykh_finansovykh_aktivakh# (дата обращения 18.01.2020 г.).

8. О внесении изменений в части первую, вторую и статью

1124 части третьей Гражданского кодекса Российской Федерации: Федеральный закон от 18.03.2019 N 34-ФЗ. // http://www.consultant.ru/document/cons_doc_LAW_320398/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100009. (дата обращения 18.01.2020 г.).

9. Сидоренко Э.Л. Наркопреступность в сети «Интернет»: современные криминологические тренды // Наркоконтроль. 2018. № 4. С. 13–18.

10. Мирзоев Б.Г. Киберпреступоность: угрозы безопасности информационного общества. // Современное право. 2006. № 1. С. 13-18.

11. Cryptocurrency thefts, fraud hit $1.2 billion in first quarter: report // https://www.reuters.com/article/us-crypto-currency-fraud/cryptocurrency-thefts-fraud-hit-1-2-billion-in-first-quarter-report-idUSKCN1S62P3.

12. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / А.П. Суходолов [и др.] // Всероссийский криминологический журнал. 2017. Т. 11, № 1. С. 13–21.

13. Иванцов С.В. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С.В. Иванцов, Э.Л. Сидоренко, Б.А. Спасенников, Ю.М. Берёзкин, Я.А. Суходолов // Всероссийский криминологический журнал. 2019. Т. 13, № 1. С. 85–93.

Статья поступила в редакцию 07.02.2020
Статья принята к публикации 27.05.2020