УДК 33

DOI: 10.34670/AR.2022.97.14.039

Проблемы уголовно-правового регулирования защиты цифровых финансовых активов

Цвик Янита Генриховна

Генеральный директор,
ООО «Каспея Групп»,
129090, Российская Федерация, Москва, Ботанический пер, 7;
e-mail: info@kaspeyagroup.ru

Аннотация

Развитие цифровой экономики не только открывает новые возможности для общества и государства, но и вооружает преступников новыми методами совершения правонарушений, создает дополнительные угрозы для многочисленных сфер общественного и общественной жизни. Информатизация кредитно-финансовой системы обусловила появление новых современных механизмов финансовых расчетов. При этом технические средства и методы, используемые в финансовой деятельности, постоянно совершенствуются. В условиях распространения пандемии в мировых масштабах был спровоцирован вынужденный переход на удаленный режим работы, что привело к увеличению количества уголовных правонарушений, совершенных с использованием передовых информационных технологий. Мошенничества с платежными картами, кражи денег с банковских счетов, распространение компьютерных вирусов, хищение хакерами персональных данных граждан, онлайн-торговля наркотиками, распространение противоправного контента – это лишь небольшая часть преступлений, которые должны расследовать и пресекать правоохранительные органы в современных условиях. Вместе с динамичным развитием информационных технологий и стремлением государства к сплошной цифровой трансформации всех сфер общественной жизни, цифровой прогресс обуславливает появление новых и совершенствование существующих инструментов для совершения уголовных правонарушений.

Для цитирования в научных исследованиях

Цвик Я.Г. Проблемы уголовно-правового регулирования защиты цифровых финансовых активов // Вопросы российского и международного права. 2022. Том 12. № 4А. С. 366-376. DOI: 10.34670/AR.2022.97.14.039

Ключевые слова

Рейдерство, криптовалюта, защита, регулирование, уголовное право.

Введение

Тотальная цифровизация общества имеет обратную сторону, негативным проявлением которой является появление новых криминальных рисков. Как свидетельствует статистика, разнообразные преступления, которые совершаются с использованием сети Интернет и других информационных технологий, имеют тенденцию к росту. В связи с появлением новых форм общественных отношений, которые проникают в виртуальную среду, актуальной и востребованной технологией для передачи информации в зашифрованном виде стала именно технология блокчейн, на основе которой функционирует система обращения криптовалют. Свидетельством того, что финансовые технологии вышли на мировом рынке на качественно новый уровень, является широкое распространение криптовалюты (виртуальной валюты), которая работает на основе децентрализованной системы блокчейн. Криптовалюты, которые освоили мир, изменили представление не только об условиях ведения бизнеса, но и частных финансов. Криптовалюта набирает популярность благодаря возможности расчета в виртуальном пространстве, поскольку не требуется их реальное выражение в виде денежных средств, ведь для таких расчетов используется только цифровой ключ, защищен криптографическим кодом, что надежно защищает криптовалютные транзакции анонимного характера [Климова, 2001]. Принцип функционирования блокчейн технологии сводится к тому, что все списки операций с криптовалютой объединяются в блоки, а блоки, в свою очередь, в цепи. При формировании цепей блоков через сетевые соединения децентрализованный сервер формирует базу данных, которая управляется автономно без единого центра. Технология блокчейн использует криптографию и цифровые подписи для удостоверения определенного лица: транзакции отслеживаются в криптографических идентификационных данных, которые теоретически анонимны, однако могут быть закреплены с реальными данными определенного пользователя.

Таким образом, функция блокчейн технологий заключается в регистрации каждой транзакции с криптовалютой. Любая передача криптовалюты подтверждается в сети внесением транзакционного блока с использованием процесса шифрования, что обеспечивает необходимую конфиденциальность и анонимность. Эта технология передачи и хранения данных стала объектом внимания преступников. Речь идет именно о криптовалюте, которая не является платежным средством в буквальном смысле, однако фактически стала суррогатом эмиссионных платежных средств. Схема работы криптовалют не регулируется какими-либо государственными органами или финансовыми учреждениями, а операции, которые происходят с криптовалютами не регламентированы международным законодательством, а потому идентифицировать их как преступные нельзя. Однако, при осуществлении противоправной деятельности в сети Интернет, криптовалюта выступает средством совершения преступления и используется в качестве платежного средства для приобретения огнестрельного оружия, наркотиков, легализации преступных доходов, финансирования терроризма и тому подобное. Преступники, используя криптовалюту, совершают немалые денежные переводы через сеть Интернет. Таким образом они игнорируют использование обычных финансовых систем, вызывая масштабные экономические убытки и посягая на основы национальной безопасности того или иного государства. Учитывая изложенное, актуальным и своевременным является рассмотрение особенностей использования возможностей технологии блокчейн в расследовании преступлений, совершенных в киберпространстве [Пушкарев, 2021].

Целью статьи является определение особенностей информационно-аналитического

обеспечения правоохранительной деятельности с использованием блокчейн-технологии, направленного на выявление фактов и попыток использования криптовалют в противоправной деятельности в сети Интернет.

Основное содержание

Впервые о рисках использования продуктов технологии блокчейн сообщил Европол еще в 2015 году. В его отчете проанализированы тренды обращения криптовалюты и использования новых финансовых инструментов в преступных целях. Было констатировано, что все чаще криптовалюта используется в сети теневого Интернета DarkNet (“Даркнет”) во время приобретения изъятых из оборота веществ и наркотических средств. В 2018 году Европол отчитался, что направления уголовного использования криптовалюты значительно увеличилось, а криптовалюта в основном используется как средство расчетов на теневых Интернет-рынках. В 2018 году рынок незаконной деятельности с биткоином составлял около \$76 млрд. США. В 2019-2020 годах наибольшее количество преступлений, совершенных с использованием криптовалют, касалось именно сферы сетевого мошенничества [Мельник, 2021].

Популярность нового финансового инструмента в криминальной среде объясняется тем, что на сегодня не разработаны юридические параметры криптовалюты и не установлены границы ее безопасного обращения. Это обусловлено неполным пониманием отечественных и международных экспертов важности исследования криптовалюты в рамках риск-ориентированного подхода, когда одновременно делается соотношение экономических рычагов и криминогенного потенциала криптоинструментов. Отсутствие комплексных исследований уголовного использования криптовалюты негативно влияет результативность работы в сфере предотвращения и профилактики такой преступной деятельности. Таким образом, своевременным и практически значимым является криминологический анализ криптопреступности как самостоятельного объекта научного познания и одновременно подсистемы криминологической модели интернет-преступности.

Под криптопреступностью следует понимать совокупность системных противоправных действий, совершаемых в отношении криптовалюты или с ее использованием. Поскольку это явление находится на стадии своего институционального становления, применение этого понятия является весьма условным. Можно выделить 3 сектора криптопреступности: незаконной продажи психоактивных веществ (наркотических и психотропных средств), других запрещенных товаров и услуг; отмывание преступных доходов с использованием криптовалюты; кража криптовалюты и другие преступления против собственности. В современных условиях за криптовалюту можно приобрести широкий спектр нелегальных товаров и услуг. Виртуальные деньги используются в сферах: незаконного оборота персональных данных; торговли поддельными документами. Иногда даже оплачиваются заказные убийства. Однако, наиболее распространенным сегментом криптопреступности остается именно незаконный оборот наркотических средств и психотропных веществ (80 % от общего объема рынка нелегальных товаров).

К сожалению, на сегодня мировая статистика криминального оборота наркотиков, порнографии, запрещенных услуг с использованием криптовалюты не ведется, однако, согласно данным экспертов же криптовалюта является средством расчетов в 95 % операций. При этом наблюдается принципиально новые криминологические тренды развития DarkNet: постепенная

спецификация отдельных уголовных сервисов и улучшения их технологических характеристик; постепенная монополизация криптовалютного рынка и тому подобное. Происходит тренд расширения спектра использования криптовалют для усовершенствования транзакций [Лаврова, 2021].

Если раньше абсолютным монополистом на криптовалютном рынке был Биткоин, то сейчас все чаще применяются новые цифровые валюты с высокой степенью анонимности (ZCash, Dash, Monero). Об этом указывает в своих отчетах Европол. Действительно, криптовалютные операции являются анонимными, поскольку адреса криптовалютных кошельков, как правило, не связаны с определенным лицом. Тем не менее, сама цепь транзакций, которая связана с определенным кошельком, не является анонимной. При необходимости, определенная цепь транзакций может быть проанализирована, в результате чего существует доля вероятности идентифицировать определенное лицо, которому принадлежит конкретный криптовалютный кошелек, по связям с другими адресами в цепи. В то же время существуют системы, которые позволяют сохранить криптовалютные транзакции конфиденциальными. Например, это сетевая система "Blender", которая доступна по адресу //blender.io. эта система предоставляет услугу сокрытия реальных адресатов криптовалютных кошельков, из которых были получены криптовалютные платежи. Это достигается тем, что сумма, которую необходимо "замаскировать", делится на части и отправляется на адреса криптовалютных кошельков, которые были созданы для клиента и не связаны с основным адресом криптовалютного кошелька, где денежные средства хранились сначала. Эта схема имеет целью запутать следы происхождения средств и ввести в заблуждение правоохранителей в случае расследования преступлений с криптовалютами и блокирование любых попыток определить реальную личность клиента. Система "Blender" имеет достаточное количество резерва криптовалютных средств, что позволяет клиенту получить свои средства с начала цепи блоков. Именно поэтому происхождение средств не будет отображаться. Например, сетевая система "Blender" не хранит информацию о обработанных транзакциях, поскольку вся история транзакций уничтожается без возможности ее будущего восстановления после того, как все криптовалютные средства отправлены на целевые адресаты криптовалютных кошельков.

По факту развития нелегального и преступного криптобизнеса формируется его направленность с одновременной специализацией лиц, привлекаемых к преступным схемам. Выделяются такие новые криминальные профессии, как: координаторы (администраторы одновременно несколько сервисов); "эксроу" (гаранты сделок); "гроверы" (лица, которые выращивают или комплектующие наркотические средства); "кладмены" (лица, которые размещают соответствующие объявления и рекламу); "дропы" (лица, которые принимают товар или осуществляют перевод криптовалют). Основная проблема использования криптовалюты в преступных целях заключается в имеющихся технических трудностях идентификации личности или группы лиц, осуществляющих криптовалютные операции противоправного характера. Преступная деятельность может быть направлена на: легализацию денежных средств, то есть сокрытие их происхождения; осуществление платежей с целью организации мошеннических схем, взлома информационных систем; финансирование терроризма и тому подобное [Троицкий, 2021].

Например, новым и популярным средством легализации криминальных доходов является их отмывание через сайты азартных игр. Именно через эти сервисы отмываются почти $\frac{3}{4}$ всех "грязных" виртуальных денег. Согласно данным "Trend Micro" преступники все чаще используют игровую валюту как средство хранения стоимости криптовалют. Для этого

приобретается валюта наиболее популярных виртуальных игр. Она продается за криптовалюту, а затем на специальных сервисах происходит ее конвертация в деньги. Существуют большие риски использования криптовалюты во время финансирования терроризма. Для большинства террористических организаций единственным способом остается физическая транспортировка наличных средств. Однако, учитывая расширение практики использования криптовалют и развития инфраструктуры транзакций, виртуальная валюта в будущем все чаще будет использоваться для финансирования терроризма [Мельник, 2021].

Еще одну группу преступлений, совершаемых с использованием криптовалюты, составляют преступления против собственности, когда криптовалюта является объектом посягательства. Лица, похищающие криптовалюту, используют фэйковые (поддельные) электронные кошельки. Потерпевшие, приобретая товар или услуги на популярных сервисах, перечисляют деньги на фишинговые кошельки, которые имеют другие адреса, через использование вирусных программ. Это может быть создание фишинговых сайтов популярных ресурсов. Использование криптовалюты мошенническим способом также практикуют краудинвестиционные проекты. Развитие новой модели коллективного инвестирования привело к появлению мошеннических компаний, которые собирают от потерпевших деньги в криптовалютах без намерения заниматься предпринимательской деятельностью.

В общем, во время расследования преступлений с использованием криптовалют правоохранительным органам необходимо иметь сведения о: условиях, порядке обращения криптовалют, особенностях осуществления транзакций, специфике функционирования криптовалютных бирж и тому подобное. Успешное расследование указанной категории преступлений также возможно только при наличии квалифицированных специалистов IT-сферы (информационно-коммуникационных технологий). Расследуя преступления, совершаемые с использованием криптовалюты, целесообразно учитывать тот факт, что эти преступления имеют свои специфические особенности. Однако существуют сложности по определению принадлежности определенного биткоин-адреса. Поэтому сотрудники правоохранительных органов ищут средства привязать определенный IP-адрес или адрес электронной почты к конкретному лицу [Пикуров, 2021].

Однако, если человек использует несколько IP-адресов, прокси-серверы, то этот процесс становится намного сложнее. Также, учитывая техническую специфику и особенности проведения криптовалютных операций, существование процедур возможного сокрытия происхождения криптовалютных активов, целесообразным видится развитие средств исследования следов деяния, разработки алгоритма установления и закрепления криминалистически значимых сведений для данного типа преступлений. Для достижения этого эффекта целесообразно провести гармонизацию права в этом направлении. Транзакции в сетях технологии блокчейн анонимны по отношению к пользователям, однако не являются анонимными в отношении самих транзакций. Поэтому технологии блокчейн с различными транзакциями должны быть подвергнуты основательному анализу, что позволяет эффективно противодействовать преступлениям, связанным с криптовалютами. Для проведения такого анализа необходимо иметь специальные знания и специальное программное обеспечение.

Например, таким программным обеспечением является “Crystal”, которое принадлежит голландскому предприятию – разработчику “Bitfury Group”. Это программное обеспечение способно обнаруживать и отслеживать незаконную деятельность в сетях технологии блокчейн, а именно: выявлять преступную и противоправную деятельность в системах блокчейну; предоставлять доказательства о заключенных подозрительных сделок на криптовалютных

биржах, отмечая при этом адреса кошельков, которые связаны с подозреваемым лицом; ускорять процесс расследования киберпреступлений (позволяет автоматизировано отслеживать наиболее подозрительных участников сети) и другие. Указанное предприятие предлагает свое программное решение, в первую очередь, для правоохранительных органов. Целесообразно указать, что "Crystal" не ограничивает свои возможности только по направлению анализа криптовалютной сети. Оно способно находить и структурировать информацию об адресах и содержательности сети из других источников, таких как форумы или другие интернет-порталы. Благодаря такому комплексному подходу "Crystal" может установить не только адрес определенного объекта, а также его реальное имя и другие реквизиты. Это программное обеспечение активно используется как правоохранительными органами, так и финансовыми организациями в США, ЕС и странах Азии [Серова, 2021].

Примером успешной работы этого программного обеспечения является борьба с вирусом "WannaCry", в результате чего были отслежены платежи от жертв вируса и установлена личность, которая требовала платежи. Существуют также и другие программные обеспечения, например, "Chainalysis", "CipherTrace", "CryptoFinance" и тому подобное. В основном задачи и функции данных программных средств похожи, но отличаются между собой алгоритмом анализа и порядком получения данных. Учитывая полученный опыт противодействия этих программ преступной деятельности, а также тот факт, что указанное программное обеспечение способно осуществлять комплексный анализ в криптовалютной сети, их практическое внедрение в правоохранительную деятельность невозможно недооценивать. Целесообразно указать, что в случае раскрытия преступления возникает закономерный вопрос ареста и в дальнейшем конфискации криптовалютных средств.

Однако, для решения этого вопроса правоохранители сталкиваются как с правовыми, так и техническими трудностями. На данный момент не существует единого общепринятого правового урегулирования этих вопросов, которое бы предусматривало порядок ареста или конфискации криптовалюты. Таким образом, не понятно как быть, когда встает вопрос об аресте или конфискации криптовалюты, если правоохранителям не известен частный цифровой ключ криптовалютного кошелька правонарушителя. Это возможно, если правонарушитель помнит и знает свой частный цифровой ключ, но разглашать его никто не имеет права. Поэтому если следствию известно, что конкретному лицу принадлежит криптовалютный кошелек, без содействия самого правонарушителя арест или конфискация невозможны по техническим причинам. В случае невозможности ареста или конфискации криптовалютных средств, адреса криптовалютных кошельков, которые используются в незаконной деятельности, возможно вносить в "черные" списки, как это делает Департамент казначейства США. С целью введения дальнейших санкций целесообразно было бы создать "черный" список криптовалютных кошельков пользователей [Иванов, Макаренко, Пушкарев, Русскевич, 2021].

Однако нередки случаи, когда криптовалютный кошелек привязан к определенной криптовалютной бирже. Тогда есть возможность обратиться с запросом к субъекту, который осуществляет обслуживание конкретной криптовалютной биржевой системы с требованием предоставить данные или осуществить арест или конфискацию, например, осуществить перевод средств правонарушителя на другой, созданный для ареста или конфискации криптовалютный кошелек. В то же время не все криптовалютные биржи публикуют свою контактную информацию, а также информацию о своем правовом статусе, что не дает возможности для такого обращения. Также не всегда определена юрисдикция таких предприятий. В результате, если правонарушитель оказывает содействие или другим способом возможно узнать о частный

цифровой ключ его криптовалютного кошелька, наиболее оптимальным является перевод преступных криптовалютных средств на другой кошелек с целью дальнейшего ареста или конфискации этих активов, поскольку оставлять их на текущем криптовалютном кошельке нельзя. Иначе, криптовалютные активы могут быть переведены на другие криптовалютные кошельки без ведома правоохранительных органов.

Масштабное использование криптовалют в незаконной деятельности – это комплексная международная проблема мирового сообщества, а не одного государства, поскольку криптовалютные операции осуществляются благодаря глобальной сети Интернет, которая не имеет территориальных и юрисдикционных границ. Однако, понимая риски и угрозы в указанном сегменте, некоторые государства мира активизируют свои усилия по направлению противодействия преступному использованию криптовалют. Так, в 2021 году Министерство юстиции США создало национальную команду по защите криптовалют (NCET) с целью проведения сложных расследований и судебного преследования преступных злоупотреблений с криптовалютой. В состав команды войдут специалисты из нескольких секторов Минюста США – отдела по борьбе с отмыванием денег и возвратом активов, а также отдела компьютерных преступлений и интеллектуальной собственности. Основная цель и задача деятельности этой команды – укрепить способность противодействовать структурам, которые процветают и получают прибыль благодаря злоупотреблениям с криптовалютными платформами. Эта группа должна не только расследовать сложные финансовые преступления, но и играть вспомогательную роль во время международных и федеральных расследований, а также во время расследований на уровне штатов. Также в 2021 году США впервые введены санкции против платформы для обмена криптовалюты, которая, как считается, способствовала проведению финансовых транзакций лиц, причастных к программ-вымогателей. Казначейство США ввело санкции против биржи SUEX с регистрацией в Москве и Праге, которая способствовала проведению финансовых транзакций лиц, причастных к программ-вымогателей. SUEX облегчала транзакции, связанные с незаконными доходами. Анализ известных транзакций SUEX демонстрирует, что более 40 % транзакций SUEX связано с незаконными субъектами. Биржи виртуальных валют, такие как SUEX, имеют решающее значение для прибыльности атак программ-вымогателей, которые помогают финансировать деятельность киберпреступников. По убеждению министра финансов США Джанет Йеллен, программы-вымогатели и кибератаки причиняют значительный ущерб малому и крупному бизнесу и представляют угрозу экономике страны.

К сожалению, мировым сообществом все еще не одобрен единый международно-правовой механизм, отсутствие которого приводит к проблемам определения юрисдикций влияния, например, сетевых криптовалютных обменных или биржевых систем. Сетевые криптовалютные обменные или биржевые системы, а также другие системы, которые предоставляют любые криптовалютные услуги, которые не афишируют на своих сайтах юридическую информацию, например, название, регистрационный номер предприятия, контактную информацию и прочее – это системы, которые преимущественно осуществляют свою деятельность незаконно, поскольку скрывают юридическую информацию о своей деятельности, либо вообще осуществляют свою хозяйственную деятельность без регистрации. Это определенным образом усложняет направление запросов от правоохранительных органов таких организаций. Возможно, такие не добропорядочные системы целесообразно блокировать или вносить их в специальные “черные” списки. Благодаря существованию разнообразных аналитических программ, которые способны проводить комплексные анализы криптовалютных сетей, увеличиваются возможности раскрытия уголовных преступлений, совершаемых с

использованием криптовалюты.

Поэтому тот факт, что адреса криптовалютных кошельков не связаны с конкретными лицами не означает, что преступления, в совершении которых используются криптовалюты не раскрываются. Напротив, современное программное обеспечение будет способствовать раскрытию правоохранителями не только фактов преступной деятельности, но и позволяет идентифицировать не только личность правонарушителя, но и отследить маршруты потоков незаконных криптовалютных средств. Однако требует ускорения разработка международно-правовых механизмов института ареста и конфискации незаконно полученных криптовалютных средств. Современные тенденции убедительно свидетельствуют о том, что транзакции в криптовалютных сетях не являются абсолютно анонимными, и могут находиться в фокусе внимания правоохранных органов, в частности путем организации проведения комплексного анализа благодаря специальному программному обеспечению и другим методам верификации [Шулепкина, 2021].

Технология блокчейн, на основе которой функционирует криптовалютная индустрия имеет следующие преимущества: 1) стабильность; 2) безопасность; 3) прозрачность работы с данными; 4) трансграничный характер операций по обмену данными. На этом фоне основной приоритет при использовании криптовалюты в преступной деятельности – это отсутствие привязки лица к определенному криптовалютному кошельку и увеличение количества кибератак по использованию программ-вымогателей. Одним из наиболее популярных средств обращения криптовалюты в преступных целях является функционирование криптовалютных бирж. В сети Интернет представлено немало криптовалютных обменных систем с неопределенной юрисдикцией. Вследствие этого существует вероятность, что эти сервисы могут использоваться в преступной деятельности. Целесообразно указать, что достаточно активно криптовалюты как расчетные средства используются в сети DarkNet, в которой данные передаются в зашифрованном виде. Также функционирует немало площадок-сайтов, на которых осуществляется незаконная деятельность. Например, только в 2019 году в скрытой сети функционировало более 2,5 тыс. магазинов наркотических и психотропных веществ, в которых расчеты происходили с помощью криптовалюты.

Поэтому важным направлением противодействия такому явлению остается использование современного программного обеспечения в правоохранных деятельности. С целью эффективности раскрытия преступлений, совершаемых с использованием криптовалют, целесообразным видится: ускорить принятие правовых основ, которые должны урегулировать криптовалюты и разработку методологических основ раскрытия и расследования этой категории уголовных правонарушений. Также правоохранным органам необходимо наладить концептуальное взаимодействие с криптовалютными компаниями с целью блокирования незаконной и противоправной деятельности в блокчейн платформах. Решение этой проблемы имеет комплексный характер и требует разработки стратегии, направленной на предотвращение использования преступниками новых современных финансовых механизмов.

Заключение

Среди приоритетных направлений развития международной уголовно-правовой политики в сфере предупреждения использования криптовалют в преступной деятельности выделяется: определение модели налогового администрирования криптовалюты и правового статуса криптовалют; обязательное лицензирование деятельности в сфере оборота криптовалют (биржевых сервисов, обменных площадок, компаний, которые выпускают токены);

установление международных стандартов по противодействию легализации преступных доходов и финансированию терроризма. Также целесообразно создать международную базу данных о лицах, которые занимаются незаконным оборотом и применением цифровых финансовых активов в контексте технологий, используемых в противоправной деятельности. Остро стоит вопрос о создании специального подразделения, к компетенции которого следует отнести проведение расследования противоправной деятельности с криптовалютами.

Библиография

1. Климова, Ю. Н. Криптовалюта как предмет преступного посягательства в преступлениях против собственности / Ю. Н. Климова, К. А. Лазарева // Вестник Владимирского юридического института. – 2021. – № 1(58). – С. 66-73. – EDN INWDGO.
2. Лаврова, О. Н. Особенности расследования преступлений, связанных с незаконным оборотом наркотических средств, совершенных с использованием криптовалюты / О. Н. Лаврова // Сборник научных статей по итогам Недели Российской науки в Рязанском филиале Московского университета МВД России имени В.Я. Кикотя, Рязань, 01–04 февраля 2021 года. – Рязань: Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 2021. – С. 297-300. – EDN BBLKQT.
3. Мельник, Л. Л. Классификация интернет-ресурсов, используемых при расследовании преступлений, совершенных посредством криптовалют и электронных денег / Л. Л. Мельник // Предварительное расследование. – 2021. – № 1(9). – С. 71-76. – EDN VXSVJU.
4. Мельник, Л. Л. Методика расследования преступлений, совершенных с использованием криптовалют и электронных денег: генезис, современное состояние, перспективы развития / Л. Л. Мельник // Юстиция Беларуси. – 2021. – № 4(229). – С. 43-47. – EDN NLYELN.
5. 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. – EDN FFFWVE.
6. Пушкарев, В. В. Преступления с использованием криптовалюты: актуальные вопросы уголовного преследования / В. В. Пушкарев, А. Ю. Терехов // Алтайский юридический вестник. – 2021. – № 1(33). – С. 122-127. – EDN SFJVLU.
7. Расследование преступлений, совершенных с использованием криптовалюты : Учебное пособие / Д. А. Иванов, М. М. Макаренко, В. В. Пушкарев, Е. А. Русскевич. – Москва : Ай Пи Ар Медиа, 2021. – 80 с. – ISBN 978-5-4497-1036-9. – EDN IXSVLY.
8. Серова, Е. Н. Криптовалюта как предмет преступлений в сфере экономики в российском и зарубежном уголовном праве / Е. Н. Серова, Л. В. Красущих // Проблемы права. – 2021. – № 1(80). – С. 83-87. – DOI 10.14529/prg-prava210116. – EDN WFGDRY.
9. Троицкий, А. А. Некоторые особенности раскрытия и расследования преступлений в сфере оборота криптовалют / А. А. Троицкий // Сборник научных статей по итогам Недели Российской науки в Рязанском филиале Московского университета МВД России имени В.Я. Кикотя, Рязань, 01–04 февраля 2021 года. – Рязань: Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 2021. – С. 786-790. – EDN KRNHJP.
10. Шулепкина, В. А. Криминологическая характеристика лиц, совершающих преступления с использованием криптовалюты / В. А. Шулепкина // Modern Science. – 2021. – № 3-1. – С. 213-216. – EDN VMFFIO.

Problems of criminal law regulation of protection of digital financial assets

Yanita G. Tsvik

General Director

LLC "Kaspea Group"

129090, 7, Botanic Lane, Moscow, Russian Federation;

e-mail: info@kaspeyagroup.ru

Abstract

The development of the digital economy not only opens up new opportunities for society and the state, but also equips criminals with new methods of committing offenses, creates additional threats to numerous spheres of public and public life. The informatization of the credit and financial system has led to the emergence of new modern financial settlement mechanisms. At the same time, the technical means and methods used in financial activities are constantly being improved. In the context of the spread of the pandemic on a global scale, a forced transition to remote operation was provoked, which led to an increase in the number of criminal offenses committed using advanced information technologies. Fraud with payment cards, theft of money from bank accounts, the spread of computer viruses, theft by hackers of personal data of citizens, online drug trafficking, distribution of illegal content are only a small part of the crimes that law enforcement agencies should investigate and stop in modern conditions. Together with the dynamic development of information technologies and the state's desire for a continuous digital transformation of all spheres of public life, digital progress leads to the emergence of new and improvement of existing tools for committing criminal offenses.

For citation

Tsvik Ya.G. (2022) Problemy ugovolno-pravovogo regulirovaniya zashchity tsifrovyykh finansovykh aktivov [Problems of criminal law regulation of protection of digital financial assets]. *Voprosy rossijskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 12 (4A), pp. 366-376. DOI: 10.34670/AR.2022.97.14.039

Keywords

Raiding, cryptocurrency, protection, regulation, criminal law.

References

1. Klimova, Ju. N. Kriptoaljuta kak predmet prestupnogo posjagatel'stva v prestuplenijah protiv sobstvennosti / Ju. N. Klimova, K. A. Lazareva // Vestnik Vladimirskogo juridicheskogo instituta. – 2021. – № 1(58). – S. 66-73. – EDN INWDGO.
2. Lavrova, O. N. Osobennosti rassledovaniya prestuplenij, svjazannyh s nezakonnym oborotom narkoticheskikh sredstv, sovershennyh s ispol'zovaniem kriptoaljut / O. N. Lavrova // Sbornik nauchnyh statej po itogam Nedeli Rossijskoj nauki v Rjazanskom filiale Moskovskogo universiteta MVD Rossii imeni V.Ja. Kikotja, Rjazan', 01–04 fevralja 2021 goda. – Rjazan': Rjazanskij filial Moskovskogo universiteta MVD Rossii imeni V.Ja. Kikotja, 2021. – S. 297-300. – EDN BBLKQT.
3. Mel'nik, L. L. Klassifikacija internet-resursov, ispol'zuemyh pri rassledovanii prestuplenij, sovershennyh posredstvom kriptoaljut i jelektronnyh deneg / L. L. Mel'nik // Predvaritel'noe rassledovanie. – 2021. – № 1(9). – S. 71-76. – EDN VXSVJU.
4. Mel'nik, L. L. Metodika rassledovaniya prestuplenij, sovershennyh s ispol'zovaniem kriptoaljut i jelektronnyh deneg: genezis, sovremennoe sostojanie, perspektivy razvitija / L. L. Mel'nik // Justicija Belarusi. – 2021. – № 4(229). – S. 43-47. – EDN NLYELN.
5. Pikurov, N. I. Problemy opredelenija juridicheskoi prirody kriptoaljut dlia kvalifikacii prestuplenij protiv sobstvennosti / N. I. Pikurov // Vestnik Universiteta prokuratury Rossijskoj Federacii. – 2021. – № 4(84). – S. 59-69. – EDN FFFWVE.
6. Pushkarev, V. V. Prestuplenija s ispol'zovaniem kriptoaljut: aktual'nye voprosy ugovolnogo presledovaniya / V. V. Pushkarev, A. Ju. Terehov // Altajskij juridicheskij vestnik. – 2021. – № 1(33). – S. 122-127. – EDN SFJVLU.
7. Rassledovanie prestuplenij, sovershennyh s ispol'zovaniem kriptoaljut : Uchebnoe posobie / D. A. Ivanov, M. M. Makarenko, V. V. Pushkarev, E. A. Ruskevich. – Moskva : Aj Pi Ar Media, 2021. – 80 s. – ISBN 978-5-4497-1036-9. – EDN IXSVLY.
8. Serova, E. N. Kriptoaljuta kak predmet prestuplenij v sfere jekonomiki v rossijskom i zarubezhnom ugovolnom prave / E. N. Serova, L. V. Krasuckih // Problemy prava. – 2021. – № 1(80). – S. 83-87. – DOI 10.14529/pro-prava210116. – EDN WFGDRY.
9. Troickij, A. A. Nekotorye osobennosti raskrytija i rassledovaniya prestuplenij v sfere oborota kriptoaljut / A. A. Troickij

// Sbornik nauchnyh statej po itogam Nedeli Rossijskoj nauki v Rjazanskom filiale Moskovskogo universiteta MVD Rossii imeni V.Ja. Kikotja, Rjazan', 01–04 fevralja 2021 goda. – Rjazan': Rjazanskij filial Moskovskogo universiteta MVD Rossii imeni V.Ja. Kikotja, 2021. – S. 786-790. – EDN KRNHJP.

10. Shulepkina, V. A. Kriminologičeskaja harakteristika lic, sovershajushhih prestuplenija s ispol'zovaniem kriptovaljuty / V. A. Shulepkina // Modern Science. – 2021. – № 3-1. – S. 213-216. – EDN VMFFIO.