Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра
экономики, финансового права и информационных технологий в деятельности органов внутренних дел

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: «Особенности выявления и расследования преступлений, совершенных с использованием криптовалюты»

Выполнил: Долгов Богдан Владиславович
40.05.01-ПОНБ 2014 г/н, группа 141
мл.лейтенант полиции

Руководитель:
Доцент кафедры экономики, финансового права и информационных технологий в деятельности ОВД, кандидат педагогических наук, полковник полиции
Турутина Елена Эдуардовна

Рецензент:
Начальник отдела дознания ОП № 5
«Московский» УМВД России по г. Казани
майор полиции
Абитова Алсу Мавлетовна

Дата защиты: « ___ » _____ 2019 г. Оценка _____

Казань 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТЫ	8
§ 1. Криптовалюта как предмет преступления	8
§ 2. Правовые и экономические аспекты использования криптовалюты	11
ГЛАВА 2. ВЫЯВЛЕНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ	23
§ 1. Динамика преступлений, совершаемых с использованием криптовалюты	23
§ 2. Особенности выявления преступлений, совершенных с использованием криптовалюты	28
ГЛАВА 3. ОРГАНИЗАЦИЯ И МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ	42
§ 1. Криминалистические особенности расследования преступлений с использованием криптовалют	42
§ 2. Особенности проведения оперативно-розыскных мероприятий при раскрытии преступлений, совершаемых с использованием криптовалюты	49
ЗАКЛЮЧЕНИЕ	59
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	62

ВВЕДЕНИЕ

Развитие компьютерных технологий и их совершенствование позволило им проникнуть практически во все виды деятельности человека, что, в свою очередь, привело к росту преступлений, совершённых с использованием компьютерной информации. Информационные ресурсы в сети «Интернет» хранят огромное количество информации, в том числе и персональной. Банки сделали доступной возможность управления свои финансами через онлайн-сервисы, да и банкоматы, через которые мы получаем зарплату, тоже являются компьютерами, подключёнными к сети. Иными словами, практически вся наша жизнь сейчас построена на зависимости от компьютеров и информации, которая на них хранится. Всё это, конечно, делает жизнь проще, экономит нам время, но также и побуждает к совершению преступлений, таких как кражи денег с банковских счетов, незаконное использование прав на определённую информацию (фотографии, финансовые документы, логотипы и т.п.). Также следует указать, что, получив доступ к вашей персональной информации, злоумышленник может воспользоваться ею в своих целях, в том числе корыстных. В последнее время хакеры, осуществляя неправомерный доступ к компьютерной информации, получают информацию о банковских счетах граждан, совершают кражу денег.

Прошедшие 2017-й и 2018-й годы характеризуются повышенным ажиотажем вокруг новомодных категорий «блокчейн», «криптовалюта», «ICO» и т.п. Этот массовый интерес был сформирован резким взлетом курса криптовалют по отношению к фиатным деньгам, особенно когда в декабре 2017 г. биткоин преодолел отметку в 20 000 долларов (высокий прирост показывали и иные альткоины). Последующая коррекция и падение курсов не охладили сформировавшийся интерес, а лишь подогревали его, подкрепляя рядом различных рассуждений, что после роста всегда идет коррекция, а затем опять рост.

Подавляющее большинство населения не в полной мере понимает принципы существования блокчейна, особенности функционирования криптовалют и т.д., но с восторгом воспринимает новости об очередном разбогатевшем студенте, который несколько лет назад, вложив в криптовалюту 10-20 долларов, благодаря росту курса стал миллионером. Естественно, каждый в глубине души желает повторить этот путь. При этом внимание общества привлекают как состоявшиеся криптовалюты (Bitcoin, Ethereum, Ripple, Litecoin, Dash, Nem и др.), так и только появляющиеся.

В данном контексте очевидно, что желание быстро разбогатеть фактически ничем не рискуя реализуется большинством граждан путем поиска «нового биткоина» или «нового эфириума», т.е. криптовалюты, только выходящей на биржу и стоящей очень дешево (не каждый может себе позволить пойти на риск и вложить крупные денежные суммы в тот же самый биткоин, который даже если и вырастет в два раза, то прибыль составит «лишь» 100%). Ожидание последующего роста на сотни, а то и на тысячи процентов именно новых криптовалют превалирует над рисками потерять вложенные инвестиции. Тем более что в случае с новыми альткоиномы эти инвестиции для одного отдельно взятого человека не так уж и велики (в этом – то и состоит главная цель таких инвесторов – получить прибыль, рискуя относительно небольшими денежными суммами). Понимая основы психологии толпы, работая на поддерживаемом, в том числе и средствами массовой информации, ажиотаже, в мире ежедневно появляются десятки новых криптовалют, которые активно предлагаются населению.

Президент России Владимир Путин на совещании, посвященном криптовалютам, указал использование криптовалют в гражданском обороте это возможность отмывания капиталов, полученных преступным путем, ухода от налогов и финансирование даже терроризма, ну и, конечно, распространение

мошеннических схем, жертвами которых, безусловно, могут стать рядовые граждане¹.

Отметим также, что денежные суррогаты более конкурентоспособны по сравнению с легальными деньгами, и это влечет их стремительное распространение. Курс только одной криптовалюты – так называемого биткоина – за последние два года вырос более чем на 1000%².

Степень разработанности темы исследования. В российской научной среде вопросы обращения криптовалюты Bitcoin, а также правовые проблемы использования цифровых финансовых (криптовалютных) технологий в контексте противодействия легализации доходов, полученных преступным путем, раскрыты в трудах Л.Н. Мамаевой, В.А. Лазаревой, К.С. Рыбаковой, М.В. Кирюхиной³, В.Д. Фетисова, Т.В. Фетисовой⁴, Д.С. Вахрушевой, О.С. Железовой, А.А. Уваровой, А.В. Рыбина⁵, Р.С. Анцерева⁶, У.Н. Миценко, Е.В. Тутинас⁷. В этих и ряде других научных исследованиях, как правило, освещены следующие основные аспекты:

¹ Путин: криптовалюты – это возможность отмывания, ухода от налогов и финансирования терроризма [Электронный ресурс] // Коммерсантъ. <https://www.kommersant.ru/doc/3435054> (дата обращения: 15.05.2019 г.).

² Козлова Н. Обман валют // Российская газета. – 2017. - № 6874 (6).

³ Мамаева Л.Н., Лазарева В.А., Рыбакова К.С., Кирюхина М.В. Безопасность финансовой системы в рамках появления криптовалюты // Экономическая безопасность и качество. – 2018. – № 1 (30). – С. 53-56.

⁴ Фетисов В.Д., Фетисова Т.В. Проблемы использования bitcoinа и экономическая безопасность России // Национальные интересы: приоритеты и безопасность. – 2018. – Т. 14. - № 3 (360). – С. 452-464.

⁵ Вахрушев Д.С., Железов О.С. Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления // Наукoведение. – 2014. – Вып. 5(24). – Режим доступа: <http://naukovedenie.ru/PDF/127EVN514.pdf/> (дата обращения: 15.05.2019 г.).

⁶ Анцеров Р.С. Регулирование криптовалют в современной информационной экономике / В сборнике: «Государство и рынок в условиях глобализации мирового экономического пространства». Сборник статей по итогам Международной научно-практической конференции. – 2018. – С. 11-14.

⁷ Миценко У.Н., Тутинас Е.В. Криптовалюта как потенциальная угроза финансовой безопасности Российской Федерации / В сборнике: «Стратегия развития российско-абхазских отношений в рамках построения межгосударственной программы национальной безопасности». Материалы международной научно-практической конференции. – 2017. – С. 247-250.

– характеристика Bitcoin (и других криптовалют), показаны его риски, а также политические установки в отношении использования и обращения криптовалют в сфере расчетов и платежей;

– основные характеристики и принципы создания и обращения Bitcoin (и других криптовалют), уделяется внимание угрозам экономической безопасности государств на примере подходов ведущих стран;

– особенности использования вычислительных возможностей электронно-вычислительных машин при решении логических задач в ходе их работы (что понимается сегодня под термином «майнинг», который происходит от англоязычного термина mining – «добыча»);

– централизованное создание криптовалют или валют определенной страны без прямого участия государственной власти, например, RS-coin в Великобритании, Augacoin в Исландии и др.

Объектом работы является криптовалюта как новое явление и средство совершения преступлений.

Предметом работы являются нормативные правовые акты, регламентирующие порядок расследования преступлений, совершаемых с использованием криптовалюты.

Цель настоящей работы: исследовать особенности выявления и расследования преступлений, совершенных с использованием криптовалюты.

Для достижения поставленной цели необходимо решение следующих задач:

– рассмотреть криптовалюту как предмет преступления;

– изучить правовые и экономические аспекты использования криптовалюты;

– охарактеризовать динамику преступлений, совершаемых с использованием крипто валюты;

– проанализировать особенности выявления преступлений, совершенных с использованием криптовалюты;

- охарактеризовать криминалистические особенности расследования преступлений с использованием криптовалют;
- исследовать особенности проведения оперативно-розыскных мероприятий при раскрытии преступлений, совершаемых с использованием криптовалюты;
- сделать выводы по проведенному исследованию.

Методологической основой исследования является система различных как общенаучных, так и частнонаучных методов: индукции, дедукции, аналогии, синтеза, сравнения, наблюдения, описания, систематизации, сравнительно-правовой, институциональный, системного анализа и другие.

Теоретическую основу исследования составили труды Г.З. Адигамова, Р.С. Анцеров, И.Т. Булгакова, В.Б. Верхов, М.Н. Дудина, В.Е. Козлова, Э.С. Маркаряна, В.С. Овчинского, В.А. Петрова, Э.Л. Сидоренко, Г.К. Синиова, К.К. Горяинова и других авторов, посвятивших свои работы данной проблематике.

Нормативную базу исследования составили Конституция Российской Федерации¹, Уголовный кодекс Российской Федерации², материалы судебной практики.

Структура работы обусловлена достижением поставленной цели и представляет собой введение, три главы, заключение, список использованной литературы.

¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ) // Российская газета. - № 237. – 25.12.1993.

² Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (принят ГД ФС РФ 24.05.1996 г.) (ред. от 17.06.2019 г.) // Собрание законодательства РФ. – 17.06.1996. - № 25. – Ст. 2954.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТЫ

§ 1. Криптовалюта как предмет преступления

На современном этапе развития новых технологий зарождаются всевозможные финансовые отношения. Среди таковых можно выделить электронные системы платежа, криптовалюту и современные программы потребительской лояльности, электронные кошельки и майнинговые фермы, которые являются ключевой составляющей технологии блокчейн. В российском праве до сих пор не решен вопрос о правовой природе данных явлений.

В условиях глобализации мировой экономики, стремительного развития электронной торговли и перехода на электронный документооборот преступные посягательства, связанные с оборотом так называемой криптовалюты, приобрели массовый характер. Они стали представлять существенную угрозу как на национальном, так и на международном уровнях.

Криптовалюта, или виртуальные денежные средства, – это электронные записи (титульные знаки) или электронные условные числовые единицы, которые используются участниками частных электронных платежных систем для взаимных расчетов. Иными словами, это частные (корпоративные) электронные деньги, эмиссия (оборот) которых не регламентируется национальным и международным законодательством, не контролируется государством или их объединением.

С точки зрения отечественного законодательства криптовалюта представляет собой компьютерную информацию, то есть «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» (примеч. 1 к ст. 272 «Неправомерный доступ к компьютерной информации» Уголовного кодекса РФ).

Среди электронных систем платежа биткоин – самая известная криптовалюта, получившая широкое развитие во всем мире. Механизм функционирования данной электронной валюты следующий: существует максимальный лимит в двадцать один миллион, за пределы которого компьютерная система не должна выходить. Участники этой системы ищут биткоины с помощью своих компьютеров. Система устроена так, что участники запускают алгоритм на своих компьютерах, который должен найти правильный код. Те лица, которые нашли данный код, получают определенное количество биткоинов.

Биткоин использует блокчейн для транзакций абсолютно любого типа, его систему можно сравнить и с другими электронными кошельками, например, с уже известной системой Qivi.

Можно заметить, что государство видит в существовании криптовалют потенциальную угрозу национальной платежной системе и общественной безопасности. Эта позиция не раз отражалась в разъяснениях Министерства финансов РФ по вопросу правовой природы криптовалют.

Опасность криптовалюты оценивается многими учеными, в том числе это получило свое отражение в докладе полицейской службы ЕС «Оценка Угрозы Организованных Интернет-Преступлений (iОСТА)» оценивающий биткоин как ключ к совершению преступлений в сети Интернет и прямой вызов всем правоохранительным органам¹. На территории РФ, согласно позиции ЦБ РФ и Генеральной Прокуратуры, биткоин оценивается как удобный инструмент для отмывания денег и финансирования терроризма. Министерством финансов был подготовлен законопроект «О внесении изменений в Федеральный закон «О Центральном банке Российской Федерации (Банке России)» и отдельные законодательные акты Российской Федерации», которые анализировали

¹ Оценка Угрозы Организованных Интернет-Преступлений (iОСТА) [Электронный ресурс] Режим доступа: <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta> (дата обращения: 15.05.2019 г.)

криптовалюты и возможность их использования на территории РФ и предусматривающий полный запрет использования криптовалют в РФ. В целом, это правильная позиция, но следует рассмотреть более развернуто на использование биткоина в качестве инструмента отмывания денег.

В настоящее время в законодательстве не решен вопрос о содержании понятия «денежный суррогат». О.М. Крылова полагает, что денежные суррогаты являются объектами, которые способны одновременно выполнять все или часть функций валюты Российской Федерации¹. Наряду с этим существует и другая точка зрения, приверженцы которой полагают, что «денежный суррогат» – это платежное средство, не отвечающее признакам законного платежного средства и не являющееся специальным законным платежным средством, выпуск в обращение которого запрещен государством и наказуем в соответствии с законодательством.

Обратимся к первой точке зрения на правовую природу денежного суррогата. Если обратиться к Федеральному закону «О Центральном банке Российской Федерации (Банке России)»², то можно судить о том, что автор, называя денежные суррогаты законным платежным средством, делает ошибочный вывод, так как в указанном Федеральном законе четко сказано о запрещенности денежного суррогата на территории Российской Федерации³. Следовательно, действия с денежными суррогатами должны быть наказуемы. Вопрос о том, должна ли это быть именно уголовная ответственность, до сих пор законодательно не решен.

Актуальность биткоина растет, на данный момент существуют такие примеры, как покупка реальных объектов, которые оплачиваются биткоином. Но

¹ Крылов О.М. Правовое регулирование денежного обращения в Российской Федерации. – М.: Контракт, 2014. – С. 102.

² О Центральном банке Российской Федерации (Банке России): Федеральный закон Российской Федерации от 10 июля 2002 г. № 86-ФЗ (в ред. от 6 июня 2019 г.) // Собрание законодательства РФ. – 15.07.2002. - № 28. – Ст. 2790.

³ Сухаренко А. Суррогаты вредные? // Юрист. – 2015. - № 41. – С. 21.

будет ли такая сделка являться мошенничеством, поскольку биткоин не является официально признанным платежным средством в Российской Федерации?

Исходя из всего вышесказанного, стоит либо уточнить понятие «денежного суррогата» как средства виртуального взаиморасчета между экономическими субъектами, не обеспеченного реальной стоимостью, что позволяет посчитать криптовалюту таковым, либо вообще запретить оборот криптовалют, введя в уголовное законодательство соответствующий запрет.

§ 2. Правовые и экономические аспекты использования криптовалюты

По данным «Coin Market Cap» сегодня в мире существует 699 видов криптовалют, их суммарная рыночная капитализация увеличилась на 53% с начала 2017 г., с 17,7 до 27,144 млрд. долл. США при том, что в январе 2016 г. составляла 6 млрд. долл. США¹. Среди наиболее популярных криптовалют в мире лидерами роста стали Bitcoin, Ethereum, DASH, Monero и NEM – им принадлежит 91% суммарной капитализации². Ряд мировых, геополитических, государственных, региональных кризисов, негативные последствия глобализации побуждают как физических лиц, так и предпринимателей искать альтернативные средства сохранения и приумножения средств. Современный отечественный потребитель особенно остро нуждается в оперативности, безопасности расчетов, защищенности, отсутствии третьих сторон, независимости ценности денежной единицы от политической ситуации в стране, и криптовалюты удовлетворяют эти потребности³.

¹ Рынок криптовалют вырос в полтора раза с начала 2017 года. – [Электронный ресурс] – Режим доступа: <http://forklog.com/rynok-kriptoalyut-vyros-v-poltora-raza-s-nachala-2017-goda>.

² Режим доступа: <http://coinmarketcap.com> (дата обращения: 15.05.2019 г.)

³ Лясников Н.В., Дудин М.Н // Менеджмент в XXI веке: сущность, проблемы и задачи // Путеводитель предпринимателя. – 2010. - № 8. – С. 83-92; Юрьева А.А. Развитие информационного общества как условие формирования инновационной экономики // Проблемы рыночной экономики. – 2016. - № 3. – С. 14-20.

Проведем анализ нормативно-правовых и институциональных аспектов, связанных с регулированием сферы цифровых финансовых технологий (в целом) и сферы расчетов / платежей с использованием ряда криптовалют (в частности, Bitcoin).

В связи с оборотом и созданием криптовалют возникает вопрос о ее правовом регулировании на национальном и на международном уровнях. Здесь возникают немало препятствий, которые необходимо в будущем преодолеть. Очевидным из них является то, что многие люди не знают и не представляют о возможном существовании криптовалюты. Следующей дилеммой является недостаточное обсуждение и отсутствие проработки сущности Bitcoin (и других криптовалют) и его аналогов со стороны государственных органов при принятии законов или других нормативных актов. Специфическая природа криптовалюты обуславливает то, что соответствующий вопрос не является первоочередным для решения. Но все-таки сейчас мировые тенденции и реалии заставляют менять свое отношение к этой проблеме. Наиболее острой проблемой становится реализация механизма обращения криптовалюты в законодательстве.

Криптовалюта – это особое электронное платежное средство, курс которого поддерживается только спросом и предложением. Такие электронные деньги не регулируются ни одной из государственных систем, в том числе Банком России. Функция наблюдателей и контролеров в этом случае лежит на пользователях сети и держателям криптовалют. Годом зарождения криптовалют принято считать 2009 г., когда лицо или объединение лиц под псевдонимом Сатоши Накамото основала свою платежную систему Bitcoin. Она использовала метод защиты Proof-of-work и имела открытый исходный код, который был использован для создания разнообразных версий (разнообразные форки) для платежных систем типа Bitcoin (в переводе с английского fork – это вилка). Форки – это те платежные системы, которые построены на базе алгоритма Bitcoin, и в основном являются его копиями, но имеют некоторые особенности,

дающие им преимущество перед Bitcoin (например, скорость обработки запроса, комиссия, максимальный порог эмиссии). Некоторые форки были созданы со спекулятивной целью и особого распространения не получили. При этом следует отметить, что Bitcoin по сути, не был революционным изобретением, а идея использования криптовалюты берет свои истоки из 90-х годов.

Основным мотивационным фактором создания криптовалют было не столько обогащение или слава его основателей, сколько обеспечение анонимности платежной системы и создание альтернативы современной финансовой системе, к которой доверие постепенно теряется. Особенности криптовалют, которые отличают их от обычной валюты является их децентрализация, то есть отсутствие регулятивного органа, который бы регулировал криптовалюту и способ ее эмиссии. Эмиссия криптовалюты имеет название «майнинг» и заключается в использовании мощностей компьютерных систем для генерации уникальных наборов символов, которые образуют криптовалюту.

Отсутствие какого-либо обеспечения, кроме доверия владельцев криптовалют, делает их высокоспекулятивным инструментом, так как в стоимость заложены только вычислительные мощности, которые используются для нужд функционирования киберсистемы и создания этих денег¹. Bitcoin – одноранговая платежная система или первая в мире криптовалюта (в зависимости от контекста)². В 2016 г. венчурные инвестиции в Bitcoin и блокчейн составили \$550 млн³, по сравнению с 2013 г. произошел рост более, чем в 5 раз. Капитализация Bitcoin в 2017 г. составила \$16,9 млрд. При этом следует

¹ Степанова Д.И., Николаева Т.Е., Иволгина Н.В. Особенности организации и направления развития криптовалютных платежных систем // Финансы и кредит. – 2016. - № 10 (682). – С. 38.

² Правовое регулирование криптовалютного бизнеса [Электронный ресурс]. – Режим доступа: <http://axon.partners/wp-content/uploads/2017/02/Global-Issues-of-Bitcoin-BusinessesRegulation.pdf> (дата обращения: 15.05.2019 г.)

³ Гурьева М. Блокчейн-экономика: тренды и перспективы [Электронный ресурс]. – Режим доступа: <https://te-st.ru/wp-content/uploads/2017/04/Marina-Gureva.pdf>. (дата обращения: 15.05.2019 г.)

отметить, что государственная исполнительная и законодательная власть отдельных стран, начиная с 2010-х годов, ведет активный мониторинг рынка криптовалют (в частности, Bitcoin и других), а также ищет оптимальные подходы к нормативно-правовому регулированию цифровой финансовой сферы.

Так, например, в 2014 году Банком Англии в ежеквартальном отчете впервые была опубликована статья «Экономика цифровых валют», авторами которой выступали представители Банка Англии. В отчете указано, что «самым большим гипотетическим риском для кредитноденежной системы от цифровых валют может стать «Bitcoinизация» экономики». При этом под «Bitcoinизацией» подразумевается применение криптовалюты как основной платежной единицы. Мы согласны с мнением М.Н. Дудинга и Н.В. Лясникова, что это должно существенно усложнить как способы государственного контроля ценообразования, так и государственное регулирование экономики другими методами¹. Хотя «Bitcoinизация» экономики считается маловероятной, использование Bitcoin на одном уровне с фунтом стерлингов – возможно. В феврале 2015 года было заявлено о банкротстве гонконгской Bitcoin-биржи, инвесторы которой понесли убытки в размере 387 миллионов долларов. Тогда же было заявлено, что, учитывая спекулятивную природу Bitcoin, нужно с особой осторожностью подходить к совершению криптовалютных операций².

Канада находится на втором месте в мире после США по числу установленных Bitcoin-банкоматов. Канадское правительство для лучшего понимания технологии Block Chain осуществляет разработку цифровой версии канадского доллара. Функционирование криптовалютных бирж было узаконено еще в 2014 году, когда генерал-губернатор Канады одобрил соответствующий законопроект. По данному законопроекту криптовалютные биржи подлежат

¹ См.: Дудин М.Н., Лясников Н.В. Использование криптовалюты в незаконных целях: обеспечение финансово-экономической безопасности // Проблемы рыночной экономики. – 2018. - № 3. – С. 16-23.

² Там же.

регистрации в Канадском центре анализа финансовых операций и отчетности (Financial Transactions and Reports Analysis Centre of Canada, далее – «FINTRAC») и обязаны соблюдать законодательство в сфере противодействия легализации (отмыванию) доходов. В других сферах деятельность бирж не урегулирована. Денежные платежи с помощью цифровых денег подлежат налогообложению как бартерные сделки. Помимо этого, при продаже криптовалюты осуществляется сбор подоходного налога (Income Tax), налога на прибыль (Corporation Income Tax) налога на прирост капитала (Capital Gains Tax)¹.

В январе 2014 года пресс-служба Банка России опубликовала информацию «Об использовании при совершении сделок «виртуальных валют», в частности, Bitcoin». В документе отмечено, что «предоставление юридическими лицами услуг по обмену цифровой валюты на рубли и иностранную валюту, а также на товары (работы, услуги) будет рассматриваться как потенциальная вовлеченность в осуществление сомнительных операций в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». В данном заявлении криптовалюта, по сути, была приравнена к денежным суррогатам, хотя прямого указания на это в нем не содержится².

В мае 2014 г. ФРС и Федеральный консультативный совет назвали Bitcoin угрозой для банковской системы, экономической деятельности и финансовой стабильности; Счетная палата США призывает обратить внимание на защиту прав потребителей, которые используют криптовалюту. Среди противников запрета на ограничение криптовалют можно назвать Президента Сбербанка РФ Германа Грефа. В июле 2014 г. на Международном банковском конгрессе первый

¹ Правовое регулирование криптовалютного бизнеса [Электронный ресурс]. – Режим доступа: <http://axon.partners/wp-content/uploads/2017/02/Global-Issues-of-Bitcoin-BusinessesRegulation.pdf> (дата обращения: 15.05.2019 г.)

² Об использовании при совершении сделок «виртуальных валют», в частности, Bitcoin [Электронный ресурс] // Центральный банк Российской Федерации. – Режим доступа: http://www.cbr.ru/press/PR/?file=27012014_1825052.htm (дата обращения: 15.05.2019 г.)

зампред Центрального банка Георгий Лунтовский заявил о том, что отвергать Bitcoin нельзя, потому что, возможно, за ним будущее¹.

Однако необходимо отметить, что многие страны и в том числе китайские эксперты отмечают уязвимость торговых платформ по операциям с Bitcoin, тем не менее ряд китайских сайтов принимают Bitcoin и проводят операции с ним².

В 2016 году появилась информация о том, что подготовлен Минфином России новый законопроект о запрете криптовалюты. В законопроекте предусматривается уже уголовная ответственность за выпуск (эмиссию) и обращение цифровых денег³. Внесение данного законопроекта неоднократно откладывалось⁴. В конце апреля 2016 года заместителем директора Росфинмониторинга заявлено, что криптовалюту следует рассматривать не со стороны запрета, а со стороны регулирования, поскольку этот инструмент развивается во всем мире⁵, а уже в мае заместитель министра финансов Алексей Моисеев отметил несовершенство законопроекта и назвал новые сроки его внесения на рассмотрение в Госдуму: до конца 2016 года⁶. В октябре 2016 г. Алексей Моисеев также сообщил, что Министерство финансов России решило «подождать и посмотреть, как будет развиваться ситуация на международном

¹ ЦБ не исключает будущего у bitcoin в России [Электронный ресурс] // Прайм. – 02.07.2014. – Режим доступа: <http://1prime.ru/finance/20140702/787649971.html> (дата обращения: 15.05.2019 г.)

² Савинский С.П. Криптовалюты и их нормативно-правовое регулирование в КНР // Деньги и кредит. – 2017. - № 7. – С. 66.

³ Законопроект об ответственности за использование криптовалют поступит в Госдуму в июне [Электронный ресурс] // ForkLog. — 25.02.2016. – Режим доступа: <https://forklog.com/zakonoproekt-ob-otvetstvennosti-za-ispolzovanie-kriptovalyut-postupit-v-gosdumu-v-iyune/> (дата обращения: 25.05.2019 г.)

⁴ Внесение законопроекта о запрете криптовалют в России откладывается [Электронный ресурс] // ForkLog. — 21.04.2016. Режим доступа: <https://forklog.com/vneseniezakonoproekta-o-zaprete-kriptovalyut-v-rossii-otkladyvaetsya/> (дата обращения: 25.05.2019 г.)

⁵ Росфинмониторинг: Законопроект о запрете криптовалют придется пересматривать [Электронный ресурс] // ForkLog. – 26.04.2016. – <https://forklog.com/rosfinmonitoringzakonoproekt-o-zaprete-kriptovalyut-pridetsya-peresmatrivat/> (дата обращения: 25.05.2019 г.)

⁶ Правительство РФ подготовит новый вариант законопроекта о запрете криптовалют [Электронный ресурс] // ForkLog. — Режим доступа: <https://forklog.com/pravitelstvo-rfpodgotovit-novyyj-variant-zakonoproekta-o-zaprete-kriptovalyut/> (дата обращения: 25.05.2019 г.)

уровне, и с учетом этого принять решение». Таким образом, работа над законопроектом была приостановлена¹.

9 июня 2017 г. заместитель министра финансов Алексей Моисеев заявил, что криптовалюту в России могут квалифицировать как «иное имущество», то есть придать ей более-менее легальный статус. Он добавил, что при проведении операций с отечественной цифровой валютой клиенты будут идентифицированы. Он также подчеркнул, что при проведении транзакций с криптовалютой необходимо ввести идентификацию клиентов и предусмотреть защиту прав покупателей. Таким образом, речь не идёт о создании полного аналога Bitcoin. Отечественная криптовалюта будет не анонимной и будет эмитироваться из единого центра, который можно легко контролировать. То есть от Bitcoin исключат 2 ключевых элемента. С другой стороны, создание криптовалюты подразумевает использование Block Chain – на сегодняшний день это одна из самых передовых технологий, которая позволяет почти на 100% защитить транзакции внутри системы².

Среди технологий и схем в сфере криптовалют популярность приобретает анонимная версия – даркнет. Термином «даркнет» обозначают совокупность веб-сайтов, видимых публично, которые имеют скрытый IP-адрес сервера, на котором они размещаются. Такие сайты могут посещать все веб-пользователи, но выяснить, кто является их автором, – очень сложно. В то же время на подобные сайты невозможно попасть, используя популярные поисковые системы. Практически все сайты, что находятся в так называемом даркнет, скрывают свою принадлежность, используя инструмент шифрования TOR. Технология TOR позволяет пользователям хранить свою анонимность в Интернете при посещении сайтов, ведении блогов и отправке сообщений. С

¹ Минфин отложил подготовку закона о запрете Bitkoinов [Электронный ресурс] // Lenta.ru. – Режим доступа: <https://lenta.ru/news/2016/10/11/minfinbitcoin/> (дата обращения: 25.05.2019 г.)

² См.: Фомин А.Н. Криптовалюты в цифровой экономике: финансово-экономические аргументы «за» и «против». Аналитический доклад. – М., 2017.

помощью технологии TOR осуществляется сокрытие личных данных и местоположения. В случае, когда в управлении сети TOR находится вебсайт, эффект наблюдается тот же, что и в ситуации с конечным пользователем. Для того, чтобы посетить сайт в даркнете, который использует инструмент шифрования TOR, веб-пользователь должен также использовать TOR. Черные рынки даркнета продают свои товары и услуги анонимным клиентам, которые часто расплачиваются криптовалютой Bitcoin. Один из крупнейших маркетов даркнета – Alphabay Market. В даркнете доступны различные виды наркотических препаратов – около 70%. Также можно купить аккаунты в соцсетях, персональную информацию и сканирование паспортов, разные документы – от номера паспорта до водительских прав. Распространенным товаром в даркнете являются сканированные копии кредитных карт, которые используются для картинга – похищение средств из этих карт. Широкое распространение приобретает даркнет и в России, где есть десятки сайтов с возможностью анонимно купить нелегальные товары.

Сдерживающим фактором пути Bitcoin к признанию на территории России способствуют несколько причин:

- нежелание законотворческих органов заключать новые и переделывать действующие нормативные акты по валютному регулированию и криптовалюты в целом;

- страх перед тем, что массовое использование криптовалюты поставит под сомнение ликвидность национальной валюты в целом;

- в перспективе переход к расчетам с использованием криптовалют может сильно ударить по банковской системе, поскольку банки не имеют влияния на рынок криптовалюты;

- нежелание отпускать в свободное плавание криптовалюту, поскольку правительство контролирует большинство сфер деятельности субъектов

хозяйствования, а рынок криптовалют действует децентрализованно и не может быть подчинен какому-то конкретному органу;

– властные органы отказываются признавать криптовалюту как собственно валюту из-за того, что, по сути, их стоимость не подкреплена ни стоимостью золота, ни товарной массой¹.

Наибольшим риском популяризации криптовалюты для России является легкость легализации средств, полученных преступным путем. Отсутствие связи между счетами в виртуальных валютах и реальными людьми в сочетании с возможностью обладать неограниченным количеством счетов в настоящее время предопределяет благоприятная цифровая среда для создания новых сложных моделей, направленных на сокрытие незаконного происхождения денежных средств.

Из положительных качеств можно отметить высокую скорость проведения операций с криптовалютами позволяющую экономить затраты времени и рабочей силы, а также повысить динамичность предпринимательской деятельности, что в конечном счете положительно повлияет на экономику стран, так как сегмент предпринимательства является локомотивом развития.

Можно сделать вывод, что возможно притормозить процесс развития криптовалют, не создавая для них необходимой инфраструктуры, но рано или поздно они все равно займут свое место в мировой финансовой системе. Поэтому, по нашему мнению, следует дождаться, когда Bitcoin и другие криптовалюты наладят свою систему безопасности и стабильность работы, после чего необходимо начать создание механизма, необходимого для их корректной работы. Прежде всего, это касается формирования законодательной базы, которая бы регулировала существование криптовалют, как в отдельно взятой стране, так и на межгосударственном уровне. Затем необходимо создать инфраструктуру, которая бы обеспечивала полноценное функционирование

¹ Дудин М.Н., Лясников Н.В. Использование криптовалюты в незаконных целях: обеспечение финансово-экономической безопасности // Проблемы рыночной экономики. – 2018. - № 3. – С. 19.

такой финансовой системы, разрешить расчеты криптовалютами через терминалы и различные актуальные сервисы, что повысит спрос на них и количество сделок, проведенных с криптовалютой.

Проблема правовой регламентации обращения криптовалют, порожденная современным глобализированным миром, имеет комплексный характер. Влияние на зарождение данной проблемы оказывают в первую очередь социально-экономические факторы современного глобализированного мира и конфликты юрисдикций, а также применение национального права разных стран к отношениям, которые возникают во время обращения криптовалют. В то же время, значительный общественный интерес к проблеме обуславливает необходимость поиска адекватного механизма правового регулирования, поскольку существующие способы саморегулирования не поколеблют права собственности и законных интересов.

По нашему мнению, государственное воздействие на отношения, складывающиеся в сфере обращения криптовалют должно происходить в определенных зонах влияния, к которым возможно отнести следующие:

- зона регламентации обращения криптовалюты на биржах и ее использование в платежных системах;
- зона ответственности за сохранение крипто валюты (прежде всего, путем технической защиты информации);
- зона применения криптовалют для совместного инвестирования;
- зона использования криптовалют в гражданско-правовых отношениях.

Кроме этого, должны быть разработаны эффективные межгосударственные механизмы взаимодействия в сфере оборота криптовалют, прежде всего, в интересах противодействия преступности и юридической ответственности за совершение правонарушений экономического характера (в частности финансового мошенничества).

Несмотря на все разные мнения относительно криптовалют, стоит признать, что их появление на мировом финансовом рынке является феноменом, который в теории и практике может в корне изменить сложившуюся в мире финансовую систему. Именно поэтому правительства стран не спешат давать разрешение на массовое внедрение криптовалюты на своих территориях, поскольку альтернатива существующей финансовой системе может изменить силу воздействия центральных органов на управление финансовыми процессами. Теоретически криптовалюта может положительно повлиять на бизнес, поскольку отсутствие комиссии во время осуществления операций позволит предприятиям получить свободные средства, которые будут использованы на развитие производства, и в целом уменьшить расходную часть субъектов хозяйствования.

Представляется, что широкое распространение Bitcoin (и других криптовалют) не приведет к краху банковской системы, однако может ее серьезно пошатнуть, так как Bitcoin (и другие криптовалюты) составляют огромную конкуренцию привычным банковским схемам, позволяя переводить и конвертировать в реальную валюту (доллары, рубли и евро) суммы со значительно более низкой комиссией, чем при операциях с валютой в банках. Значительная часть Bitcoin (и других криптовалют) находится в частных руках, ограниченной группы лиц, которая может управлять курсом данной валюты. Кроме того, валюта, не имеющего определенного контроля со стороны Центробанка, может привести к финансовому коллапсу¹.

Изучению феномена блокчейн (block chain) целесообразно уделять всестороннее внимание, поскольку это позволит предотвращать преступным технологиям и схемам связанных с использованием цифровых валют. В данном контексте особое внимание следует уделять обучению и повышению

¹ Дудин М.Н., Лясников Н.В. Использование криптовалюты в незаконных целях: обеспечение финансово-экономической безопасности // Проблемы рыночной экономики. – 2018. - № 3. – С. 21.

квалификации специалистов, госслужащих и правоохранительных органов на основе сотрудничества с правительствами других стран и международной правовой помощи. Также представляется, что необходимо минимизировать анонимность, которая является одним из главных недостатков криптовалют. Для этих целей возможно ввести полную идентификацию в банке при покупке Bitcoin, а также обязать компании, которые принимают платежи в криптовалюте, проводить идентификацию. Это поможет добиться определенного качества в контроле за оборотом криптовалюты в России.

ГЛАВА 2. ВЫЯВЛЕНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

§ 1. Динамика преступлений, совершаемых с использованием криптовалюты

Противники криптовалют часто утверждают, что криптомонеты массово используются в отмывании денег, торговле наркотиками, оружием, финансовых преступлениях и финансировании террористов. В прессе регулярно выходят статьи об очередном взломе криптобиржи или отмывании денег через биткоины. Проведем анализ масштабов проблемы, для этого проанализируем преступления, совершаемые с использованием криптовалюты по следующим группам:

Взломы бирж и кошельков. Больше всего преступники украли у бирж – зачастую их легче взломать, чем отдельный кошелек, а потенциальный доход несоизмеримо больше.

По данным Group-IB, CipherTrace, Carbon Black, хакеры украли в 2018 году криптовалют на сумму от \$1.1 до \$1.7 миллиарда, из которых \$960 миллионов – у криптобирж и платежных систем. Количество таких случаев выросло в 3.5 раза по сравнению с 2017 годом, и в 7 раз по сравнению с 2016 годом. 56% криптокраж пришлось на биржи Южной Кореи и Японии¹.

Самые крупные кражи в 2018 году:

- \$532 миллиона у Coincheck
- \$60 миллионов у Zaif
- \$40 миллионов у Coinrail
- \$31 миллион у Bithumb

В большинстве случаев причинами краж стала незащищенность горячих кошельков, на которых хранились средства пользователей.

¹ Group-IB: ущерб от 14 кибератак на криптобиржи составил \$882 млн [Электронный ресурс] // Режим доступа: <https://www.group-ib.ru/media/gib-crypto-summary/> (дата обращения 18.06.2019).

Хакеры работают командами, а не поодиночке. Большинство хакерских атак совершают не одиночки, а командные игроки.

Согласно исследованию аналитической компании Chainalysis, 2 группы хакеров провели 60% всех зарегистрированных взломов криптобирж и суммарно украли криптовалюты на сумму более \$1 миллиарда¹.

Исследователи обозначили хакерские группы как «Альфа» и «Бета». «Альфа» – это гигантская, жестко контролируемая организация, которая преследует не только денежные цели. «Бета» – менее организована, хуже следит за безопасностью и полностью сосредоточена на деньгах.

Обе группы действуют с украденными криптовалютами по-разному. «Альфа» переводит монеты сразу после взлома, «Бета» – в течение 18 месяцев. Хакеры ждут минимум 40 дней, пока интерес к краже стихнет, после чего стараются обналечить монеты как можно быстрее – 50% всех украденных средств обналечиваются в течение 112 дней.

Обычно хакеры крадут монеты на \$90 миллионов за раз, но увеличилось и количество «незначительных краж» на \$20–\$30 миллионов. После кражи, в среднем, они пропускают украденные криптовалюты около 5000 раз через систему кошельков, обменников и одноранговых транзакций до того, как обменять их на фиатные валюты.

Для обналечивания денег иногда используются даже регулируемые биржи, соблюдающие строгие процедуры AML – процессов по борьбе с отмыванием денег. Отследить украденные или отмытые деньги сложно – о происхождении денег можно узнать лишь постфактум, но не в режиме реального времени.

Исследователи считают, что обе группы, скорее всего, все еще активны².

ICO-мошенничество и фейки в Twitter. По разным данным, от половины до 80% ICO изначально создавались как мошеннические: их организаторы знают о нереализуемости проекта, а значительная часть собранных средств тратится на

¹ Crypto Crime Series: расшифровка хаков [Электронный ресурс] // Режим доступа: <https://blog.chainalysis.com/reports/crypto-crime-hacks> (дата обращения 18.06.2019).

² Там же.

личные или рекламные цели¹. При этом в 2017 году за счет ICO было привлечено от \$5.6 до \$6.2 миллиарда. Раз ICO никак не регулируются, то у их организаторов нет никакой ответственности перед инвесторами. Согласно данным Европейского центра анализа киберпреступности ЕС, в 2017-2018 годах скам-проекты привели к потере \$1.4 миллиарда инвесторами².

Самый яркий пример ICO-мошенничества в 2018 году – американский проект Centra. Весной проект, который рекламировал боксер Флойд Мейвезер и другие знаменитости, обманом привлек \$32 миллиона, после чего руководство попыталось сбежать из страны. В ноябре интересный случай произошел со скам-проектом Pure Bit – руководитель стартапа сначала сбежал с \$2.7 миллиона, а потом раскаялся и вернул деньги пользователям.

В 2018 году в Twitter также были популярны так называемые «нигерийские письма» – вид мошенничества, когда с поддельных страниц знаменитостей обещают бесплатно раздать монеты в обмен за небольшой платеж. Мошенничество быстро раскрывается, но фейки могут успеть заработать по несколько тысяч долларов, а вся «отрасль», по некоторым оценкам, приносит от \$50,000 до \$100,000 в день.

Фишинг, криптоджекинг и вымогательство. Одна из популярных схем обмана пользователей – фишинг – создание сайтов-клонов известных бирж, ICO-проектов и кошельков (86% подделок – кошелек MyEtherWallet). Когда пользователи вводят свои данные в фишинговой программе, злоумышленники получают полный доступ к счетам жертвы.

Судя по данным Лаборатории Касперского, каждый квартал преступники крадут таким образом по \$2–\$3 миллиона³.

¹ CRYPTOASSET MARKET COVERAGE INITIATION [Электронный ресурс] // Режим доступа: https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ (дата обращения: 18.06.2019).

² Европейский центр анализа киберпреступности ЕС [Электронный ресурс] // Режим доступа: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf (дата обращения: 18.06.2019).

³ Спам и фишинг во втором квартале 2018 года [Электронный ресурс] // Режим доступа: <https://securelist.com/spam-and-phishing-in-q2-2018/87368/> (дата обращения: 18.06.2019).

Также распространен незаконный майнинг – криптоджекинг, когда преступники используют зараженный компьютер для незаметного майнинга в свою пользу. Количество подобных случаев в 2018 году увеличилось в 4 раза, вирусами были заражены около 13 миллионов устройств. Сначала криптоджекинг применяли для майнинга, со временем его стали использовать и для проведения DDoS-атак и других киберпреступлений. Главные жертвы криптоджекинга – компании. По данным Carbon Black, атаки на предприятия составили пятую часть всех хакерских атак¹.

Кибер-вымогательство – это еще одна новая форма киберпреступлений. Вирусы шифруют файлы на зараженном компьютере, после чего требуют выкуп в криптовалютах за ключ дешифровки. Яркие примеры: CryptoWall, Locky, KeRanger, XCodeGhost, WannaCry, NotPetya. По оценкам Cyber Threat Alliance, вирусы-вымогатели могли суммарно вытянуть у их жертв \$325 миллионов².

Отмывание денег. Из-за анонимности и правовой неопределенности криптовалют их принято обвинять в использовании при отмывании незаконных доходов. По данным Европола и Великобритании через криптовалюту отмывают \$5.5 миллиарда в год. 97% криминальных биткоинов отмывают через биржи со слабой AML-политикой.

Исследователи утверждают, что доля нелегальных транзакций с биткоином снижается каждый год и составляет 0.6%–1% от всех транзакций (по японским данным, всего 0.19%)³.

По данным ООН, ежегодный объем нелегальных сделок составляет \$1–\$2 триллиона⁴. На этом фоне \$1–\$2 миллиарда кажутся незначительными – это

¹ В этом году была украдена криптовалюта на 1,1 миллиарда долларов, и это было легко сделать [Электронный ресурс] // Режим доступа: <https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html> (дата обращения: 18.06.2019).

² CYBER THREAT ALLIANCE UNCOVERS CRYPTOWALL VERSION 4 [Электронный ресурс] // Режим доступа: <https://www.cyberthreatalliance.org/analysis/cyber-threat-alliance-uncovers-cryptowall-version-4/> (дата обращения: 18.06.2019).

³ Преступники прячут «миллиарды» в криптовалютах - Европол [Электронный ресурс] // Режим доступа: <https://www.bbc.co.uk/news/technology-43025787> (дата обращения: 18.06.2019).

⁴ ВСЕМИРНЫЙ ДОКЛАД О НАРКОТИКАХ [Электронный ресурс] // Режим доступа: http://www.unodc.org/wdr2017/field/WDR_Booklet1_Exsum_Russian.pdf (дата обращения: 18.06.2019).

десятые доли процента. Вся капитализация Monero, Dash и ZCash – \$2.2 миллиарда на данный момент. Очевидно, что денежная масса отмываемых через криптовалюты средств незначительна.

Террористы и наркотики. Связывать криптовалюты с наркотиками стали еще со времен Silk Road. Согласно официальным данным, оборот площадки составил около \$1.2 миллиарда, доход – \$90–\$126 миллионов, ее использовали несколько тысяч нелегальных продавцов и более 100,000 покупателей по всему миру.

Согласно данным Фонда борьбы за демократию (FDD), на оборот наркотиков приходится до 90% всех незаконных транзакций с криптовалютами. Годовой оборот такой торговли может составлять \$4–\$5 миллиардов, доходить до 0.5%–1% от общего оборота и охватывать до трети всех покупателей¹.

Что касается терроризма, то, по данным отчета Европола и правительственной комиссии Великобритании, биткоин и другие криптовалюты в последнее время не использовались для финансирования терактов на территории Европы и маловероятно, что ситуация изменится в течение ближайших пяти лет. Исследование Center of a New American Security говорит о том, что террористы плохо понимают технологию криптовалют и предпочитают наличные и банковские переводы, как более удобные и безопасные. Но эксперты предостерегают, что ситуация может измениться, если террористы «распробуют» технологию и начнут ей доверять².

Из-за анонимности транзакций, быстроты переводов в обход финансовых организаций и отсутствия необходимости уплаты налогов криптовалюты кажутся идеальными средствами для ухода от налогов, отмывания денег и покупки оружия. Но на деле они не так удобны для преступников, как может

¹ BITCOIN LAUNDERING [Электронный ресурс] // Режим доступа: <https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf?hssc=222901956.3.1516201470218&hstc=222901956.b7d6531ad164bec182c043c05b5510ba.1516201470217.1516201470217.1516201470217.1&hsp=3478668143&hsCtaTracking=66a034a3-865d-481a-8e56-f510419fde74%7C840a3208-7448-4fe6-ad03-a3731f462b7d> (дата обращения: 18.06.2019).

² ОЦЕНКА УГРОЗЫ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ В ИНТЕРНЕТЕ 2018 [Электронный ресурс] // Режим доступа: <https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018> (дата обращения: 18.06.2019).

показаться. Цифры гласят, что криптовалюты не так популярны среди преступников, как принято думать.

Опыт борьбы с даркнетом показывает, что государство способно бороться с киберпреступностью, а анонимность криптовалют сильно преувеличена – анонимно обменять деньги становится все сложнее, спецслужбы умеют связывать транзакции с конкретным пользователем, от чего не спасают даже сверханонимные монеты. В таких условиях криптовалюты – лишнее посредническое звено, ведь наличные отследить сложнее.

Если объединить цифры выше, то за последние 2 года назвать преступными очень примерно можно \$13–\$16.7 миллиарда из вращающихся в криптомире средств. Много это или мало, зависит от размера капитализации крипторынка. При капитализации в \$700 миллиардов это всего 2%, при капитализации в \$100 миллиардов – уже 13%–16%. Зато очевидно, что на фоне преступных триллионов долларов, это незначительная величина.

Фиатные наличные деньги используются преступниками в сотни раз шире, но это не повод к их запрещению. Понятно, что криптовалюты, как инструмент преступности, гораздо менее универсальны и удобны, чем их традиционные аналоги.

§ 2. Особенности выявления преступлений, совершенных с использованием криптовалюты

За последние несколько лет криптовалюты из числа сугубо технологических вопросов перешли в разряд наиболее обсуждаемых проблем развития мировой и национальных финансовых систем. Поводом для резкой трансформации взглядов стали стремительный рост капитализации криптовалют и развитие модели коллективного инвестирования (краудфандинг).

По экспертным оценкам, по состоянию на конец 2018 г. капитализация всех криптовалют составила 213 289 302 529 дол. Из них наибольший объем

имеют Bitcoin (111 млрд дол.), Ethereum (21 млрд дол.) и Ripple (20 млрд дол.)¹. В настоящее время популярность цифровых активов как объекта комплексных научных исследований² обусловлена набором экономических и технических качеств технологии распределенных реестров: безвозвратность проведенных операций (транзакций), отказ от централизованного хранения данных на серверах и, как следствие, гораздо меньшая уязвимость данных, возможность заключения и ведения смарт-контрактов непосредственно между сторонами в отсутствие посредников, возможность круглосуточного функционирования системы, низкая цена транзакций и сокращение производственной (бизнес) цепочки за счет устранения посредников и пр.

Но эти и другие преимущества новой технологии не могут быть в полном объеме оценены по причине отсутствия правового статуса как у самого блокчейна, так и у его продуктов. Вынужденный правовой вакуум приводит к увеличению числа рисков их использования и, как следствие, к нежеланию крупных финансовых и производственных структур внедрять эту технологию в свои бизнес-процессы.

Впервые о рисках использования продуктов технологии блокчейн заговорил Европол. В своем отчете за 2015 г. он проанализировал тренды оборота криптовалюты и заключил, что наибольшую популярность новые финансовые инструменты приобретают в криминальной сфере (коррупционные преступления, торговля наркотиками, психоактивными веществами и порнографией). Чаще всего криптовалюта используется в нелегальном Интернете (даркнете) при покупке изъятых из оборота веществ и продуктов. К концу 2018 г. число направлений криминального использования криптовалюты существенно увеличилось, но по-прежнему на первом месте находится

¹ Top 100 Cryptocurrencies by Market Capitalization. URL: <https://coinmarketcap.com> (дата обращения 18.06.2019).

² Булгаков И.Т. Правовые вопросы использования технологии блокчейн // Закон. – 2016. – № 12. – С. 80.

использование цифровых денег как средства расчетов на теневых интернет-рынках¹.

В конце 2018 г. рынок незаконной деятельности с биткойном составил примерно 76 млрд дол. в год (46% биткойн-транзакций), что по объемам близко к масштабам американского и европейского рынков незаконного оборота наркотиков. Кроме того, примерно пятая часть (23%) от общей долларовой стоимости транзакций и примерно половина биткойн-кошельков (49%) так или иначе связаны с незаконной деятельностью с использованием криптоалгоритмов².

По данным бизнес-школы Сиднея, оборот психоактивных веществ с использованием виртуальной валюты на протяжении пяти лет сохраняет тенденцию к росту (показатель прироста от 5 до 15%) со спецификацией на отдельных направлениях деятельности. Каждый год проводится около 40 млн криминальных сделок на сумму, превышающую 76 млн дол. Если исходить из того, что сегодня насчитывается около 22 млн владельцев цифровой валюты, то можно говорить о том, что примерно четверть из них хотя бы раз применяли криптовалюту в нелегальных расчетах³.

Популярность нового финансового инструмента в криминальной среде объясняется тем, что до настоящего времени не выработаны юридические параметры криптовалюты и не установлены границы ее безопасного оборота. Во многом это обуславливается недопониманием со стороны отечественных и международных экспертов важности исследования криптовалюты в рамках риск-ориентированного подхода, когда одновременно соотносятся экономические преимущества и криминогенный потенциал криптоинструментов. Отсутствие комплексных исследований трендов

¹ См.: Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. – 2017. – Т. 10, № 6. – С. 149-150; Спасенников Б.А. Актуальные проблемы уголовного права: обзор литературы // Актуальные вопросы образования и науки. – 2015. – № 1-2 (47-48). – С. 36-38.

² Там же. – С. 38.

³ Там же.

криминального использования криптовалюты с неизбежностью влияет на результативность работы в сфере предупреждения криптопреступлений¹.

В свете изложенного своевременным и практически значимым является криминологический анализ криптопреступности как относительно самостоятельного объекта научного познания и одновременно подсистемы криминологической модели интернет-преступности.

Под криптопреступностью предлагается понимать совокупность обладающих едиными системными свойствами деяний, совершаемых в отношении виртуальной валюты либо с ее использованием. Поскольку данное явление находится в стадии своей институционализации, применение этого термина носит условный характер. Можно выделить три основных сектора криптопреступности:

- незаконная продажа психоактивных веществ (наркотических средств, психотропных веществ и др.), иных запрещенных товаров, контента или услуг;
- отмыwanie преступных доходов с использованием новой цифровой валюты;
- хищение криптовалюты и иные преступления против собственности.

В настоящее время за криптовалюту можно приобрести широкий спектр нелегальных товаров и услуг. Виртуальные деньги используются в порноиндустрии, в сфере незаконного оборота персональных данных, в торговле поддельными документами, нелегальными лекарствами, и даже ими оплачивают заказные убийства. Но при этом самым распространенным сегментом криптопреступности остается незаконный оборот наркотических средств и психотропных веществ (80% общего объема рынка нелегальных товаров).

Первым удачным опытом выявления нелегальной торговли с использованием криптовалюты было дело Silk Road. На этом нелегальном интернет-рынке сбывалось более 10 тыс. разновидностей нелегальных товаров, а общий годовой оборот превышал 17 млн дол. Но раскрытие этого преступления

¹ Архипов В.В. Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. – 2014. – № 9. – С. 90.

только на время затормозило развитие нового сегмента криминального бизнеса. Появившиеся после Silk Road рынки (в первую очередь Silk Road 2.0 и Evolution) увеличили свой доход в среднем в 10 раз¹.

К сожалению, в настоящее время мировая статистика криминального оборота наркотиков, порнографии и запрещенных услуг с использованием цифровой валюты не ведется, но, согласно данным экспертов, именно криптовалюта является средством расчетов в 95% случаев.

При этом наблюдаются принципиально новые криминологические тренды развития теневого Интернета: постепенная спецификация отдельных криминальных сервисов и улучшение их технологических характеристик, монополизация рынка с выделением крупных игроков национального и мирового масштаба. В качестве примера можно привести данные о размерах рынка наркотических средств и психотропных веществ в плоскости развития наиболее крупных интернет-сервисов (табл. 2.1).

Таблица 2.1

Динамика дистанционной продажи наркотиков в Интернете с использованием виртуальной валюты, %²

Сервис теневого Интернета	2015	2016	2017	2018	Все годы
Абракас / Abrahax	–	–	8,99	–	3,00
Агора / Agora	0,02	42,43	47,89	0,05	26,30
Альфапей / Alfapay	–	–	9,38	46,65	6,26
Эволюшн / Evolution	–	8,36	10,08	–	5,50
Северо-восточный маркет-плейс / Northwest Marketplace	–	0,05	5,58	–	1,89
Ньюклиас / Nuklias	–	0,01	13,60	31,21	6,64
Шип маркетплейс / Ship Marketplace	84,10	–	–	–	6,64
Силк роад / Silk Road	10,30	–	–	–	32,03
Силк роад 2.0 / Silk Road 2.0	4,85	40,50	–	–	10,20
Всего	99,37	91,34	95,54	77,91	98,34

¹ Сидоренко Э.Л. Криптовалюта как новый юридический феномен // Общество и право. – 2016. – № 3 (57). – С. 193-197.

² Иванцов С.В., Сидоренко Э.Л., Спасенников Б.А., Берёзкин Ю.М., Суходолов Я.А. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // Всероссийский криминологический журнал. – 2019. – Т. 13, № 1. – С. 88.

Согласно приведенным данным, несмотря на предпринимаемые правоохранителями единичные усилия, отсутствие системной предупредительной работы приводит к тому, что отдельные криминальные сервисы после вынужденной остановки деятельности возобновляют работу и увеличивают свою доходность¹. В то же время нельзя не указать на некоторое сокращение числа традиционных площадок в силу объективного увеличения количества криминальных способов дистанционной продажи наркотиков с использованием криптовалюты².

Важно отметить и тренд расширения спектра используемых криптовалют для совершения транзакций. Если раньше абсолютным монополистом на рынке был биткойн, то сейчас все чаще стали применяться валюты с высокой степенью анонимности (ZCash, Dash, Monero). На это, в частности, указывает в своих отчетах Европол³.

Летом 2017 г. была проведена крупная операция по выявлению крупнейших наркосервисов в теневого Интернета. Результатами работы стало закрытие сервисов Альфапей и Ганза (совокупный клиентский пул – около 1 млн пользователей). Но уже через полтора года криминальный рынок смог восстановить свои объемы и нарастить их. При этом общее количество пользователей сократилось, но незначительно (приблизительно на 10%).

Масштабы наркоторговли в Интернете с использованием криптовалюты продолжают увеличиваться примерно со скоростью 44 млн дол. в год⁴.

Россия в настоящее время занимает второе место в мире по числу пользователей даркнета в части оборота психоактивных веществ. Около 300 тыс.

¹ Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты. – М.: Юрлитинформ, 2017. – С. 195.

² BITCOIN LAUNDERING // Режим доступа URL: <https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf> (дата обращения 18.06.2019).

³ Преступный преступный мир сбрасывает биткойны за другую валюту URL: <https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency> (дата обращения 18.06.2019).

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

чел. из России (более 10% от общего числа пользователей) ежедневно входят в теневой Интернет¹.

Существуют устойчивые методики продажи психоактивных веществ с применением теневых интернет-сервисов. Администратор сервиса даркнета традиционно работает на комиссии от каждой произведенной с его помощью транзакции и при этом получает фиксированную сумму (обычно в биткойнах) от продавца.

По мере развития бизнеса формируется его направленность с одновременной специализацией лиц, вовлеченных в преступные схемы. Выделяются такие новые криминальные профессии, как координаторы (администраторы одновременно нескольких сервисов), эскроу (гаранты сделки), гроверы (выращивающие наркосодержащие растения), кладмены, трафаретчики (лица, размещающие объявления на асфальте), перевозчики, дропы (посредники, принимающие товар или перевод криптовалюты) и др.

В российском сегменте криптонаркоторговли преобладают психотропные вещества и легкие наркотические средства. Изучение рынка теневого Интернета (структуры и специализации наркосервисов) позволяет говорить о том, что первое место по объемам торговли занимает каннабис, второе – психостимуляторы, третье – экстази и эйфоретики, четвертое – психоделические вещества, и лишь затем идут тяжелые наркотики (опиаты).

По данным на начало 2019 г., только на русскоговорящем ресурсе «Гидра» (Hydra) занимаются продажей каннабиса около 1,5 тыс. сервисов, стимуляторов – 1,3 тыс., экстази – 500, каннабиоидов – 200 сервисов и т.д.

Новым трендом является растущее предложение так называемых химических конструкторов, позволяющих пользователю самостоятельно изготавливать наркотики. При этом оплата этих конструкторов в 100% случаев осуществляется с использованием криптовалюты.

¹ Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты. – М.: Юрлитинформ, 2017. – С. 196.

Как правило, за криптовалюту в теневом Интернете приобретаются легкие наркотики и порнография, в абсолютном большинстве случаев именно за цифровую валюту – детская порнография. Согласно мониторингу активности такого рода сайтов, в 70% случаев клиенты-педофилы для покупки контента используют биткойны и в 30% – другую криптовалюту и альтернативные средства платежа.

Таким образом, есть основания полагать, что в настоящее время незаконная продажа наркотиков уходит в теневой Интернет и институционализируется посредством углубления специализации сайтов, расширения перечня криминальных профессий и использования криптовалюты как основного средства платежа.

Вторым важным направлением криминального использования криптовалют является отмывание преступных доходов. На опасность нового сегмента криминального бизнеса указал Банк России в информационном письме «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» от 27 января 2014 г.¹

Предостережение относительно использования виртуальной валюты в легальной экономической деятельности было повторено в информационном сообщении Федеральной службы по финансовому мониторингу Российской Федерации «Об использовании криптовалют»² и информационном письме Банка России «Об использовании частных «виртуальных валют» (криптовалют)» от 4 сентября 2017 г.³ В письме 2017 г. ЦБ РФ в качестве криминологических рисков оборота криптовалюты назвал ее анонимность и латентный характер использования физическими и юридическими лицами для проведения транзакций.

¹ Информация Банка России от 27.01.2014 г. «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» // Вестник Банка России. - № 11. – 05.02.2014.

² Информационное сообщение Росфинмониторинга «Об использовании криптовалют» // URL: <http://www.fedsfm.ru/news/957> (дата обращения 18.06.2019).

³ Информация Банка России от 04.09.2017 г. «Об использовании частных «виртуальных валют» (криптовалют)» // Вестник Банка России. - № 80. – 14.09.2017.

Однако если в незаконном обороте наркотиков важным маркетинговым свойством виртуальной валюты является ее анонимность, то применительно к отмыванию преступных доходов – правовой вакуум и отсутствие у криптовалюты правового статуса¹.

По мере расширения потребительского рынка криптовалюты возрастает и количество факторов легализации, совершенных с ее использованием. Если четыре года назад этот сегмент преступности составлял 5-7% от общего объема криптопреступности, то в 2018 г. он увеличился в 8 раз².

Многочисленное увеличение объемов этого сегмента криптопреступности обуславливается рядом факторов:

1. Существует потребность в поиске качественно новых механизмов отмывания преступных доходов ввиду возрастания их объема в сети Интернет. Данный вывод подтверждают следующие данные: около 80% клиентов организаций, занимающихся отмыванием преступных доходов, – это крупные нелегальные сервисы по продаже порнографии и психоактивных веществ.

2. Правовой вакуум вокруг статуса криптовалют и системы их финансового контроля является мощным стимулом для развития квазифинансовых структур, обеспечивающих сохранность денежных потоков с использованием технологии блокчейн либо занимающихся конвертацией криптовалюты в фиатную валюту. В 2018 г. на счета сервисов по конвертации около четверти средств пришло от организаций, занимающихся незаконной деятельностью.

3. До настоящего времени так и не выработан единый подход к определению предупредительной политики в этой сфере. ФАТФ в числе основных препятствий для сотрудничества государств в сфере выявления и пресечения отмывания преступных доходов с использованием цифровой валюты

¹ Архипов В.В. Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. – 2014. – № 9. – С. 71.

² Европол предупреждает, что Zcash, Monero и Ether играют все более важную роль в киберпреступности // URL: <https://www.coindesk.com/europol-warns-zcash-monero-and-ether-playing-growing-role-in-cybercrime> (дата обращения 18.06.2019).

указала неконтролируемые масштабы легализуемых средств, анонимные отношения между пользователями, отсутствие идентификации клиента, отсутствие единого координационного органа для выработки единой уголовной политики в отношении незаконных криптовалютных транзакций¹.

Сегодня ни в России, ни в мире не ведется учет легализованных с использованием виртуальной валюты преступных доходов. Это, однако, не препятствует выявлению и анализу отдельных криминологических трендов. В частности, важно обратить внимание на полномасштабное развитие сервисов для конвертации криптовалюты и обналичивания фиатных средств. Как правило, эти транзакции имеют характер P2P (от человека к человеку) с использованием криптоматов. По информации сервиса Coin ATM Radar, в настоящее время в мире установлено больше тысячи таких устройств, а если принять во внимание латентность данных, можно говорить и о цифрах в 30 раз больше. За комиссию в размере 15% сервис обеспечивает бесперебойность перевода и анонимность клиента.

Другой способ легализации – использование «программ-смесителей». Они предлагают клиентам запутать историю транзакций либо отмыть доходы, купив для другого лица товары в Интернете за «грязные» деньги. Покупатель компенсирует расходы клиента, за исключением суммы комиссии. В итоге клиент сервиса получает «чистые» деньги, а покупатель – дисконт на товар.

Но особое внимание следует обратить на нелегальные сервисы по конвертации криптовалюты. Самые большие объемы отмываемых 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

¹ ОТЧЁТ ФАТФ ВИРТУАЛЬНЫЕ ВАЛЮТЫ // URL: <http://docplayer.ru/25790197-Otchyot-fatf-virtualnye-valyuty-kluychevye-opredeleniya-i-potencialnyeriski-v-sfere-pod-ft.html> (дата обращения 18.06.2019).

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 валюту¹.

В специальных источниках нередко указывается на высокие риски использования криптовалюты при финансировании терроризма². Существует мнение, что в настоящее время эти прогнозы несколько преувеличены. Специалисты недооценивают традиционность этого сегмента преступности и не учитывают неготовность террористов использовать новые технологии при организации преступных доходов. Для большинства террористических организаций единственным способом транша остается физическая транспортировка наличных денег. Однако по мере расширения применения криптовалюты и развития инфраструктуры транзакций виртуальная валюта будет все чаще использоваться для финансирования терроризма³.

Третью группу преступлений с использованием криптовалюты составляют корыстные 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 среднем +400% ежегодно). Это объясняется рядом обстоятельств: анонимность цифровых кошельков и клиентов, препятствующая определению статутного владельца цифрового актива, невозможность отнесения криптовалюты к объектам гражданских прав и др.

Лица, похищающие криптовалюту, применяют следующие способы:

¹ The Cybercriminal Roots of Selling Online Gaming Currency // URL: <http://documents.trendmicro.com/assets/wp/wp-cybercrime-online-gaming-currency.pdf> (дата обращения 18.06.2019).

² «АГОРА», КРУПНЕЙШИЙ РЫНОК НАРКОТИКОВ «ТЕМНОЙ ПАУТИНЫ», ОТКЛЮЧАЕТСЯ // URL: <https://www.wired.com/2015/08/agora-dark-webs-biggest-drug-market-going-offline> (дата обращения 18.06.2019).

³ Новый рубеж в сборе средств для терроризма: Биткойн // URL: <https://www.thecipherbrief.com/column/private-sector/new-frontier-terror-fundraising-bitcoin-1089> (дата обращения 18.06.2019).

– использование фейковых (поддельных) электронных кошельков. Потерпевшие, покупая товар или услуги на популярных сервисах, перечисляют деньги на фишинговые кошельки, имеющие другие адреса, посредством использования преступниками вирусных программ. Так, в 2017 г. на площадке AppStore было выявлено несколько фишинговых кошельков популярных компаний GreenAddress, Simple Bitcoin Wallet, GreenBits Bitcoin Wallet, Bitcoin Armory Wallet и др.¹, позволяющих воровать деньги и персональные данные клиентов легальных сайтов;

– создание фишинговых сайтов (или сайтов- копий) популярных ресурсов. По данным Управления ООН по наркотикам и преступности, уровень виктимизации населения в 21 стране мира в сфере компьютерного мошенничества (фишинга) составляет от 5 до 17%, что сравнимо с уровнем виктимизации в сфере краж со взломом, грабежей и угона автомобилей. В настоящее время криптовалютный фишинг только начинает активно развиваться, но уже к середине 2019 г. может превысить настоящие показатели на 200% в связи с ростом количества сервисов, оказывающих биржевые услуги (обменники, криптобиржи и др.);

– краудинвестиционные 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 данным С.В. Иванова, Э.Л. Сидоренко, Б.А. Спасенкова, более трех четвертей всех организованных в 2017-2018 гг. краудфандинговых компаний являются мошенническими²;

– создание инвестиционных фондов, работающих с использованием криптовалюты. Если учесть тот факт, что они создавались на фоне высокой

¹ На Apple iTunes App Store появились фальшивые криптовалютные кошельки // URL: <https://bits.media/news/na-apple-itunes-app-store-poyavilis-falshivye-kriptoalyutnye-koshelki> (дата обращения 18.06.2019).

² См.: Иванцов С.В., Сидоренко Э.Л., Спасенников Б.А., Берёзкин Ю.М., Суходолов Я.А. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // Всероссийский криминологический журнал. – 2019. – Т. 13, № 1. – С. 91.

волатильности криптовалюты и в условиях отсутствия правовых гарантий защиты вкладчиков, логично предположить, что более 40% из них потенциально могут иметь криминальные цели¹. 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. Это дает мощный импульс к развитию нового сегмента криминального бизнеса, и, по нашим оценкам, уже в 2019 г. количество криминальных криптофондов может увеличиться более чем в 2 раза.

В заключение анализа важно подчеркнуть, что современная криптопреступность демонстрирует негативную качественную и количественную трансформацию на фоне очевидной неготовности правоохранительных органов разработать единые стандарты предупреждения такого рода преступлений, а законодателей – определить правовой статус криптовалюты и других цифровых продуктов блокчейна. Для криптопреступности характерно увеличение динамики, углубление специализации компаний и «опривычивание» криминального использования виртуальной валюты.

В целях предупреждения дальнейшего развития криптопреступности важно разработать такую модель правового регулирования оборота, в которой одновременно были бы решены две задачи: предупреждение совершения корыстных преступлений и поддержка инновационного развития российской экономики.

Целесообразно обозначить некоторые приоритетные направления правового регулирования новых финансовых инструментов с одновременным обеспечением безопасности участников рынка:

¹ Общее число криптовалютных хедж-фондов увеличилось до рекордных 226 // URL: <https://forklog.com/obshhee-chislo-kriptoalyutnyh-hedzh-fondov-uvelichilos-do-rekordnyh-226> (дата обращения 18.06.2019).

- включение криптовалюты в число объектов гражданских прав (ст. 128 ГК РФ¹) с одновременным определением в специальных нормативных правовых актах пределов безопасности использования модели коллективного инвестирования (краудфандинга);
- введение требования об обязательной идентификации владельцев цифровых активов и иных лиц, участвующих в их обороте;
- установление режима конвертации цифровой криптовалюты в фиатную;
- определение правовых критериев и стандартов предупреждения отмывания криминальных доходов, в том числе с использованием криптовалюты²;
- введение уголовной и административной ответственности за нарушение стандартов оборота криптоинструментов³;
- создание международной базы данных о лицах, занимающихся незаконным оборотом и применением цифровых финансовых активов⁴, в контексте используемых технологий и субъектов криптопреступности;
- определение модели налогового администрирования криптовалюты и иных цифровых активов и др.⁵;
- лицензирование профессиональной деятельности, связанной с созданием и оборотом новых цифровых активов.

¹ Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 г. № 51-ФЗ (ред. от 03.08.2018 г.) // СПС КонсультантПлюс.

² См.: Иванцов С.В., Новиков С.В. Преступления на рынке ценных бумаг: криминологическая характеристика и предупреждение. – М.: Юнити-Дана, 2012. – 119 с.

³ Ларина Е., Овчинский В. Криптовалюта: свет и тени // Наш современник. – 2018. – № 8. – С. 224.

⁴ Суходолов А.П. и др. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. – 2017. – Т. 11, № 1. – С. 13-21.

⁵ См.: Сидоренко Э.Л., Шайдуллина В.К., Киракосян С.А. Токенизация угольной промышленности: экономические и криминологические риски // Уголь. – 2018. – № 12. – С. 54-59.

ГЛАВА 3. ОРГАНИЗАЦИЯ И МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

§ 1. Криминалистические особенности расследования преступлений с использованием криптовалют

На современном этапе развития появились и уже довольно прочно закрепились в использовании такие платежные системы, как WebMoney, «Яндекс.Деньги», Qiwi, EasyPay и др. Однако прогресс не стоит на месте и, начиная с 2009 г., мир узнал о существовании абсолютно новой электронной платежной системы Bitcoin (от англ. bit – единица информации «бит» и coin – «монета»), использующей одноименные единицы расчета. Bitcoin относят к децентрализованным виртуальным валютам или к так называемым криптовалютам¹.

Создание электронных платежных систем, основанных на применении криптографии, с практически анонимными расчетами, их широкое распространение, явились не только новым свидетельством технического прогресса, но и с неизбежностью повлекли за собой и негативные последствия, связанные с использованием их в преступных целях.

В связи тем, что контролировать распространение криптовалют чрезвычайно трудно и расчет с их помощью неподконтролен какому-либо ведомству, Bitcoin представляет значительную угрозу для мирового сообщества. Так как Bitcoin набирает популярность, он становится все более привлекательным инструментом, используемым для совершения как «традиционных» видов преступлений, так и при расчетах за наркотики, азартные игры, торговлю людьми, детскую порнографию, терроризм и при других

¹ Рудик М.В., Торопов С.А. Несовершеннолетний как субъект преступлений в сфере компьютерной информации // Евразийский юридический журнал. – 2016. - № 3 (94). – С. 222.

преступлениях. Bitcoin используют преступники, которые избегают традиционных финансовых систем, и проводят глобальные денежные переводы в интернет-пространстве.

Это свидетельствует об остроте проблемы борьбы с преступлениями, совершенными с помощью электронных платежных систем. Такого рода преступления причиняют серьезный экономический ущерб и даже представляют непосредственную угрозу существованию человечества.

Распространение преступлений данной категории ставит сотрудников правоохранительных органов перед необходимостью детального изучения программно-технических возможностей совершения платежей в криптовалюте, совершенствованию, как методики расследования таких преступлений в целом, так и проведения отдельных следственных действий. Помимо недостаточной разработанности проблемы, существуют также и потребности в дальнейшем развитии криминалистической теории, обогащения ее достижениями смежных наук и углубления научных знаний о методике расследования такого вида преступлений.

Существуют определенные особенности, связанные с процессом расследования преступлений, совершаемых с помощью электронных платежных систем на основе криптографии. Одной из таких особенностей является наличие так называемых «виртуальных» следов. Это связано с тем, что все расчеты при работе с сетью Bitcoin осуществляются с использованием компьютера или иного аппаратного средства и подключения к глобальной сети Интернет. Необходимо учитывать данные особенности при проведении отдельных следственных действий. Следовательно, для проведения качественного расследования необходимо владеть не только знаниями компьютерной технологии, но и знанием механизма функционирования сети Bitcoin¹.

¹ Аслаян Р.Г. Понятие и признаки информации как предмета преступлений в сфере экономической деятельности // Библиотека уголовного права и криминологии. – 2016. - № 1 (13). – С. 7.

При расследовании преступлений, совершенных с использованием криптовалют востребованы сведения о самой платежной системе, криптовалюте, порядке регистрации и использовании электронного кошелька, обороте, порядке осуществления транзакций, порядке регистрации и использования электронного кошелька и т.д. При этом большое значение имеет наличие или отсутствие возможности обмена криптовалют на другие криптовалюты или наличные деньги. Событие преступления, совершаемого с использованием криптовалют, имеет особенности, связанные со спецификой таких его существенных элементов, подлежащих установлению по уголовному делу, как место и время совершения преступления.

Традиционно местом преступления признается место, где произошло деяние, значимое в криминалистическом и уголовно-правовом отношении.

При расследовании преступлений, совершенных с использованием криптовалют, необходимо обследовать не только место нахождения потерпевшего, но и предполагаемое место из которого был совершен доступ к сети криптовалют. Необходимо обозначить место нахождения компьютера или иного аппаратного средства, через которое совершено преступление (например, через компьютер, телефон, планшетный компьютер на который установлено необходимое программное обеспечение, через адрес рабочего компьютера и т.д.).

В рассматриваемых преступлениях большое значение имеет именно местоположение преступника и используемых им программных и аппаратных средств совершения преступления. Нередко в силу особенностей проведения операций с криптовалютами местоположение программных и аппаратных средств совершения преступления и преступника – не совпадают. Эти особенности необходимо учитывать при проведении и процессуальном оформлении осмотра места происшествия и места совершения преступления.

Также важен тот факт, что преступления рассматриваемой категории нередко имеют международный характер. Однако в виду характерных

особенностей, присущих криптовалютам, процедура получения сведений о самой системе платежей и транзакциях, не составляет особого труда, даже если операции проводились с IP-адресов устройств, расположенных на территории иностранных государств. Проверка проводится через сайт: <http://blockchain.info>.

Время совершения преступления как элемент события преступления, совершаемого с использованием криптовалют, также обладает своей спецификой. Необходимо учитывать тот факт, что различные подсистемы компьютера фиксируют время того или иного события не только в различной кодировке, но и в различных часовых поясах. В случае если интерпретация содержимого компьютерных журналов будет ошибочной, ошибочной будет и интерпретации времени события. Это в свою очередь может повлечь за собой получение недостоверного «доказательства» работы пользователя с криптовалютой, а соответственно вины или невинности лица подозреваемого в совершении преступления.

Время совершения преступления также имеет значение в случае совершения многоэпизодного преступления, поскольку позволяет выявить определенную взаимосвязь между отдельными элементами преступного деяния¹. Примером многоэпизодного преступного деяния может служить периодичное хищение криптовалют из кошелька в одно и то же время, что может свидетельствовать об особенностях графика работы преступника, его местонахождении, технических особенностях доступа к сети Интернет и т.д.

Личность преступника занимает особое место в криминалистической характеристике преступлений, является важным фактором, подлежащим учету в ходе выявления и расследования преступлений. Исходя из специфики механизма функционирования систем, основанных на использовании криптовалют, можно

¹ О времени совершения преступления см.: Сокол В.Ю. Научно-исследовательские проблемы криминалистики // Общество и право. – 2008. - № 1. – С. 17–18.

предположить, что субъекты преступной группы будут обладать особыми чертами¹.

Поскольку преступления рассматриваемой категории всегда совершаются с использованием аппаратно-программных средств, можно предположить, что типичные черты личности будут в целом такими же, как и у лиц, совершающих преступления в сфере информационно-коммуникационных технологий².

На сегодняшний день необходимым условием качественного проведения расследования любого преступления является производство комплексных исследований, связанных с познанием закономерностей, обусловивших возникновение следов преступной деятельности и других процессов, происходящих во время его формирования. Все элементы механизма преступления, так или иначе, образуют многочисленные следы, содержащие информацию о преступлении.

Как и все преступления, преступления, совершенные с использованием криптовалют, оставляют определенные характерные следы, знание которых поможет субъекту расследования, как выявить преступление, так и выбрать тактику проведения следственных действий, получить необходимую информацию о способе совершения преступления и лице, его совершившем.

Одной из наименее исследованных проблем использования криптовалют в преступных целях является проблема обнаружения и выявления следов данных преступлений.

Классификация следов, оставленных на месте преступления, будет в первую очередь зависеть от способов хранения криптовалюты Bitcoin.

Существует несколько способов хранения Bitcoin:

¹ Адигамоваг. З., Канищева О.И. Проблемы раскрытия и расследования экономических преступлений в сфере жилищно-коммунального хозяйства на основе бухгалтерской информации // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. – 2016. - № 19-2. – С. 53.

² Матюшенко В.А. Общая характеристика преступлений в сфере компьютерной информации // крымские юридические чтения материалы научно-практической студенческой конференции. Академия Генеральной прокуратуры Российской Федерации, Крымский юридический институт. 2016. – С. 405.

1. На личном компьютере. В данном случае для хранения используются различные Bitcoin-клиенты (например, Bitcoin Core, Armory, Electrum и др.), которые обеспечивают качественную шифровку и защиту кошелька паролем.

2. На съемном носителе. Копии кошелька размещаются на различных носителях съемного типа, включая всевозможные flash-накопители, внешние жесткие и оптические диски, которые по желанию можно поместить в сейф или банковскую ячейку, например. В результате легко восстановить содержимое кошелька и необходимые настройки в случае повреждения системы или выхода из строя самого компьютера.

3. На веб-сервисе или бирже. Данные онлайн ресурсы используются в основном для хранения небольшого числа Bitcoin, доступ к которым прост и оперативен. Чтобы воспользоваться кошельком достаточно наличия мобильного устройства. Нет необходимости в сложном программном обеспечении системы Bitcoin. Коды и пароли к хранилищам средств подбираются с использованием генераторов паролей, чтобы последние были, как можно, сложнее. Однако, в случае легальной работы биржи на территории России, пользователь перестает анонимно пользоваться хранилищем, так как на биржу понадобится выслать сканы документов¹.

4. На бумажном носителе. Распечатывая Bitcoin-кошелек на бумаге, пользователь может получить 100%-ю гарантию конфиденциальности информации о своих Bitcoin. Вся информация представляется в виде QR-кода (двумерного штрих-кода, предоставляющего информацию для быстрого ее распознавания с помощью камеры на мобильном телефоне), считывая который, ключи и адреса можно импортировать в Bitcoin-клиент на компьютер и получить доступ к своим Bitcoin. Хранить кошелек на бумаге безопасно и надежно, если поместить ее, например, в банковскую ячейку.

¹ Герман Т.В. Личность преступника как элемент криминалистической характеристики преступлений в сфере компьютерной информации // Юридическая наука и практика: традиции и новации Сборник статей Международной научно-практической конференции. – 2016. – С. 32.

5. На карте. Bitcoin-карты просты для пополнения и списания средств с кошелька при нахождении пользователя в любой точке мира, где установлены Bitcoin-банкоматы, удобны при конвертации валюты. Они содержат QR-код на одной стороне и Bitcoin-адрес – на другой.

Следы, образуемые в процессе функционирования сети Bitcoin, в силу своей специфики редко остаются в виде изменения внешней среды. Они в большинстве случаев носят информационный характер, то есть представляют собой те или иные изменения компьютерной информации.

На основании изложенного, представляется целесообразным рассматривать следы, образуемые в процессе функционирования Bitcoin, которые могут быть обнаружены, зафиксированы и изъяты при проведении следственных действий, как совокупность:

1. Материально фиксированных, или классических «трассологических», следов¹. Ими могут быть какие-либо рукописные записи, распечатки, а также отпечатки пальцев на клавиатуре, элементах системного блока, всевозможные микроследы и т.п., свидетельствующие о подготовке к совершению и непосредственном совершении преступления.

2. Виртуальных следов. Данные следы занимают, условно, промежуточную позицию между материальными и идеальными следами. Прежде всего, такие следы остаются на магнитных носителях информации – жестких дисках, флешкартах, внешних жестких дисках, оптических дисках и др.

Особую сложность представляет обнаружение именно виртуальных следов, указывающих на работу с криптовалютами. Преступления, совершенные с использованием криптовалют, предполагают нахождение таких следов в первую очередь в виде специфических изменений аппаратно-программной среды, зафиксированных на электронных носителях информации.

Предпосылками к успешному расследованию преступления с использованием криптовалют в большинстве случаев будут быстрота и решительность действий следователя и оперативного сотрудника,

организованное взаимодействие с различными подразделениями правоохранительных органов, а также наличие квалифицированного специалиста в области информационно-коммуникационных технологий.

§ 2. Особенности проведения оперативно-розыскных мероприятий при раскрытии преступлений, совершаемых с использованием криптовалюты

Создание электронных платежных систем, основанных на применении криптографии, с практически анонимными расчетами, их широкое распространение, явились не только новым свидетельством технического прогресса, но и с неизбежностью повлекли за собой и негативные последствия, связанные с использованием их в преступных целях.

В связи тем, что контролировать распространение криптовалют чрезвычайно трудно и расчет с их помощью неподконтролен какому-либо ведомству, Bitcoin представляет значительную угрозу для мирового сообщества. Так как Bitcoin набирает популярность, он становится все более привлекательным инструментом, используемым для совершения как «традиционных» видов преступлений, так при расчетах за наркотики, азартные игры, торговлю людьми, детскую порнографию, терроризм и при других преступлениях. Bitcoin используют преступники, которые избегают традиционных финансовых систем, и проводят глобальные денежные переводы в интернет-пространстве.

Это свидетельствует об остроте проблемы борьбы с преступлениями, совершенными с помощью электронных платежных систем. Такого рода

преступления причиняют серьезный экономический ущерб и даже представляют непосредственную угрозу существованию человечества¹.

Распространение преступлений данной категории ставит сотрудников правоохранительных органов перед необходимостью детального изучения программно-технических возможностей совершения платежей в криптовалюте, совершенствованию, как методики расследования таких преступлений в целом, так и проведения отдельных следственных действий. Помимо недостаточной разработанности проблемы, существуют также и потребности в дальнейшем развитии криминалистической теории, обогащения ее достижениями смежных наук и углубления научных знаний о методике расследования такого вида преступлений.

Существуют определенные особенности, связанные с процессом расследования преступлений, совершаемых с помощью электронных платежных систем на основе криптографии. Одной из таких особенностей является наличие так называемых «виртуальных» следов. Это связано с тем, что все расчеты при работе сетью Bitcoin осуществляются с использованием компьютера или иного аппаратного средства и подключения к глобальной сети Интернет. Необходимо учитывать данные особенности при проведении отдельных следственных действий.

Следовательно, для проведения качественного расследования необходимо владеть не только знаниями компьютерной технологии, но и знанием механизма функционирования сети Bitcoin.

При расследовании преступлений, совершенных с использованием криптовалют востребованы сведения о самой платежной системе, криптовалюте, порядке регистрации и использовании электронного кошелька, обороте, порядке осуществления транзакций, порядке регистрации и использования электронного

¹ Маркарян Э.С. Особенности получения данных о механизме слепообразования при расследовании преступлений, совершенных с использованием криптовалют // Библиотека криминалиста. Научный журнал. – 2017. - № 4 (33). – С. 176-187.

кошелька и т.д. При этом большое значение имеет наличие или отсутствие возможности обмена криптовалют на другие криптовалюты или наличные деньги.

Событие преступления, совершаемого с использованием криптовалют, имеет особенности, связанные со спецификой таких его существенных элементов, подлежащих установлению по уголовному делу, как место и время совершения преступления.

Традиционно местом преступления признается место, где произошло деяние, значимое в криминалистическом и уголовно-правовом отношении.

При расследовании преступлений, совершенных с использованием криптовалют, необходимо обследовать не только место нахождения потерпевшего, но и предполагаемое место из которого был совершен доступ к сети криптовалют. Необходимо обозначить место нахождения компьютера или иного аппаратного средства, через которое совершено преступление (например, через компьютер, телефон, планшетный компьютер на который установлено необходимое программное обеспечение, через адрес рабочего компьютера и т.д.).

В рассматриваемых преступлениях большое значение имеет именно местоположение преступника и используемых им программных и аппаратных средств совершения преступления. Нередко в силу особенностей проведения операций криптовалютами местоположение программных и аппаратных средств совершения преступления и преступника – не совпадают. Эти особенности необходимо учитывать при проведении и процессуальном оформлении осмотра места происшествия и места совершения преступления.

Для развития оперативно-розыскной деятельности (далее – ОРД), использование приемов, средств и методов в ходе проведения оперативно-розыскных мероприятий (далее – ОРМ) в сети «Интернет» важны оба подхода. В зависимости от информационно-телекоммуникационной среды, зависят способы совершения преступлений, а также специфика следов преступной

деятельности. Следов специфических, виртуальных, оставленных в ходе совершения компьютерного преступления¹. В связи с этим необходим выбор определенных технических средств, сил, методов получения оперативной информации в информационных сетевых массивах. ««Виртуальный след» – это система команд ЭВМ, где виртуальный объект будет являться следообразующим»². Поэтому «Интернет» имеет свою специфику совершения в его информационном пространстве преступлений, и естественно накладывает отпечаток на стратегию и тактику ОРД, которая используется с криминальными проявлениями в сети «Интернет»³.

Мы согласны с мнением Е.М. Шаповаловой «Информационные следы существуют на электронных и иных материальных носителях, наделены физическими свойствами виртуальных следов, но, в отличие от них, и конкретным информационным содержанием, в связи с чем не могут быть отнесены ни к одному из элементов традиционной классификации следов преступлений ... В то же время информационный след, представленный в отрыве от среды и первоначальной формы, уже не несет своего истинного доказательственного значения»⁴. Именно по этой причине необходимы оперативно-разыскные технологии для борьбы с преступностью в сети «Интернет».

Понятие «сетевое информационное пространство» имеет очень важное и необходимое значение для ОРД. Очевидно, что использование глобальной сети «Интернет» на современном этапе, являет собой не только прогресс и позитивные результаты в жизни общества, но и является «регрессом», так как

¹ Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. – Воронеж: Воронежск. гос. ун-т, 2001. – С. 74–76.

² Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия – Телеком, 2002. – С. 144.

³ Маркарян Э.С. Криминалистически значимые данные о механизме следообразования при расследовании преступлений, совершенных с использованием криптовалют // Библиотека криминалиста. Научный журнал. – 2017. - № 2 (31). – С. 198-206.

⁴ См.: Шаповалов Г.М. Возможность использования информационных следов в криминалистике. дис. ... канд.юрид.наук. – Владивосток, 2005

способствует появлению новых источников социальной опасности в виде проявления криминальной деятельности в информационном сетевом пространстве. «До недавнего времени интернет-преступления рассматривались только в рамках класса преступлений в сфере компьютерной информации. Сегодня Интернет принят на вооружение преступниками любых категорий, являясь не только способом (30%), но и средством совершения «традиционных» преступлений (46% – средство подготовки преступлений, 24% – средство их сокрытия), выходя таким образом за ранее обозначенные рамки»¹. В настоящее время продолжается рост преступлений с использованием сетевого пространства в «Интернете».

Проведение ОРМ в сети «Интернет» представляют собой особые условия деятельности, так как осуществляются под воздействием, во-первых, специфических свойств самого сетевого пространства, а во-вторых, специфических качеств самих сетевых компьютерных преступлений. Одно из основных специфических свойств сетевого пространства является то, что оно с одной стороны имеет привязку с помощью серверов, сетевого оборудования, каналов связи и т.д. к определенному месту, т.е. к физическому сетевому объекту. С другой стороны, сетевое пространство имеет трансграничные признаки, т.е. не имеет по сути границ какого-либо государства, они являются для глобальных сетей «Интернет» «прозрачными». Поэтому, то, что не кажется проблемой, может в нее превратиться по той причине, что «в случае совершения в сетевом пространстве преступления, как правило, можно установить физическое местонахождение преступника и жертвы, а также места сохранения следов в аппаратных устройствах сетевой инфраструктуры, однако попытка пространственно локализовать определенные информационные объекты может

¹ Введенская О.Ю. Особенности слепообразования при совершении преступления посредством сети Интернет // Юридическая наука и правоохранительная практика. – 2015. - № 4 (34). – С. 210.

остаться безрезультатной»¹. Дело в том, что в сети «Интернет» преступник имеет возможность заниматься криминальной деятельностью практически одновременно в разных операционно-вычислительных системах, при этом находясь на определенно большом расстоянии (или даже не имея физической привязки к какому-то конкретному географическому положению; используя ноутбук, смартфон) от объекта воздействия. Такое явление называется «размывание» физического места совершения преступления, с нарушением пространственной локализации.

Предпосылками к успешному расследованию преступления с использованием криптовалют в большинстве случаев будут быстрота и решительность действий следователя и оперативного сотрудника, организованное взаимодействие с различными подразделениями правоохранительных органов, а также наличие квалифицированного специалиста в области информационно-коммуникационных технологий.

Можно предположить, что самым основным ОРМ, которое может реализовываться в глобальной сети является «снятие информации с технических каналов связи» (далее – СИТКС). Поскольку основной интерес для решения задач ОРД вызывает содержание сообщений граждан, которые передаются с определенного электронного адреса на другой, либо на социальных сетях ведется переписка между лицами, то СИТКС, это основное ОРМ проводящееся в сети «Интернет». С помощью СИТКС, осуществляется «перехват» сообщений, который может быть в двух формах, как пассивной, так и активной. Если оперативным сотрудником осуществляется только отслеживание и копирование сообщений без вмешательства в их поток, это пассивный «перехват». Если же оперативным сотрудником предпринимаются действия по изменению содержания передаваемого сообщения, либо уничтожение сообщения, в результате чего оно не доходит до адресата, изменение содержания сообщения,

¹ Теория оперативно-розыскной деятельности: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Сениова. – М.: ИНФРА-М, 2016. – С. 326.

задержания сообщения (иногда пользователи «Интернета» думают на плохую работу сервера, как они отмечают: «инет глючит») то, такой «перехват» называется активным (естественно, что «активный» перехват, если пользователь сайта осведомлен об организации и тактики ОРД снижает конспиративность данного ОРМ). СИТКС ограничивает конституционные права граждан на тайну связи, поэтому осуществляется на основании судебного решения¹.

Так называемый «скайп», интернет – телефония (IP – телефония) с голосовой связью и визуальным контактом пользователей «Интернета», которая контролируется не только таким ОРМ как СИТКС, но и подпадает под технологию такого ОРМ, как «прослушивание телефонных переговоров» (ПТП). Данное ОРМ, является мероприятием судебного санкционирования.

Иногда возникает потребность в целях решения задач ОРД получить доступ к информации, которая содержится в компьютерах разрабатываемых лиц. Данная процедура осуществляется в тайне от «разрабатываемых» в процессе дистанционного негласного обследования содержания их компьютера, в тот момент, когда он подключен к «Интернету», сотрудниками оперативного подразделения (как правило УСТМ – управления специальных технических мероприятий ФСБ) через сетевой узел в компьютерной сети, построенной по протоколу.

В том случае, когда в ходе обследования содержания информации в компьютере, производится копирования информации (файлы, содержащие тексты документов, фото, видео изображения, интернет-адреса и т. п.) для последующего ее изучения, в этом случае можно говорить о таком ОРМ, как «сбор образцов для сравнительного исследования» и «исследование предметов и документов».

¹ Маркарян Э.С. Криминалистически значимые данные о механизме слепообразования при расследовании преступлений, совершенных с использованием криптовалют // Библиотека криминалиста. Научный журнал. – 2017. - № 2 (31). – С. 198-206.

Самым простым ОРМ, которое можно провести в сети «Интернет» – это «опрос», при проведении которого, оперативный сотрудник, в зависимости от обстоятельств, может не скрывать свою принадлежность к оперативным органам, а может использовать механизм зашифровки как целей опроса, так и своего профессионального отношения к оперативному подразделению.

Используя персональные страницы пользователей (разрабатываемых) в социальных сетях (Одноклассники, ВКонтакте и др.) и имеющимся там же биографическим данным возможно проведение такого ОРМ, как «отождествление личности». Отметим, что технология и правила проведения ОРМ «отождествление личности» отличается от следственного действия «предъявление для опознания», в связи с чем возможно проведение указанного ОРМ по таким признакам, как особенности стилистики общения в «Интернете», особенности орфографии лица при обмене сообщениями, интеллектуальные способности лица, знания им определенных обстоятельств и фактов, которые прослеживаются в процессе изучения сообщений и т.п.

То обстоятельство, что в «интернете» имеют место эффективные справочно-информационные системы, это способствует проведение в сети такого ОРМ, как «наведения справок», путем непосредственного изучения различных документов на сайтах сети (запросов по электронной почте в различные организации об интересующих сведениях).

В сети «Интернет» возможно такое ОРМ, как «наблюдение», которое, во-первых, направлено на негласное изучение преступных проявлений лиц в сетевом общении с применением электронных средств, а во-вторых электронное наблюдение за самим разрабатываемым через веб-камеру в ноутбуке или компьютере (через вход узла IP – адреса), на обстановку в его комнате, нахождение в ней определенных вещей, его внешний вид и возможное поведение.

В определенном объеме в сети «Интернет» возможно проведение такого ОРМ, как «контроль почтовых отправлений, телеграфных и иных сообщений».

Конечно методы контроля почтовой корреспонденции, связанной с «Почтой России», отличаются от контроля сообщений на «электронной почте» в сети «Интернет». Тем не менее данное ОРМ, позволяет не только контролировать электронные сообщения, но и в определенных случаях создавать препятствия для обмена сообщениями между разрабатываемыми лицами (лицом).

В связи с большим массивом операций в сфере торговли, проходящих через «Интернет», возможно проведение таких ОРМ, как «контролируемая поставка» и «проверочная закупка». Цель проведения данных ОРМ выявления преступления в сфере торговли в сети «Интернет» (мошенничество со стороны интернет-магазинов), а также пресечение распространения запрещенных к обороту товаров (порнографию с участием несовершеннолетних, наркотических средств, оружия, взрывных устройств и т.д.). Одно из сложных ОРМ, которое можно провести в сети «Интернет» – это «оперативный эксперимент», осуществление которого связано с искусственно созданным в сети, негласно контролируемого объекта. Данные искусственно созданные объекты должны представлять интерес для криминального мира, т.е. это могут быть, как уже выше указано, сайты «ловушки», «приманки». При создании «ловушек», «приманок», естественно используются названия, например, экстремистского характера (возможно со скрытой информации в названии) «Музыка для белых», «Национализм наш путь развития», «Россия для русских» и т.д. В ходе использования сайтов «ловушек» оперативными подразделениями ФСБ и их сотрудниками применяется «легендированная» переписка в сети «Интернет», где они создают условия доверительного общения, с целью выявления у разрабатываемого преступных намерений (очень часто в социальных сетях, например «Одноклассники» в различных «статусах», «комментариях», «форумах», можно прочесть просьбы и требования пользователей к провайдером убрать сайты «экстремистского» содержания, которые на самом деле установлены ФСБ РФ).

Самым сложным ОРМ, на наш взгляд, является – «оперативное внедрение», содержанием которого является легендированный ввод оперативного сотрудника или лиц оказывающих конфиденциальное содействие субъектам, осуществляющим ОРД в криминальную среду. Вся сущность оперативного внедрения сводится к приобретению лиц, из разрабатываемых, способных оказывать конфиденциальное содействие оперативным подразделениям МВД, ФСБ. Местом подбора конфиденциальных источников рассматриваются места общения в сети «Интернет» (сайты, форумы, чаты). Следует заметить, что большинство таких мест в сети, носит «закрытый» характер и ни каждый желающий может получить туда доступ. Вот почему автор выше указывал на то, что оперативному сотруднику желательно иметь конфиденнта из числа хакеров. Которые, находясь на стороне криминалитета, предпринимают меры против оперативного внедрения со стороны МВД, ФСБ. Если же хакер, является конфидентом субъектов осуществляющих ОРД, то в этом случае, он наоборот будет способствовать внедрению оперативного сотрудника в сетевую криминальную среду.

Развитие современных технологий и социальных отношений с помощью «Интернета» предоставило спецслужбам уникальную возможность решать вопросы и принимать меры уголовно-правового характера по противодействию и профилактике преступлений. Учитывая то, что повсеместно, происходит внедрение «Интернета» во все сферы человеческой жизни, автор убежден, что проблема преступности в сети «Интернет», носит экзистенциальный характер и является элементом информационной безопасности государства. Оперативно-розыскные технологии являются, необходимым условием для успешной борьбы с преступностью в глобальной сети «Интернет».

ЗАКЛЮЧЕНИЕ

В заключении проведенного исследования можно сделать следующие выводы.

Заявления о том, что биткоин надо регулировать из-за отмывания денег и финансирования терроризма появляются в медиа-пространстве с завидной регулярностью несмотря на то, что некоторые учреждения вроде Европола или британского министерства финансов, которые едва ли можно заподозрить в нежных чувствах к криптовалюте, утверждают, что существует очень мало доказательств того, что подобное происходило хоть раз. «Очень мало доказательств» на дипломатическом языке, вероятно, означает «вообще ни одного доказательства» и просто учитывает некоторые другие связанные с биткоином преступления, не обо всех из которых может быть известно.

Тем не менее, хотя террористы и не пользуются биткоином для финансирования своей деятельности, а коварные бизнесмены биткоином предпочитают всяческие офшоры, было бы нечестно утверждать, что биткоин никак не связан с преступностью. Известны многочисленные случаи, когда криптовалюта оказывалась в самом центре преступных схем.

Кроме того, существуют определенные особенности, связанные с процессом расследования преступлений, совершаемых с помощью электронных платежных систем на основе криптографии. Одной из таких особенностей является наличие так называемых «виртуальных» следов. Это связано с тем, что все расчеты при работе с сетью Bitcoin осуществляются с использованием компьютера или иного аппаратного средства и подключения к глобальной сети Интернет. Необходимо учитывать данные особенности при проведении отдельных следственных действий. Следовательно, для проведения качественного расследования необходимо владеть не только знаниями компьютерной технологии, но и знанием механизма функционирования сети Bitcoin.

При расследовании преступлений, совершенных с использованием криптовалют востребованы сведения о самой платежной системе, криптовалюте, порядке регистрации и использовании электронного кошелька, обороте, порядке осуществления транзакций, порядке регистрации и использования электронного кошелька и т. д. При этом большое значение имеет наличие или отсутствие возможности обмена криптовалют на другие криптовалюты или наличные деньги. Событие преступления, совершаемого с использованием криптовалют, имеет особенности, связанные со спецификой таких его существенных элементов, подлежащих установлению по уголовному делу, как место и время совершения преступления.

В рассматриваемых преступлениях большое значение имеет именно местоположение преступника и используемых им программных и аппаратных средств совершения преступления. Нередко в силу особенностей проведения операций с криптовалютами местоположение программных и аппаратных средств совершения преступления и преступника – не совпадают. Эти особенности необходимо учитывать при проведении и процессуальном оформлении осмотра места происшествия и места совершения преступления.

Поскольку преступления рассматриваемой категории всегда совершаются с использованием аппаратно-программных средств, то типичные черты личности будут в целом такими же, как и у лиц, совершающих преступления в сфере информационно-коммуникационных технологий, не связанных с криптовалютой.

Предпосылками к успешному расследованию преступления с использованием криптовалют в большинстве случаев будут быстрота и решительность действий следователя и оперативного сотрудника, организованное взаимодействие с различными подразделениями правоохранительных органов, а также наличие квалифицированного специалиста в области информационно-коммуникационных технологий.

В действующем отечественном законодательстве в настоящее время отсутствуют нормы, регулирующие общественные отношения, связанные с оборотом виртуальных денег, а также с созданием и функционированием соответствующих платежных систем. В связи с чем, правоохранительные органы оказались не в полной мере готовы эффективно противостоять новым видам преступных посягательств, связанных с оборотом виртуальных денег.

Раскрытие и расследование преступлений выделенного вида остается довольно сложной задачей для большинства сотрудников органов предварительного расследования. Это обусловлено следующими факторами:

1) отсутствием обобщений материалов следственной и судебной практики;

2) отсутствием методических рекомендаций по организации раскрытия и расследования выделенных преступных посягательств;

3) отсутствием опыта работы у следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в виде электронных сообщений и документов, страниц и сайтов сети Интернет;

4) недостаточным уровнем подготовки специалистов соответствующего профиля в высших учебных заведениях, которых в соответствии с действующим уголовно-процессуальным законодательством в обязательном порядке необходимо привлекать для участия в следственных действиях¹;

5) недоступностью компетентных специалистов в области работы с компьютерной информацией и ее электронными носителями для подавляющего числа сотрудников органов предварительного расследования.

¹ См.: Вехов В.Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения. – 2016. – № 1. – С. 155-158; Вехов В.Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. – 2013. – № 10. – С. 22-24.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

а) законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ) // Российская газета. - № 237. – 25.12.1993.
2. Гражданский кодекс Российской Федерации (часть первая): Федеральный закон Российской Федерации от 30 ноября 1994 г. № 51-ФЗ (в ред. от 3 августа 2018 г.) // Собрание законодательства РФ. – 05.12.1994. - № 32. – Ст. 3301.
3. Уголовный кодекс Российской Федерации: Федеральный закон Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 17 июня 2019 г.) // Собрание законодательства РФ. – 17.06.1996. - № 25. – Ст. 2954.
4. О Центральном банке Российской Федерации (Банке России): Федеральный закон Российской Федерации от 10 июля 2002 г. № 86-ФЗ (в ред. от 6 июня 2019 г.) // Собрание законодательства РФ. – 15.07.2002. - № 28. – Ст. 2790.
5. Информация Банка России от 27.01.2014 г. «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» // Вестник Банка России. - № 11. – 05.02.2014.
6. Информация Банка России от 04.09.2017 г. «Об использовании частных «виртуальных валют» (криптовалют)» // Вестник Банка России. - № 80. – 14.09.2017.

б) монографии, учебники, учебные пособия

1. Иванцов С.В. Преступления на рынке ценных бумаг: криминологическая характеристика и предупреждение / С.В. Иванцов, С.В. Новиков. – М.: Юнити-Дана, 2012. – 119 с.
2. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – М.: Горячая линия – Телеком, 2002. – 336 с.
3. Крылов О.М. Правовое регулирование денежного обращения в Российской Федерации / О.М. Крылов. – М.: Контракт, 2014. – 104 с.
4. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ / В.А. Мещерякова. – Воронеж: Воронежск. гос. ун-т, 2001. – 176 с.
5. Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты / В.А. Перов. – М.: Юрлитинформ, 2017. – 197 с.
6. Теория оперативно-розыскной деятельности: учебник / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Сенинова. – М.: ИНФРА-М, 2016. – 712 с.

в) статьи, научные публикации

1. Адигамова Г.З. Проблемы раскрытия и расследования экономических преступлений в сфере жилищно-коммунального хозяйства на основе бухгалтерской информации / Г.З. Адигамова, О.И. Канищева // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. – 2016. - № 19-2. – С. 53-56.
2. Анцеров Р.С. Регулирование криптовалют в современной информационной экономике / Р.С. Анциферов / В сборнике: «Государство и рынок в условиях глобализации мирового экономического пространства». Сборник статей по

- итогам Международной научно-практической конференции. – 2018. – С. 11-14.
3. Архипов В.В. Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр / В.В. Архипов // Закон. – 2014. – № 9. – С. 69-90.
 4. Асланян Р.Г. Понятие и признаки информации как предмета преступлений в сфере экономической деятельности / Р.Г. Асланян // Библиотека уголовного права и криминологии. – 2016. - № 1 (13). – С. 7-9.
 5. Булгаков И.Т. Правовые вопросы использования технологии блокчейн / И.Т. Булгаков // Закон. – 2016. – № 12. – С. 82-90.
 6. Введенская О.Ю. Особенности слепообразования при совершении преступления посредством сети Интернет / О.Ю. Введенская // Юридическая наука и правоохранительная практика. – 2015. - № 4 (34). – С. 209-216.
 7. Вехов В.Б. Понятие, виды и особенности фиксации электронных доказательств / В.Б. Вехов // Расследование преступлений: проблемы и пути их решения. – 2016. – № 1. – С. 155-158.
 8. Вехов В.Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства / В.Б. Вехов // Российский следователь. – 2013. – № 10. – С. 22-24.
 9. Герман Т.В. Личность преступника как элемент криминалистической характеристики преступлений в сфере компьютерной информации / Т.В. Герман // Юридическая наука и практика: традиции и новации Сборник статей Международной научно-практической конференции. – 2016. – С. 32-36.
 10. Дудин М.Н. Использование криптовалюты в незаконных целях: обеспечение финансово-экономической безопасности // Проблемы рыночной экономики / М.Н. Дудин, Н.В. Лясников. – 2018. - № 3. – С. 16-23.

11. Иванцов С.В. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С.В. Иванцов и др. // Всероссийский криминологический журнал. – 2019. – Т. 13, № 1. – С. 85-93.
12. Козлова Н. Обман валют / Н. Козлов // Российская газета. – 2017. - № 6874 (6).
13. Ларина Е. Криптовалюта: свет и тени / Е. Ларина, В. Овчинский // Наш современник. – 2018. – № 8. – С. 224-228.
14. Лясников Н.В. Менеджмент в XXI веке: сущность, проблемы и задачи / Н.В. Лясников, М.Н. Дудин // Путеводитель предпринимателя. – 2010. - № 8. – С. 83-92.
15. Мамаева Л.Н. Безопасность финансовой системы в рамках появления криптовалюты / Л.Н. Мамаева, В.А. Лазарева, К.С. Рыбакова, М.В. Кирюхина // Экономическая безопасность и качество. – 2018. – № 1 (30). – С. 53-56.
16. Маркарян Э.С. Криминалистически значимые данные о механизме слепообразования при расследовании преступлений, совершенных с использованием криптовалют / Э.С. Маркарян // Библиотека криминалиста. Научный журнал. – 2017. - № 2 (31). – С. 198-206.
17. Маркарян Э.С. Особенности получения данных о механизме слепообразования при расследовании преступлений, совершенных с использованием криптовалют / Э.С. Маркарян // Библиотека криминалиста. Научный журнал. – 2017. - № 4 (33). – С. 176-187.
18. Матюшенко В.А. Общая характеристика преступлений сфере компьютерной информации / В.А. Матюшенко // Крымские юридические чтения материалы научно-практической студенческой конференции. Академия Генеральной прокуратуры Российской Федерации, Крымский юридический институт. 2016. – С. 405-408.
19. Миценко У.Н. Криптовалюта как потенциальная угроза финансовой безопасности Российской Федерации / У.Н. Миценко, Е.В. Тутинас / В

- сборнике: «Стратегия развития российско-абхазских отношений в рамках построения межгосударственной программы национальной безопасности». Материалы международной научно-практической конференции. – 2017. – С. 247-250.
20. Рудик М.В. Несовершеннолетний как субъект преступлений в сфере компьютерной информации / М.В. Рудик, С.А. Торопов // Евразийский юридический журнал. – 2016. - № 3 (94). – С. 222-246.
 21. Савинский С.П. Криптовалюты и их нормативно-правовое регулирование в КНР / С.П. Савинский // Деньги и кредит. – 2017. - № 7. – С. 65-67.
 22. Сидоренко Э.Л. Криминологические риски оборота криптовалюты / Э.Л. Сидоренко // Экономика. Налоги. Право. – 2017. – Т. 10, № 6. – С. 147-154.
 23. Сидоренко Э.Л. Криптовалюта как новый юридический феномен / Э.Л. Сидоренко // Общество и право. – 2016. – № 3 (57). – С. 193-197.
 24. Сидоренко Э.Л. Наркопреступность в сети «Интернет»: современные криминологические тренды / Э.Л. Сидоренко // Наркоконтроль. – 2018. – № 4. – С. 13-18.
 25. Сидоренко Э.Л. Токенизация угольной промышленности: экономические и криминологические риски / Э.Л. Сидоренко, В.К. Шайдуллина, С.А. Киракосян // Уголь. – 2018. – № 12. – С. 54-59.
 26. Сокол В.Ю. Научоведческие проблемы криминалистики / В.Ю. Сокол // Общество и право. – 2008. - № 1. – С. 17-18.
 27. Спасенников Б.А. Актуальные проблемы уголовного права: обзор литературы / Б.А. Спасенков // Актуальные вопросы образования и науки. – 2015. – № 1-2 (47-48). – С. 36-38.
 28. Степанова Д.И. Особенности организации и направления развития криптовалютных платежных систем / Д.И. Степанова, Т.Е. Николаева, Н.В. Иволгина Н.В. // Финансы и кредит. – 2016. - № 10 (682). – С. 33-45.
 29. Сухаренко А. Суррогаты вредные? / А. Сухаренко // Юрист. – 2015. - № 41. – С. 21-24.

30. Суходолов А.П. 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.
31. Фетисов В.Д. Проблемы использования bitcoin и экономическая безопасность России / В.Д. Фетисов, Т.В. Фетисова Т.В. // Национальные интересы: приоритеты и безопасность. – 2018. – Т. 14. - № 3 (360). – С. 452-464.
32. Фомин А.Н. Криптовалюты в цифровой экономике: финансово-экономические аргументы «за» и «против». Аналитический доклад / А.Н. Фомин. – М., 2017. – 5с.
33. Шаповалов Г.М. Возможность использования информационных следов в криминалистике: дис. ... канд. юрид. наук / Г.М. Шаповалов. – Владивосток, 2005. – 210 с.
34. Юрьева А.А. Развитие информационного общества как условие формирования инновационной экономики / А.А. Юрьева// Проблемы рыночной экономики. – 2016. - № 3. – С. 14-20.

г) эмпирические материалы (материалы судебной, следственной практики и т.д.)

1. Обзор судебной практики Верховного Суда Российской Федерации № 2 (2018) (утв. Президиумом Верховного Суда РФ 04.07.2018 г.) // Бюллетень Верховного Суда РФ. - № 3. – март, 2019.
2. Апелляционное определение Ульяновского областного суда от 31.07.2018 г. по делу № 33-3142/2018 // СПС «КонсультантПлюс».
3. Апелляционное определение Санкт-Петербургского городского суда от 04.06.2018 г. № 33а-12820/2018 по делу № 2-10119/2016 // СПС «КонсультантПлюс».

4. Апелляционное определение Свердловского областного суда от 08.11.2018 г. по делу № 33а-19381/2018 // СПС «КонсультантПлюс».

д) Электронные ресурсы сети Интернет

1. Внесение законопроекта о запрете криптовалют в России откладывается [Электронный ресурс] // ForkLog. – 21.04.2016. Режим доступа: <https://forklog.com/vneseniezakonoproekta-o-zaprete-kriptoalyut-v-rossii-otkladyvaetsya/> (дата обращения: 25.05.2019).
2. Вахрушев Д.С. Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления / Д.С. Вахрушев, О.С. Железов // Наукоедение. – 2014. – Вып. 5(24). – Режим доступа: <http://naukovedenie.ru/PDF/127EVN514.pdf/> (дата обращения: 15.05.2019).
3. Информационное сообщение Росфинмониторинга «Об использовании криптовалют» // URL: <http://www.fedsfm.ru/news/957> (дата обращения: 18.06.2019).
4. Гурьева М. Блокчейн-экономика: тренды и перспективы [Электронный ресурс]. – Режим доступа: <https://te-st.ru/wp-content/uploads/2017/04/Marina-Gureva.pdf> (дата обращения: 15.05.2019).
5. Законопроект об ответственности за использование криптовалют поступит в Госдуму в июне [Электронный ресурс] // ForkLog. – 25.02.2016. – Режим доступа: <https://forklog.com/zakonoproekt-ob-otvetstvennosti-za-ispolzovanie-kriptoalyut-postupit-v-gosdumu-v-iyune/> (дата обращения: 18.06.2019).
6. Минфин отложил подготовку закона о запрете Bitcoinов [Электронный ресурс] // Lenta.ru. – Режим доступа: <https://lenta.ru/news/2016/10/11/minfinbitcoin/> (дата обращения: 18.06.2019).
7. Об использовании при совершении сделок «виртуальных валют», в частности, Bitcoin [Электронный ресурс] // Центральный банк Российской Федерации. – Режим доступа:

- http://www.cbr.ru/press/PR/?file=27012014_1825052.htm (дата обращения: 15.05.2019).
8. Правительство РФ подготовит новый вариант законопроекта о запрете криптовалют [Электронный ресурс] // ForkLog. — Режим доступа: <https://forklog.com/pravitelstvo-rfpodgotovit-novyy-variant-zakonoproekta-o-zaprete-kriptovalyut/> (дата обращения: 18.06.2019).
 9. Правовое регулирование криптовалютного бизнеса [Электронный ресурс]. — Режим доступа: <http://axon.partners/wp-content/uploads/2017/02/Global-Issues-of-Bitcoin-BusinessesRegulation.pdf> (дата обращения: 15.05.2019).
 10. Путин: криптовалюты – это возможность отмывания, ухода от налогов и финансирования терроризма [Электронный ресурс] // Коммерсантъ. <https://www.kommersant.ru/doc/3435054> (дата обращения: 18.06.2019).
 11. Росфинмониторинг: Законопроект о запрете криптовалют придется пересматривать [Электронный ресурс] // ForkLog. — 26.04.2016. — <https://forklog.com/rosfinmonitoringzakonoproekt-o-zaprete-kriptovalyut-bridetsya-peresmatrivat/> (дата обращения: 25.05.2019).
 12. Рынок криптовалют вырос в полтора раза с начала 2017 года. — [Электронный ресурс] — Режим доступа: <http://forklog.com/rynok-kriptovalyut-vyros-v-poltora-raza-s-nachala-2017-goda> (дата обращения: 15.05.2019).
 13. ЦБ не исключает будущего у bitcoin в России [Электронный ресурс] // Прайм. — 02.07.2014. — Режим доступа: <http://1prime.ru/finance/20140702/787649971.html> (дата обращения: 25.05.2019).