МОСКОВСКАЯ АКАДЕМИЯ СЛЕДСТВЕННОГО КОМИТЕТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

На правах рукописи

Перов Валерий Александрович

КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Специальность 5.1.4. Уголовно-правовые науки

Диссертация
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, доцент
Ермолович Ярослав Николаевич

Москва − 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Криптовалюта – одна из разновидностей цифровой валюты, которая появилась в 2009 году и получила постепенное распространение в мире с помощью так называемой блокчейн-технологии, то есть технологии, основанной на криптографическом построении цепочек замкнутых информационных блоков в децентрализованной системе данных.

Правовой режим криптовалюты в разных странах мира неоднороден, а в некоторых вообще не определен, что приводит к правовым коллизиям, в том числе при квалификации преступлений, совершенных с ее использованием. Ситуация осложняется ещё и тем, что такого рода преступления могут совершаться на территории нескольких государств, в которых криптовалюта имеет различный правовой режим. Кроме того, отсутствует единый подход к определению стоимости отдельных видов криптовалют.

В законодательстве Российской Федерации правовой режим криптовалюты изменялся и до настоящего времени четко не определен. Указанные обстоятельства приводят не только к ошибкам в квалификации преступлений, совершенных с использованием криптовалюты в разные периоды времени, но и к невозможности определения точной суммы имущественного ущерба, причиненного такими преступлениями.

Согласно данным Генеральной прокуратуры Российской Федерации, в 2020–2022 гг. на деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приходится одно из четырех регистрируемых преступлений. За последние пять лет число таких преступлений увеличилось более чем в 11 раз, и их удельный вес в структуре преступности возрос с 1,8 % до 25 %. Большинство так называемых «киберпреступлений» совершается с использованием сети

Интернет (300,3 тыс. – в 2022 г.) либо при помощи средств мобильной связи (218,7 тыс. – в 2022 г.)[1].

Приведенные статистические и аналитические данные свидетельствуют о том, что количество преступлений в сфере высоких технологий, к которым относятся и преступления с использованием криптовалюты, неуклонно возрастает, что требует правильной их квалификации. Кроме того, используемый законодателем и правоприменителем понятийный аппарат нуждается в уточнении и унификации, без чего единообразная квалификация преступлений, совершаемых с использованием криптовалюты, и эффективное противодействие указанным преступлениям не представляются возможными.

Всё это обусловливает необходимость научного обоснования проблем, связанных с квалификацией преступлений, совершаемых с использованием криптовалюты, создание научно обоснованной методики расследования таких преступлений и обучение следователей Следственного комитета Российской Федерации ее использованию.

Степень научной разработанности темы исследования. В Российской Федерации исследованием проблем цифровой валюты, киберпреступности или преступлений в сфере высоких технологий, в том числе и проблем квалификации преступлений, совершенных с использованием криптовалюты, занимался ряд ученых[2]. Уголовно-правовые, криминологические,

---

[1] Состояние преступности в России (2020–2022 гг.). М., 2022. С. 7.

[2] См., напр.: Хисамова З.И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: автореф. дис. ... канд. юрид. наук. Краснодар, 2016. 32 с.; Дюдикова Е.И. Перспективы развития электронных денег как элемента национальной платежной системы Российской Федерации: автореф. дис. ... канд. экономич. наук. Ставрополь, 2017. 27 с.; Летёлкин Н.В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет»: автореф. дис. ... канд. юрид. наук. Нижний Новгород, 2018. 24 с.; Бадамшин С.К. Преступления террористической направленности, совершаемые с использованием электронных или информационно-телекоммуникационных сетей: уголовно-правовая и криминологическая характеристика: дис. ... канд. юрид. наук. М., 2018. 275 с.; Фролов М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук. М., 2019. 26 с.; Соловьева Е.А. Преступления, совершаемые в платежных системах: автореф. дис. ... канд. юрид. наук. Саратов, 2019. 33 с.; Немова М.И. Альтернативные средства

криминалистические, уголовно-процессуальные проблемы борьбы с преступностью в сфере высоких технологий исследовались А.И. Бастрыкиным, А.А. Бессоновым, А.И. Бойцовым, А.В. Бриллиантовым, Е.Г. Быковой, Л.В. Бертовским, С.К. Бадамшиным, А.Г. Волеводзом, Б.В. Волженкиным, Я.Ю. Васильевой, В.Г. Голубевым, О.С. Гузеевой, Г.Р. Григоряном, М.С. Дашяном, Д.В. Добровольским, М.М. Долгиевой, Е.И. Дюдиковой, И.И. Кучеровым, И.А. Клепицким, Н.Н. Ковалевой, А.Н. Копырюлиной, А.А. Коренной, Т.А. Купцовой, Н.В. Летёлкиным, Т.М. Лопатиной, А.А. Лебедевой, И.И. Малыгиным, И.С. Мочалкиной, М.И. Немовой, К.В. Ображиевым, Н.И. Пикуровым, Т.В. Пинкевич, Е.А. Русскевичем, В.Г. Степановым-Егиянцом, Э.Л. Сидоренко, Е.А. Соловьевой, А.В. Токоловым, А.В. Федоровым, М.Д. Фроловым, З.И. Хисамовой и другими. Не преуменьшая научную значимость работ названных ученых, необходимо отметить, что многие из их трудов утратили актуальность ввиду внесения многочисленных изменений в уголовное законодательство, что поставило новые вопросы перед юридической наукой.

Объектом исследования выступают общественные отношения, складывающиеся в сфере уголовно-правового противодействия совершению преступлений с использованием криптовалюты.

Предметом диссертационного исследования является уголовное и гражданское законодательство, а также законодательство о валютном

расчёта как предмет и средство совершения преступлений в сфере экономики: дис. ... канд. юрид. наук. М., 2020. 236 с.; Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... докт. юрид. наук. М., 2020. 521 с.; Григорян Г.Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: автореф. дис. ... канд. юрид. наук. Самара, 2021. 23 с.; Мочалкина И.С. Цифровые права и цифровая валюта как предмет преступлений в сфере экономики: дис. ... канд. юрид. наук. М., 2022. 240 с., Купцова Т.А. Функционирование денежных суррогатов в форме криптовалюты в системе современных экономических отношений: автореф. дис. ... канд. экономич. наук. Самара, 2022. 22 с.; Токолов А.В. Правовое регулирование информационных отношений в сфере оборота цифровых финансовых активов: автореф. дис. ... канд. юрид. наук. М., 2022. 21 с.; и др.

регулировании и валютном контроле, научные представления, образующие теоретико-правовую основу уголовно-правового противодействия совершению преступлений с использованием криптовалюты, а также практика деятельности следственных органов СК России, российских судов, Центрального банка России в рассматриваемой сфере.

Целью диссертационного исследования является разработка правил квалификации преступлений, совершенных с использованием криптовалюты, а также определение основных направлений совершенствования законодательства об уголовной ответственности за совершение преступлений с использованием криптовалюты.

Для достижения указанной цели были поставлены и решены следующие **задачи**:

1. Исследовать правовую природу криптовалюты в системе национального законодательства Российской Федерации, научно обосновав понятийный аппарат, путем выделения ключевых отличительных признаков криптовалюты от других объектов права.

2. Проанализировать статистические данные о количестве, видах и способах совершения преступлений с использованием криптовалюты в Российской Федерации. Определить соотношение указанных показателей с общемировыми тенденциями, выявив наиболее характерные способы совершения таких преступлений, разработать комплекс мер уголовно-правового противодействия указанным преступлениям.

3. Выявить социальную обусловленность уголовно-правовой охраны общественных отношений, связанных с оборотом криптовалют различного вида.

4. Обосновать возможность признания криптовалюты в качестве предмета преступления.

5. Выявить особенности правового режима криптовалют различного вида как предмета и средства совершения преступления.

6. Определить основные тенденции развития уголовного законодательства, направленного на защиту прав и законных интересов добросовестных участников криптовалютного рынка.

Научная новизна исследования заключается в том, что в работе доказана необходимость повышения эффективности уголовно-правового регулирования общественных отношений, возникающих в связи с совершением преступлений с использованием криптовалют, и определены его пути и средства.

На основании анализа судебной практики и данных судебной статистики о преступлениях, совершенных с использованием криптовалюты, выявлены факторы, детерминирующие социальную обусловленность уголовно-правовой охраны общественных отношений, связанных с оборотом криптовалют различного вида, с учетом которых оптимизирован алгоритм квалификации преступлений, совершенных с использованием криптовалюты, и доказана его эффективность.

Впервые определен понятийный аппарат, характеризующий отдельные признаки составов преступлений, совершенных с использованием криптовалюты.

Доказана эффективность применения предложенных автором параметров определения стоимостных критериев общественно опасных последствий совершения преступлений с использованием криптовалют.

Проведен анализ целесообразности применения методики квалификации преступлений, совершенных с использованием криптовалют, а также доказано, что ее применение повышает эффективность уголовно-правового противодействия совершению преступлений с использованием криптовалюты.

Теоретическая и практическая значимость работы. Совокупность теоретических положений, разработанных в диссертации на основании выполненного автором исследования, является решением научной задачи обоснования необходимости повышения эффективности уголовно-правового

противодействия совершению преступлений с использованием криптовалюты.

Теоретическая значимость работы также определяется разработкой положений о криптовалюте как предмете и средстве совершения преступлений, суррогатном средстве платежа при совершении определенных преступлений, научной классификации преступлений, совершенных с использованием криптовалюты, позволяющей обосновать методологические подходы к изучению преступности и преступлений, совершенных с использованием криптовалюты, правил их квалификации.

Практическая значимость работы заключается в возможности использования ее результатов в решении задач, возникающих в правотворческой деятельности органов государственной власти и правоприменительной деятельности, выработке рекомендаций по совершенствованию уголовного законодательства.

Положения, выводы и рекомендации диссертации могут быть использованы в правоприменительной деятельности судов и следственных органов СК России, правотворческой деятельности органов государственной власти, а также в процессе преподавания курса «Уголовное право», при реализации дополнительных профессиональных программ – программ повышения квалификации в образовательных организациях СК России.

Методология и методы исследования. В процессе разработки теоретических и научно-прикладных положений, решения поставленных задач автор руководствовался философской теорией диалектического познания действительности, а также комплексом научных методов познания правовых явлений и процессов: такими общенаучными методами, как анализ, синтез, дедукция, индукция, обобщение, а также такими частными научными методами познания социально-правовых явлений, как конкретно-исторический и юридико-догматический.

В качестве **эмпирической базы** исследования были использованы: обзоры и справки Судебной коллегии по уголовным делам Верховного Суда

Российской Федерации, Генеральной прокуратуры, Следственного комитета Российской Федерации, данные судебной статистики, материалы судебной и следственной практики, в том числе материалы 200 архивных уголовных дел, расследованных в 2017–2022 гг. следственными органами СК России. Такое количество изученных уголовных дел с учетом требований статистической методологии исследования достаточно для выработки обоснованных выводов.

Кроме того, эмпирическую базу исследования составляют результаты социологического опроса методом анкетирования по актуальным вопросам уголовно-правового обеспечения следственной деятельности Следственного комитета Российской Федерации, проведенного автором среди сотрудников следственных подразделений Следственного комитета Российской Федерации. Автором проведено социологическое исследование методом анкетирования по актуальным вопросам уголовно-правового противодействия совершению преступлений с использованием криптовалюты, в ходе которого были опрошены 100 следователей Следственного комитета Российской Федерации, что с учетом генеральной совокупности – общего числа следователей СК России и величины допустимой ошибки – обеспечивает достоверность полученных результатов.

Теоретическую основу исследования составляют научные труды российских и зарубежных ученых в области правового регулирования криптовалют и уголовной ответственности за преступления, совершаемые с использованием криптовалют, специальная литература в области философии, общей теории права, конституционного, уголовного, гражданского права и информатики.

Положения, выносимые на защиту:

1. Автором разработан и научно обоснован понятийный аппарат, характеризующий отдельные признаки составов преступлений, совершенных с использованием криптовалюты, необходимый для квалификации рассматриваемых преступлений:

– авторское определение криптовалюты, в качестве которой в сфере уголовно-правового регулирования предлагается рассматривать результат процесса информатизации и взаимодействия субъектов информационной инфраструктуры, использующей математический код и криптографические элементы. Криптовалюта рассматривается в качестве разновидности цифровой валюты, то есть особой разновидности электронного платёжного средства, обязательным местом оборота которого является информационная система. В зависимости от способа совершения преступления криптовалюта выступает в качестве предмета или средства совершения преступления;

– авторское определение технологии блокчейн, понимаемой для целей уголовного права как децентрализованный реестр данных, позволяющий осуществлять криптовалютный оборот в виртуальном пространстве, в том числе и для совершения преступлений в виртуальном пространстве, являющийся в рамках рассматриваемых правоотношений средством совершения преступлений с использованием криптовалюты.

2. Автором предлагается местом совершения преступления с использованием криптовалюты (с учетом того, что такое преступление будет считаться оконченным с момента закрытия блока в децентрализованном реестре) считать географически определенную точку в пространстве, обозначающую место использования преступником компьютерного оборудования.

3. Авторская классификация преступлений с использованием криптовалюты основывается на характере совершенного преступления, в соответствии с которой криптовалюта может быть:

1) предметом хищений (ст. ст. 158, 158.1, 159, 159.6, 160, 161, 162 УК РФ);

2) предметом оказания противоправного влияния на результат официального спортивного соревнования или зрелищного коммерческого конкурса, взятки, коммерческого подкупа либо подкупа в сфере закупок товаров, работ, услуг для обеспечения государственных или муниципальных

нужд, а равно провокации этих преступлений, а также совершения иных преступлений, сопряженных с подкупом (ст. ст. 110.1, 141, 142, 183, 184, 200.5, 200.7, 204, 204.1, 204.2, 290, 291, 291.1, 291.2, 304, 309 УК РФ);

3) предметом легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем, а также приобретения или сбыта имущества, заведомо добытого преступным путем (ст. ст. 174, 174.1, 175 УК РФ);

4) средством финансирования незаконной деятельности (ст. ст. 205.1, 208, 212, 281.1, 282.3, 359, 361 УК РФ);

5) средством совершения других преступлений против личности, общественной безопасности и т. д. в качестве суррогатного средства платежа (ст. ст. 105, 111, 117, 206, 222, 222.1, 222.2, 228.1, 228.4 УК РФ и др.).

4. Выявлены основные детерминанты, повышающие латентность преступлений, совершенных с использованием криптовалюты:

– возможность извлечения в виртуальном пространстве при совершении преступлений с использованием криптовалюты незаконного дохода при невысоком риске привлечения к уголовной ответственности;

– низкий уровень осведомлённости в области информационной безопасности у пользователей блокчейн-сетей;

– анонимность пользователей, позволяющая осуществлять обезличенные транзакции в блокчейн-сетях.

5. Предлагается авторский подход к определению стоимостных критериев признаков состава преступлений, совершенных с использованием криптовалюты, а именно: экономическая соразмерность количественных параметров крупного и особо крупного ущерба, дохода или размера преступной деятельности, устанавливаемой для каждой группы таких преступлений в зависимости от вида охраняемой сферы общественных отношений (непосредственного объекта преступления) и определенных экономических показателей ценообразования и доходности.

6. Автором разработаны законодательные меры противодействия преступлениям, совершаемым с использованием криптовалюты:

Автором разработаны законодательные меры противодействия преступлениям, совершаемым с использованием криптовалюты:

1. Обоснована необходимость введения уголовной ответственности за деяния, которые нарушают установленный законодательный запрет на использование криптовалют в качестве средства платежа за реализуемые и приобретаемые юридическими и физическими лицами-резидентами Российской Федерации товары, работы, услуги.

2. Обоснована необходимость введения уголовной ответственности за деяния, которые нарушают установленный законодательный запрет на организацию криптобиржами, криптообменными пунктами, виртуальными P2P-платформами на территории Российской Федерации выпуска, обмена, обращения, а также непосредственно выпуск и обмен криптовалюты.

3. Обоснована необходимость введения уголовной ответственности за деяния, которые нарушают установленный законодательный запрет для финансовых организаций на осуществление собственных вложений в криптовалюты и финансовые инструменты, связанные непосредственно с криптовалютами, а также за деяния, нарушающие установленный законодательный запрет на использование инфраструктуры российского финансового рынка либо российских финансовых посредников в целях осуществления операций с криптовалютой: приобретение и отчуждение криптовалюты, осуществление перечислений и платежей с использованием криптовалюты или любое иное способствование проведению аналогичных операций, в том числе оказание услуг по хранению или содействие принятию рисков через производные финансовые инструменты.

Степень достоверности и апробация результатов исследования.

Достоверность результатов исследования обусловлена широкой научной и эмпирической базой исследования, обеспечена методологией исследования, использованием автором сведений судебной практики и данных

судебной статистики, результатами социологического опроса, а также логической непротиворечивостью, связностью, внутренней согласованностью и обоснованностью полученных результатов, согласованностью полученных выводов с юридической практикой.

Апробация и внедрение результатов исследования осуществлялись следующим образом:

1. Результаты исследования нашли отражение в научных публикациях автора, в том числе монографиях, а также научных статьях, опубликованных в рецензируемых журналах, рекомендованных ВАК Минобрнауки России для публикации основных научных результатов диссертаций на соискание ученых степеней доктора и кандидата наук.

2. Рекомендации автора отражены в научных докладах и выступлениях на научных и научно-практических конференциях, в том числе на IX Международной научно-практической конференции «Современная экономика: концепции и модели инновационного развития» (15-16 февраля 2018 г., РЭУ им. Г.В. Плеханова), VIII Российско-германском круглом столе «Преступления в сфере экономики: российский и европейский опыт» (21 октября 2016 г., МГЮА им. О.Е. Кутафина), круглом столе «Криптовалюты VS цифровые валюты центральных банков: будущее экономики и права» (15 апреля 2022 г., МГИМО МИД России), всероссийской научно-практической конференции «Уголовное право как средство управления обществом» (17 марта 2022 г., Московская академия Следственного комитета) и других.

3. Материалы исследования внедрены в практическую работу следственных органов СК России, а также в учебный процесс по подготовке специалистов для следственных органов в Московской академии Следственного комитета, использованы при разработке учебников, учебных и учебно-методических пособий, учебных программ по уголовному праву, а также дополнительных профессиональных программ – программ повышения квалификации.

Диссертация состоит из введения, двух глав, заключения, списка использованной литературы и нормативных правовых актов, а также приложения.

Глава 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

§ 1.1. Криптовалюта как предмет и средство совершения преступления

Конец XX и начало XXI века ознаменовались серьезными изменениями в общественной жизни, в том числе непосредственно связанными с новыми научными разработками, используемыми в повседневной жизни современного человека. Многие люди уже сегодня не мыслят своей жизни без каждодневного использования информационных технологий, что порождает качественные изменения в их повседневной жизни: характере общения между собой, приобретении товаров и услуг, развлечениях и осуществлении трудовых функций. Практически все стороны жизни современного человека претерпевают качественные изменения благодаря так называемым «информационным технологиям», уже ставшими неотъемлемой частью жизни современного общества. Как полагали М.Г. Лазар, И.И. Лейман, продолжающаяся научно-техническая революция во многом порождается «лавинообразным процессом инноваций, материализованных научных идей, научных открытий, технических изобретений и разработок, с принципиально новыми технологическими процессами, которые в совокупности, в свою очередь, порождают стремительные, динамичные изменения в социальной структуре общества»[3]. Аналогичного мнения придерживаются и современные ученые. Так, например, Л.М. Борщ, С.В. Герасимова полагают, что принципиально новые, инновационные идеи, такие, например, как цифровая экономика, должны кардинально изменить нашу жизнь и «перевернуть привычный для нас ее уклад» [4].

---

[3] См.: Лазар М. Г. НТР и нравственные факторы научной деятельности: Очерки этики науки. Л., 1977. С. 7—8.

[4] Борщ Л. М. Современные аспекты сдвигов инновационной парадигмы от цифровой экономики к цифровой трансформации // Инновационная парадигма экономических механизмов хозяйствования: сборник научных трудов VII Всероссийской научно-

Подобного рода изменения общественной жизни качественно видоизменили такие виды человеческих взаимоотношений, как общение, осуществляемое сегодня людьми посредством электронных технических средств, непосредственные финансовые расчеты также чаще всего сегодня осуществляются с помощью электронных средств, оснащенных специализированными компьютерными программами. Появление электронной подписи делает возможным удостоверение документа дистанционно с использованием телекоммуникационной сети Интернет.

Интегрированные в жизнь общества цифровые технологии, в том числе криптовалюта, позволяют говорить о новой цифровой реальности. Данная реальность не только оказывает определенное влияние на жизнь общества и каждого конкретного человека, но и изменяет привычный нам материальный мир как мы его, представляли до этого. Более того, изменяется само понятие материи как определенного философского постулата. Используемые современные цифровые технологии оказывают воздействие на человека, в том числе на образ его мышления, его материальное благосостояние, способы приобретения человеком товаров, работ, услуг для личного использования и инновационные способы оплаты таких товаров.

Изменения в общественной жизни, к сожалению, порождают и новые, ранее не существовавшие способы совершения преступлений, которые также требуют уголовно-правовой оценки. В противном случае охрана прав, свобод человека и гражданина, его собственности остаются невыполненными.

Следует согласиться с мнением Э.Л. Сидоренко о том, что «одной из задач уголовного законодательства является предупреждение совершения преступлений, и квалификация хищений криптовалюты не должна оставаться вне рамок уголовно-правового регулирования»[5].

практической конференции с международным участием, Симферополь, 16 мая 2022 года. Симферополь, 2022. С. 73–77.

[5] Сидоренко Э.Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. 2018. № 2. С. 134.

Но для того, чтобы такая задача, как предупреждение совершения преступлений, была реализована и право собственности добросовестных приобретателей криптовалюты от преступных посягательств было защищено, необходимо разрешение нескольких проблем уголовно-правового характера, возникающих при расследовании соответствующих уголовных дел и влияющих на квалификацию преступлений, совершаемых с использованием криптовалюты.

К таковым можно отнести:

1. Различный правовой режим криптовалюты исходя из требований национального законодательства Российской Федерации в разные временные периоды, что приводило к тому, что виртуальная валюта похищалась из криптокошельков, но правоохранительные органы, как правило, отказывали в возбуждении уголовного дела, мотивируя это тем, что отсутствует предмет посягательства[6].

2. Отсутствие единой методики определения ущерба, причиненного собственнику в результате совершения различных видов хищения криптовалюты.

Квалификация преступлений с использованием криптовалюты находится в прямой связи с указанными проблемами, так как правовой режим криптовалюты в определенный временной период и её стоимость могут непосредственно повлиять на квалификацию действий лиц, совершивших преступления, в которых криптовалюта является предметом преступления.

В теории уголовного права всегда признавалась взаимосвязь гражданско-правового и уголовно-правового понятия имущества. Справедливо отмечает Н.А. Лопашенко: «Уголовное право не изобретает своего понятия имущества; оно пользуется в основном тем, которое существует в гражданском праве...»[7].

---

[6] Сидоренко Э.Л. Правовой статус криптовалют в Российской Федерации. С. 134.

[7] Лопашенко Н.А. Преступления против собственности // Авторский курс. Кн. I. Общетеоретическое исследование посягательств на собственность: Монография. М., 2019. С. 70.

Таким образом, рассматривая криптовалюту как предмет преступления, необходимо исходить из требований ст. 128 ГК РФ, определяющей общие понятия объектов гражданских прав и относящих криптовалюту к не конкретизированному «иному имуществу» и Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», конкретизирующие криптовалюту как иное имущество в виде одной из разновидностей цифровой валюты. Федеральный закон от 31 июля2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» регулирует отношения, возникающие при выпуске, учете и обращении цифровых финансовых активов, особенности деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и операторов обмена цифровых финансовых активов, а также отношения, которые возникают при обороте цифровой валюты в Российской Федерации. Указанный закон разделяет понятия «цифровой финансовый актив» и «цифровая валюта».

Цифровыми финансовыми активами вышеуказанным законом признаются некие цифровые права, включающие денежные требования, а также возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном Федеральным законом от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы.

В свою очередь, цифровой валютой признается совокупность конкретно не определенных законом электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.

Учитывая, что оборот криптовалюты осуществляется с использованием различных пиринговых, то есть не имеющих оператора[8], платежных систем, использующих определенную расчетную единицу и соответствующий протокол передачи данных, для обеспечения деятельности которых используются криптографические методы, то понятие криптовалюта охватывается понятием цифровая валюта. То есть криптовалюта является одной из разновидностей цифровой валюты, на ряду с токенами, стейблкоинами, игровыми деньгами, но при этом имеет принципиальное отличие от них. Оно заключается в отсутствии эмитента, имеющего возможность оказывать влияние на выпуск (генерирование) криптовалюты. Создание (генерирование) криптовалюты происходит в процессе так называемого «майнинга» – вычислительных операций специального характера, осуществляемых ЭВМ и позволяющих получить электронные (виртуальные) условные единицы – криптомонеты, являющиеся виртуальной

[8] См.: Жигас М.Г., Кузьмина С.Н. Природа и сущность криптовалюты // Известия Байкальского государственного университета. 2018. Т. 28. № 2. С. 201–207.

валютой (криптовалютой), которая может быть конвертирована в фиатные денежные средства.

Конкретизировано-унифицированное определение криптовалюты как разновидности цифровой валюты, с одной стороны, позволяет использовать механизмы ее правового регулирования в том числе и на международном уровне, а с другой — возникает вопрос относительно правового режима криптовалюты как объекта гражданского права. В соответствии со статьей 128 Гражданского кодекса Российской Федерации к объектам гражданских прав относятся вещи (включая наличные деньги и документарные ценные бумаги), а также иное имущество, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права); результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага. Но криптовалюта, являясь разновидностью цифровой валюты, не является цифровым правом, так как представляет собой лишь совокупность конкретно не определенных законом электронных данных (цифрового кода), которые содержатся в соответствующей информационной системе и не предоставляют своим владельцам каких-либо прав, предусмотренных статьей 141.1 Гражданского кодекса Российской Федерации. Таковыми признаются только лишь поименованные в данном качестве в законе обязательственные, либо иные права, содержание, а также осуществление которых должны определяться в соответствии с правилами информационной системы, которая, в свою очередь, должна отвечать определенным признакам, установленным законом.

Таким образом, криптовалюта получила законодательное определение как разновидность цифровой валюты, но цифровая валюта, в свою очередь, не является конкретно определенным объектом гражданского права, предусмотренного статьей 128 Гражданского кодекса Российской Федерации, по сути оставаясь неконкретизированным «иным имуществом», что не только

не позволяет конкретизировать криптовалюту как предмет преступления, но и может привести к неправильному определению совокупности объективных и субъективных признаков, закреплённых в уголовном законе, которые определяют общественно опасное деяние как преступление.

Анализируя нормы гражданского права Российской Федерации, историю правового регулирования криптовалюты в России можно условно разделить на три периода.

Первый период — до 1 октября 2019 года. Он характеризуется отсутствием в законодательстве Российской Федерации правового определения криптовалюты как некоего самостоятельного объекта гражданского права, но при этом все же позволявшего говорить о ней как о некоем хотя бы «ином», но все же имуществе, что само по себе вызывало нескончаемые юридические споры[9].

Так, часть юридического сообщества придерживалась мнения, что при отсутствии правовых норм, определяющих криптовалюту как некий самостоятельно обособленный объект гражданского права, она (криптовалюта) таковым объектом вообще не может являться[10]. Следовательно, все сделки с ее использованием в силу требований статьи 166 Гражданского кодекса Российской Федерации являются ничтожными и не влекут за собой юридических последствий.

В качестве обоснования, как правило, ссылались[11] на статью 27 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в соответствии с которой запрещено

---

[9] См. Перов В.А. Проблемные уголовно-правовые аспекты, возникающие при расследовании преступлений, совершенных с использованием криптовалюты // Уголовное право как средство управления обществом: Материалы всероссийской научно-практической конференции (Москва. 17 марта 2022 года). Часть 2). М., 2022. С. 153.

[10] См.: Аблятипова Н. А. Самохина А. Н. К вопросу о необходимости законодательного закрепления виртуальной валюты // Вопросы российского и международного права. 2018. Т. 8, № 11А. С. 61–69.

[11] См.: Кочергин, Д. А. Криптоактивы: экономическая природа, классификация и регулирование оборота // Вестник международных организаций: образование, наука, новая экономика. 2022. Т. 17. № 3. С. 75–130.

введение на территории Российской Федерации других денежных единиц кроме рубля Российской Федерации, а также запрещен выпуск денежных суррогатов. При этом не принималось во внимание, что в соответствии с действующим законодательством Российской Федерации криптовалюта не является денежной единицей, вследствие чего ее оборот на территории Российской Федерации законодательно не запрещался и не ограничивался.

Первые упоминания о криптовалюте биткоин относят к 2009 году, хотя разработка программы была окончена в конце 2008 года[12]. В указанный временной период на территории Российской Федерации действовала статья 128 Гражданского кодекса Российской Федерации, в соответствии с которой к объектам гражданских прав относились вещи, в том числе деньги, ценные бумаги, а также любое иное имущество и имущественные права. Кроме того, к объектам гражданских прав также относят работы и услуги, охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность), а также нематериальные блага. Соответственно криптовалюта относилась к специально не обособленному «иному имуществу», предусмотренному статьей 128 Гражданского кодекса Российской Федерации, хотя далеко не все юристы придерживались такого мнения, полагая, что криптовалюта как некий виртуальный актив никоим образом не регулировалась действующим законодательством Российской Федерации[13]. Так, например решением[14] Волгодонского районного суда (Ростовская область) отказано в удовлетворении исковых требований о взыскании с ответчика неосновательного обогащения и процентов за пользование чужими денежными средствами на том основании, что доводы истца о получении им

[12] См.: Гаврилова Э.Н. Биткоин и современные деньги: история возникновения, различия и перспективы развития // Экономические и гуманитарные науки. 2020. № 4(339). С. 66–71.
[13] Аблятинова Н.А. Указ. соч. С. 61–69.
[14] Решение Волгодонского районного суда по гражданскому делу № 2—4140/2018 от 18 марта 2019 г. [Электронный ресурс] / Волгодонский районный суд Ростовской области. URL: http://volgodonskoy.ros.sudrf.ru/ (дата обращения: 21.11.2022).

дохода в виде криптовалюты, которая в дальнейшем была обменена им же на рубли и перечислена на счет банковской карты ответчика, не основаны на законе, так как операции с криптовалютами совершаются вне правового регулирования Российской Федерации. Криптовалюты не гарантируются и не обеспечиваются Банком России[15].

Таким образом, при использовании в процессуальных документах терминов криптовалюта «биткойн» в период времени до 1 октября 2019 года необходимо указывать, что данный объект гражданского права является неконкретизируемым законом «иным имуществом»[16].

Второй период, изменивший правовой режим криптовалюты[17], связан с принятием Федерального закона от 18 марта 2019 года № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» (далее 34-ФЗ). В соответствии с указанным 34-ФЗ внесены изменения в статью 128 Гражданского кодекса Российской Федерации. Соответственно, к объектам гражданских прав стали относиться вещи, в том числе наличные деньги, а также документарные ценные бумаги, иное имущество и имущественные права, результаты работ, оказание услуг; охраняемые результаты интеллектуальной деятельности, приравненные к ним средства индивидуализации (интеллектуальная собственность), нематериальные блага. Федеральный закон № 34-ФЗ вступил в силу с 1 октября 2019 года, вследствие чего криптовалюта и, в частности, ее разновидность «биткойн» стала конкретизированным объектом гражданского права, то есть «цифровым правом».

Таким образом, с 1 октября 2019 года по 1 января 2021 года в связи с вступлением в силу Федерального закона от 31 июля 2020 года № 259-ФЗ «О

---

[15] Там же.

[16] Статья 128 части первой Гражданского кодекса Российской Федерации в редакции Федерального закона от 02.07.2013 № 142-ФЗ «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации».

[17] См.: Перов В. А. Проблемные вопросы, возникающие при расследовании уголовных дел о преступлениях с использованием криптовалюты // Российский следователь. 2020. № 7. С. 20–22.

цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», правовое положение криптовалюты изменилось. Из законодательного определения следует, что криптовалюта по своим технологическим свойствам является неким цифровым правом, правда не совсем понятно правом на что, и если это право, то каков механизм его реализации? На эти вопросы действующее на указанный период времени законодательство ответов не давало. Таким образом, после вступления в силу вышеуказанного закона криптовалюту в Российской Федерации следовало рассматривать как цифровое право соответствующей криптовалюты и в качестве такового она подлежала указанию в процессуальных документах (например: «цифровое право криптовалюты биткоин»). Такого мнения придерживались многие ученые, полагавшие, что криптовалюта относится именно к цифровым правам, так как присутствует ее непосредственная связь с «информационной системой», «более известной как блокчейн криптовалюты»[18].

Понятие цифрового права изложено в статье 141.1 Гражданского кодекса Российской Федерации, в соответствии с которой таковыми признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам.

Федеральный закон от № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» не только конкретизировал правовое положение криптовалюты, но фактически повторно изменил её правовой режим, определив криптовалюту как конкретизированное «иное имущество» в виде «цифровой валюты».

---

[18] Лыков А.А. Хищение криптовалюты: проблемы уголовно-правовой квалификации // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования. 2019. Т. 2. № 1(1). С. 13–18.

Таким образом, правовое положение криптовалюты в Российской Федерации в различные временные периоды кардинальным образом менялось, что влияло непосредственно на квалификацию преступлений, совершаемых с использованием криптовалюты, так как фактически с изменением правового режима криптовалюты изменялся непосредственно предмет преступления.

Третий период связан[19] с вступившим в силу с 1 января 2021 года Федеральным законом от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», который уже предусматривает такое понятие, как «цифровая валюта».

В соответствии с п. 3 ст. 1 вышеуказанного закона под термином «цифровая валюта» понимается некая совокупность электронных данных в виде цифрового кода либо обозначения, содержащиеся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам. Данная формулировка более точно определяет правовое положение криптовалюты в системе национального права, как одну из разновидностей цифровой валюты. Таким образом, криптовалюта становится законодательно определенным объектом гражданского права как «иное имущество в виде цифровой валюты»

[19] См.: Перов В.А. Проблемные вопросы… С. 20–22.

соответствующей разновидности[20] (например, «иное имущество в виде цифровой валюты биткоин») и в качестве такового может быть указана в соответствующих уголовно-процессуальных документах[21], в том числе в качестве предмета преступления.

Соответственно объектом познания уголовного права будут являться общественные отношения, складывающиеся в сфере уголовно-правового противодействия совершению преступлений с использованием криптовалюты.

Функционирование подавляющего большинства криптовалют связано с технологией блокчейн, но сама технология блокчейн может быть использована не только для осуществления криптовалютных переводов (транзакций)[22]. Тем не менее, одними из самых распространенных на сегодняшний день преступлений, совершаемых с использованием блокчейн-технологий, являются преступления с использованием криптовалюты, принцип оборота которой основан на указанной технологии и представляет собой разновидность децентрализованной, одноранговой (пиринговой) сети, основанной на равноправии всех ее участников. Исходя из законодательного определения понятия «цифровая валюта» можно сделать вывод о том, что криптовалюта является одной из разновидностей цифровой валюты, которая имеет свои характерные особенности, отличающие ее от других разновидностей криптовалют. Одной их таких особенностей является использование технологии блокчейн для осуществления ее (криптовалюты) оборота и использования хэширования для создания новых блоков. В целях объективности необходимо отметить, что попытки создания криптовалют имели место до создания технологии блокчейн, однако подавляющее

---

[20] См.: Егорова М.А., Ефимова Л.Г. Понятие криптовалют в контексте совершенствования российского законодательства // Lex Russica (Русский закон). 2019. № 7(152). С. 130–140.

[21] См.: Пинкевич Т.В. Предупреждение преступлений, совершаемых в сфере оборота цифровой валюты (криптовалюты) // Правовое государство: теория и практика. 2021. № 4(66). С. 82–96.

[22] См: Риски цифровизации: виды, характеристика, уголовно-правовая оценка: монография / отв. ред. Ю.В. Грачева. М., 2022. С. 46.

большинство известных ныне криптовалют функционируют именно с использованием данной технологии. Другие разновидности цифровой валюты генерируются, и их оборот осуществляется с использованием отличных от криптовалюты технологических принципов. К основным принципам, которые лежат в основе создания (майнинга) и последующего использования полученной в результате майнинга криптовалюты, относятся:

- децентрализация выпуска криптовалют. Отсутствует единый эмитент, который может оказать влияние на количество генерируемых криптомонет, уменьшать или увеличивать процесс их генерации, оказывая тем самым искусственное влияние на их стоимость (манипулируя рынком криптовалют);

- отсутствие возможности регулирования и контроля , в том числе со стороны государства, за выпуском и обращением криптовалюты. В данном случае под контролем следует понимать возможность контроля количества сгенерированных системой криптомонет;

- анонимность лиц, использующих криптовалюту, при полной открытости ее обращения и в то же время возможность проследить оборот (транзакции) каждой из созданных криптомонет любым лицом, имеющим такое желание. Анонимно заключенные сделки с использованием криптовалюты лишают стороны возможности предъявить друг другу претензии в случае неисполнения обязательства сторонами такой сделки;

- отсутствие административных, территориальных и политических барьеров для создания и использования криптовалюты;

- возможность анонимного совершения любых сделок вне зависимости от того, разрешены они или нет действующим национальным законодательством определенной страны[23].

Все вышеуказанные принципы создания и использования криптовалюты имеют определенное юридическое значение, то есть могут порождать юридические последствия, не присущие другим разновидностям

[23] См.: Перов В.А. Криптовалюта как объект гражданского права // Гражданское право. 2017. № 5. С. 7.

цифровой валюты, и обязательно должны учитываться при квалификации преступлений, совершаемых с ее использованием. Из всех принципов, свойственных тем или иным явлениям, особо важное значение имеют именно правовые принципы, потому что только право является единственным базовым социальным, универсальным, интегративным, обязательным, охраняемым государством институтом, который постоянно совершенствуется и является регулятором всех жизненно важных общественных отношений[24]. Вышеуказанные отличительные принципы создания и функционирования криптовалюты отличают их от других видов цифровой валюты. На различных сайтах телекоммуникационной сети Интернет можно встретить чрезвычайно большое количество вариантов возможной классификации криптовалют, носящих технологический характер и не имеющих юридического значения.

Другой разновидностью блокчейн-технологий являются смарт-контракты. Однако принцип их функционирования исключает возможность совершения преступлений с их использованием.

Объективная сторона преступлений с использованием криптовалюты выполняется либо непосредственно в виртуальном пространстве, либо последовательно в виртуальном пространстве и вне его.

Преступления с использованием криптовалюты, совершаемые в виртуальном пространстве, обладают определенной спецификой, которая заключается в разграничении действий, совершаемых непосредственно субъектом преступления, то есть человеком, и совершаемых машиной, то есть комплексом программно-аппаратных средств, без участия человека, вследствие чего при осуществлении квалификации указанных преступлений следует рассматривать в качестве доказательств в том числе и так называемые «виртуальные» («цифровые», «электронные») следы, то есть такие данные,

[24] См.: Дробязко С.Г. Принципы в праве // Проблемы развития юридической науки и совершенствование правоприменительной практики: сб. науч. тр. Минск, 2005. С. 27–33.

которые оставляет человек при работе в интернет-сети[25] и подтверждающих совершение преступления.

Как было отмечено Л.Д. Гаухманом, «уголовно-правовая оценка содеянного слагается из двух компонентов: отграничение преступного от непреступного и квалификация преступного, т.е. квалификация преступления»[26]. Данное положение является верным и при квалификации преступлений с использованием криптовалюты. При этом для того чтобы отграничить преступное от непреступного, сначала необходимо отграничение действий, совершаемых человеком от действий, совершаемых машиной и не зависящих от воли человека. Технология блокчейна, являющаяся базовой структурой большинства криптовалют, защищена с помощью различных механизмов, включающих в себя «криптографические методы и математические модели поведения и принятия решений»[27], предотвращающих дублирование или уничтожение такого рода цифровых денег, вследствие чего преступными действия человека могут признаваться только в том случае, когда он имеет прямой умысел, направленный на обход существующей системы безопасности функционирования сети и осуществляет во исполнение задуманного соответствующие действия.

Речь может идти о совершении преступлений разного вида, в которых криптовалюта может выступать либо как предмет преступления, либо как средство совершения преступления, а в определенных случаях используется фактически как платежное средство. Таким образом, мы классифицировали преступления по месту и роли криптовалюты в составе преступления:

---

[25] См.: Сукманов А.О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений // Вестник Калининградского юридического института МВД России. 2010. № 4 (22). С. 104–107.

[26] См.: Гаухман Л. Д. Квалификация преступлений: закон, теория, практика. М., 2010. С. 10.

[27] См.: Ловцов Д. А. Информационная безопасность автоматизированных блокчейн систем: угрозы и способы повышения // Трансформация национальной социально-экономической системы России: Материалы II Международной научно-практической конференции, Москва, 22 ноября 2019 года. М., 2020. С. 464–473.

1. Криптовалюта является предметом следующих преступлений: кража (ст. 158 УК РФ), мошенничество (ст. 159 УК РФ), присвоение или растрата (ст. 160 УК РФ), грабёж (ст. 161 УК РФ), разбой (ст. 162 УК РФ), вымогательство (ст. 163 УК РФ), легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174 УК РФ), легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления (ст. 174^1 УК РФ), приобретение или сбыт имущества, заведомо добытого преступным путем (ст. 175 УК РФ), уклонение от исполнения обязанностей по репатриации денежных средств в иностранной валюте или валюте Российской Федерации (ст. 193 УК РФ), а также преступлений, в которых криптовалюта выступает в виде имущественных прав или средства совершения преступления.

2. К преступлениям, в которых криптовалюта выступает в виде имущественных прав или средства совершения преступления, можно отнести преступления, предусмотренные главой 30 Уголовного кодекса Российской Федерации (преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления). Это преступления, предусмотренные следующими статьями Уголовного кодекса Российской Федерации: 290 (получение взятки), 291 (дача взятки), 291^1 (посредничество во взяточничестве), 291^2 (мелкое взяточничество). Кроме того, диспозиция ст. 110^1 (склонение к совершению самоубийства или содействие совершению самоубийства) предусматривает склонение к совершению самоубийства путем подкупа, ст. 141 (воспрепятствование осуществлению избирательных прав или работе избирательных комиссий) предусматривает совершение указанного деяния соединенное с подкупом, ст. 142 (фальсификация избирательных документов, документов референдума, документов общероссийского голосования), предусматривающая возможность подделки избирательных подписей, равно как и подписей участников референдума в поддержку выдвигаемого кандидата, а также списка

кандидатов, которые были выдвинуты, а также по иным основаниям, предусмотренным диспозицией указанной статьи, соединенные с подкупом, ст. 183 (незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну), предусматривающую собирание сведений, которые составляют банковскую, налоговую или коммерческую тайну, путем подкупа, ст. 200^5 (подкуп работника контрактной службы, контрактного управляющего, члена комиссии по осуществлению закупок), ст. 200^7 (подкуп арбитра (третейского судьи)), ст. 204 (коммерческий подкуп), ст. 204^1 (посредничество в коммерческом подкупе), ст. 204^2 (мелкий коммерческий подкуп), ст. 304 (провокация взятки, коммерческого подкупа либо подкупа в сфере закупок товаров, работ, услуг для обеспечения государственных или муниципальных нужд), ст. 309 (подкуп или принуждение к даче показаний или уклонению от дачи показаний либо к неправильному переводу). Кроме перечисленного сюда же можно отнести еще и другую группу преступлений, предусмотренных ст. 205^1 (содействие террористической деятельности), связанных с финансированием терроризма. При организации совершения хотя бы одного из преступлений, которые предусмотрены ст. ст. 205, 205^3, частями третьей и четвертой ст. 206, частью четвертой ст. 211, равно как руководство его совершением, либо организация финансирования терроризма, под которым понимается предоставление, а также сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации террористической организации, либо лиц для ведения ими террористической деятельности.

Сюда также можно отнести финансирование совершения различных преступлений экстремистской и террористической направленности: ст. 208 (организация незаконного вооруженного формирования или участие в нем, а равно участие в вооруженном конфликте или военных действиях в целях, противоречащих интересам Российской Федерации), диспозиция которой предусматривает в том числе финансирование вооруженного формирования,

ст. 282^3 (финансирование экстремистской деятельности), ст. 359 (наемничество), ст. 361 (акт международного терроризма).

Также к преступлениям, в которых криптовалюта выступает в виде определенных имущественных прав, можно отнести преступления, предусмотренные ст. 200^7 (подкуп арбитра (третейского судьи), ст. 204 (коммерческий подкуп), ст. 204^1 (посредничество в коммерческом подкупе), 204^2 (мелкий коммерческий подкуп).

3. Криптовалюта может выступать и в виде фактического платежного средства при совершении следующих преступлений, предусмотренных Уголовным кодексом Российской Федерации: преступления, предусмотренные ст. 222

(незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение оружия, основных частей огнестрельного оружия, боеприпасов), ст. 222^1 (незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение взрывчатых веществ или взрывных устройств), ст. 222^2 (незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему), ст. 228^1 (незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества), ст. 228^4 (незаконные производство, сбыт или пересылка прекурсоров наркотических средств или психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих прекурсоры наркотических средств или психотропных веществ, либо их частей, содержащих прекурсоры наркотических средств или психотропных веществ), ст. 282^3 (финансирование экстремистской деятельности).

В данном случае в качестве фактического денежного средства выступают не только денежные средства в валюте Российской Федерации,

либо иностранной валюте, но и безналичные денежные средства, а также криптовалюта.

Криптовалюта может использоваться в качестве фактического средства оплаты и при совершении преступлений по найму, таких как убийство (ст.105), склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110^1), умышленное причинение тяжкого вреда здоровью (ст. 111), истязание (ст. 117), захват заложника (ст. 206), а также иных преступлений, совершенных по найму.

При совершении таких преступлений криптовалюта используется как фактическое платежное средство при оплате лицам, совершающим вышеуказанные преступления по найму.

Необходимо также учитывать требования статьи 1 Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16.05.2005, а также рекомендации 15 ФАТФ, согласно которым предметом преступлений, предусмотренных статьями 174 и 174^1 УК РФ, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), которые были приобретены в результате совершения преступления.

В соответствии с разъяснениями, данными в Постановлении Пленума Верховного Суда Российской Федерации от 07 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», крупный или особо крупный размер деяния, предусмотренного статьями 174 и 174^1 УК РФ, определяется исходя из фактической стоимости имущества, составляющего предмет данных преступлений, на момент начала осуществления с ним финансовых операций или сделок, а в случае совершения нескольких финансовых операций или сделок – на момент начала осуществления первой из них. При отсутствии сведений о фактической стоимости имущества она

может быть установлена на основании заключения специалиста или эксперта[28].

Если предметом преступления являются денежные средства в иностранной валюте, крупный или особо крупный размер деяния, предусмотренного ст. ст. 174 и 174[1] УК РФ, определяется по официальному курсу соответствующей валюты, установленному Банком России на основании статьи 53 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» на момент начала осуществления с указанной валютой финансовых операций или сделок. Криптовалюта не является иностранной валютой, вследствие чего данные рекомендации, отраженные в Постановлении Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», к определению её стоимостных характеристик принять за основу нельзя.

Необходимо отметить, что, кроме указанных выше, к преступлениям, совершаемым с использованием криптовалюты, можно отнести и иные преступления, тем или иным образом связанные с имущественными отношениями, однако ввиду особенностей объективной и (или) субъективной стороны будут рассмотрены отдельно.

Из изложенного можно сделать вывод, что в зависимости от совершенного преступления криптовалюта может являться как предметом совершения таких преступлений, так и средством их совершения. В случаях, когда криптовалюта используется в качестве фактического средства оплаты,

---

[28] Постановление Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». СПС «Консультант плюс» (дата обращения – 29.03.2023).

она является признаком объективной стороны соответствующего преступления.

В различных преступлениях, совершенных с использованием криптовалюты, присутствует разная степень использования непосредственно виртуального пространства, различны способы их совершения, объекты и предметы преступного посягательства, характер и степень общественной опасности данных преступлений. Соответственно, невозможно классифицировать преступления, совершаемые с использованием криптовалюты, по одному лишь объекту преступления. Не всегда криптовалюта выступает и в качестве предмета преступления. Она может выступать в качестве фактического средства платежа при совершении преступлений по найму, преступлений коррупционной направленности. Таким образом, объект преступлений, совершаемых с использованием криптовалюты, может быть различен.

Представляется, что объединяющими признаками всех подобных преступлений является место, условие и средство их совершения, то есть использование виртуального пространства и технологии блокчейн, являющихся основой функционирования криптовалют. Какое бы преступление с использованием криптовалют не совершалось, условием его совершения является использование субъектом такого преступления технологии блокчейн в виртуальном пространстве. При этом преступник использует различные телекоммуникационные средства, позволяющие ему осуществить доступ в виртуальное пространство и совершить определенные действия по обороту криптовалюты, что и будет являться обязательным условием совершения таких преступлений.

Аналогичного мнения придерживается Е.А. Русскевич, полагающий, что «самостоятельным видом преступлений, совершаемых с использованием информационно-коммуникационных технологий, к которым естественно отнести и преступления, совершаемые с криптовалютой, являются

преступления в сфере компьютерной информации»[29]. Е.А. Русскевич особо отмечает следующее: «Природа данных преступлений специфична в том смысле, что само их происхождение, существование и, следовательно, совершение немыслимы без информационной среды»[30]. Соответственно, «без теоретического обоснования понятия криптовалютных отношений такие деяния будут находиться в правовом вакууме, среди спорных и неоднозначных мнений правоприменителей, влекущих существенные разногласия в судебной практике»[31].

Вышеизложенное раскрывает понятие «преступление с использованием криптовалюты» через такие его обязательные признаки, как средство совершения (компьютерная техника, информационно-телекоммуникационные сети, технология блокчейн) и условия совершения (оборот криптовалюты соответствующего вида). При отсутствии хотя бы одного из указанных обязательных признаков нельзя говорить о составе преступления, совершенного с использованием криптовалюты. В качестве примера можно привести преступления, совершаемые в сетях Даркнет[32]. В виртуальном пространстве с использованием даркнет-сети осуществляется торговля запрещенными к гражданскому обороту веществами, оружием. Расчет за приобретенные товары осуществляется в криптовалюте. В начале апреля 2022 года управление по контролю за зарубежными активами Минфина США (OFAC) ввело санкционные меры[33] в отношении одной из самых крупных и популярных в мире рынка Даркнета виртуальной торговой площадки Hydra

---

[29] Русскевич Е. А. Уголовное право и информатизация // Журнал российского права. № 8. 2017. С. 76.

[30] Там же.

[31] См.: Долгиева М.М. Особенности объекта и предмета преступлений, совершаемых в сфере оборота криптовалюты // Уголовная юстиция. № 12. 2018. С. 19.

[32] Даркнет (англ. DarkNet — «скрытая сеть», «темная сеть» или «теневая сеть») представляет собой скрытый сегмент Интернета, который доступен только при использовании специализированного браузера.

[33] См.: Жандров В.Ю., Фильченко А.П. Использование режима санкций и системы комплаенс в снижении рисков незаконных операций с виртуальными активами: зарубежный и российский опыт // Правовое государство: теория и практика. 2022. № 3(69). С. 171–183.

(даркнет-рынок по торговле наркотиками за криптовалюту), которая действовала не только в России, но и в других странах мира[34]. Данная торговая площадка начала свою деятельность в 2015 году и является самым популярным рынком Даркнета в Российской Федерации и одним из самых крупных рынком Даркнета в мире[35]: «Приблизительно 86 % нелегальных биткойнов, приобретенных конкретно российскими биржами цифровых денег в 2019 году, поступили от Hydra»[36]. При этом «выручка Hydra резко росла с менее чем 10 миллионов долларов в 2016 году до больше чем 1,3 млрд. долларов в 2020 году»[37].

По мнению Центрального банка Российской Федерации, в мире наблюдается стремительный рост рынка криптовалют. Совокупный объем их капитализации в декабре 2021 года достигал 2,3 трлн. долларов США, что соответствует примерно 1% глобальных финансовых активов. Доля платежных транзакций, приходящаяся на криптовалюты, ничтожно мала по сравнению с показателями традиционных платежных систем, но благодаря анонимности денежные суррогаты активно используются для расчетов в рамках противоправной деятельности, в том числе для неподконтрольного государству вывода денежных средств за рубеж. Вовлеченность в криптовалютный рынок традиционных финансовых посредников пока ограничена, но активизируется торговля производными финансовыми инструментами и паями биржевых фондов (ETF – инвестиционный инструмент, использующий криптовалюту в качестве базового актива), связанными с криптовалютами, развиваются экосистемы децентрализованных

---

[34] См.: Бровко Н.А., Криштаносов В.Б. Концептуально-аналитические подходы к возникновению потенциальных угроз в цифровой экономике // Alter Economics. 2023. Т. 20. № 1. С. 216–245.

[35] См.: Раднаева Э.Л., Салихов Р.Н. Незаконный оборот наркотических средств и их аналогов с использованием компьютерных технологий (сети интернет) // Банзаровские чтения: Материалы международной научной конференции, посвященной 200-летию со дня рождения Д. Банзарова и 90-летию БГПИ-БГУ. Часть 2. Улан-Удэ, 2022. С. 73–76.

[36] Там же.

[37] Там же.

финансов (DeFi)[38]. Объем сделок российских граждан с криптовалютами, по некоторым оценкам, достигает 5 миллиардов долларов США в год. Российские граждане являются активными пользователями интернет-платформ, осуществляющих торговлю криптовалютами. Кроме того, Россия находится в числе лидеров по объему мировых майнинговых мощностей[39].

Долгосрочный потенциал применения криптовалют для расчетов представляется ограниченным. Стремительный рост их рыночной стоимости определяется в первую очередь спекулятивным спросом в расчете на дальнейший рост курса, что приводит к формированию финансового пузыря, запускающего инфляционные процессы. Криптовалюты также имеют характеристики финансовой пирамиды, поскольку рост их цены во многом поддерживается спросом со стороны вновь входящих на рынок участников[40].

По мнению специалистов Центрального Банка Российской Федерации, распространение криптовалют создает существенные угрозы для благосостояния российских граждан и стабильности финансовой системы государства. Высокая волатильность курса криптовалют, значительная распространенность мошенничества в торговле криптовалютами создают для граждан риски утраты существенной части вложенных средств, а при торговле с использованием заемных средств – риски остаться должником. Криптоизация, как и валютизация, ограничивает суверенитет денежно-кредитной политики государства, в результате чего для сдерживания инфляции Центральному банку Российской Федерации необходимо будет поддерживать на постоянной основе более высокий уровень ключевой ставки, что в свою очередь снизит доступность кредитования как для граждан, так и для бизнеса. Распространение криптовалют приводит к выводу сбережений

---

[38] См.: Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 27–31.

[39] См.: Куликова К. Россия намайнила серебро. Она вышла на второе место в мире по производству криптовалют // Коммерсант. 2023. 7 апреля. Режим доступа: https://www.kommersant.ru/doc/5915688 (дата обращения – 10.04.2023).

[40] См.: Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 10–12.

граждан за периметр российского финансового сектора и, как следствие, сокращению его возможностей по финансированию реального сектора и снижению потенциального роста экономики, что, как результат, уменьшает количество рабочих мест и потенциал роста доходов граждан. Криптовалюты активно используются в противоправной деятельности (отмывание доходов, наркоторговля, финансирование терроризма и т.д.). Их распространение создает благоприятные условия для незаконных финансовых операций, а также для совершения таких преступлений, как вымогательство и взяточничество, и является вызовом для глобальной системы противодействия отмыванию денег и финансированию терроризма (далее — ПОД/ФТ). По мнению специалистов Центрального банка Российской Федерации, обеспечить необходимую прозрачность обращения криптовалют невозможно, вследствие чего глобальный подход к регулированию криптовалют пока окончательно не сформирован. Во многих странах деятельность по обращению криптовалют находится в так называемой «серой» зоне, но в целом можно отметить тенденцию к ужесточению регулирования. Так, например, ряд стран уже ввел запрет на использование криптовалют (например, Китай) или планирует ввести такой запрет (например, Индия), некоторые страны (например, Китай, Иран) установили также запрет на осуществление майнинга. Другие страны разрешают работу криптовалютных бирж, но планомерно ужесточают к ним требования в части ПОД/ФТ и т.д. Потенциальные риски финансовой стабильности, связанные с криптовалютами, значительно выше для стран с формирующимися рынками, в том числе для России, в частности, из-за традиционно более высокой склонности к валютизации и недостаточного уровня финансовой грамотности. Страны, в особенности с резервными валютами, пока могут позволить себе более мягкое отношение к криптовалютам, следуя по пути постепенного расширения охвата регулирования. При этом более жесткий подход реализуется по отношению к необеспеченным криптовалютам, чем к стейблкойнам. Вместе с тем

скоординированная реакция ведущих стран по недопущению запуска глобального стейблкойна Либра (Libra), который мог представлять более серьезную угрозу для их финансовых систем, показывает крайне настороженное отношение регуляторов и к стейблкоинам[41], так как стейблкойны могут использоваться как альтернатива фиатным деньгам, а также с целью легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем.

Периодически имеют место случаи, когда участники сетей блокчейн открывают так называемые «корпоративные» криптокошельки. Иногда происходит смешение понятий «корпоративный» криптокошелек и «корпоративный» блокчейн до степени их отождествления. Однако это не так. «Корпоративный» блокчейн — это сеть блокчейнов, которая может быть интегрирована и использована для целей определенной организации. Понятие же «корпоративный» криптокошелек вовсе не означает, что им владеет юридическое лицо, имеющее четкое правовое определение в гражданском законодательстве. К таковым относятся либо организация, имеющая обособленное имущество и отвечающая им по своим обязательствам, которая может от своего имени приобретать и осуществлять гражданские права, а также нести гражданские обязанности, быть истцом и ответчиком в суде. Такое юридическое лицо должно существовать в одной из организационно-правовых форм, предусмотренных Гражданским кодексом Российской Федерации, и быть зарегистрировано в едином государственном реестре юридических лиц.

Если владельцам криптокошелька выступает именно юридическое лицо, то в случае совершения имущественного преступления (хищения) в отношении принадлежащих ему криптомонет именно оно и выступает в качестве потерпевшего. Однако понятие «корпоративный» криптокошелек подразумевает не принадлежность его какому-либо юридическому лицу, а

---

[41] См. Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 11–29.

использование его несколькими физическими лицами, имеющими от него пароль. При этом не все эти лица юридически могут иметь права на находящиеся в таком криптокошельке криптомонеты. Часть из них могут осуществлять техническую поддержку, не являясь при этом собственниками криптомонет. В таком случае при совершении их хищения потерпевшим будет выступать их фактический собственник, которому непосредственно причинен имущественный вред. Действия, направленные на хищение криптовалюты из криптокошелька в зависимости от способа хищения могут образовывать состав преступления, предусмотренного ст. 158 УК РФ (кража).

Правоохранительные органы в отсутствие законодательно установленной системы отслеживания крипто-финансовых потоков и информации об идентифицированных держателях цифровых валют не могут не только эффективно реагировать на преступления, совершаемые с их использованием, но, по сути, лишены возможности выявления указанных преступлений и их учета[42]. Кроме того, общественную опасность указанных преступлений усиливает специфика способа их совершения предполагающая возможность удаленного доступа к криптокошельку при помощи технических средств, что позволяет лицу оставаться анонимным и совершать преступление из любой точки мира, имея лишь доступ к телекоммуникационной сети Интернет. По мнению прокуратуры Республики Коми, «при квалификации компьютерных преступлений, совершаемых в сфере оборота криптовалюты, основным непосредственным объектом будут являться именно криптовалюта и криптовалютные отношения, а посягательство на нормальное функционирование компьютерной информации будет выступать в качестве дополнительного объекта»[43]. Нельзя полностью согласиться с данным утверждением, так как непосредственно криптовалюта не может являться

[42] «Концепция законодательного регламентирования механизмов организации оборота цифровых валют». СПС Консультант-плюс (дата обращения – 14.04.2023).

[43]См.: Официальный сайт прокуратуры Республики Коми. Режим доступа: https://epp.genproc.gov.ru/web/proc_11/sections?section=25924455 (дата обращения – 01.05.2022).

объектом преступления вследствие того, что не относится к общественным отношениям, охраняемым уголовным законом, которым преступлением причиняется вред либо создается реальная угроза причинения такого вреда. По сути, происходит смешение таких понятий, как предмет преступления, то есть неких доступных для восприятия человеком измерений, фиксации и оценки явлений (элементов) внешнего мира (материальной вещи или интеллектуальной ценности), путем воздействия на которые причиняется или может быть причинен вред объекту посягательства, и объект преступления, под которым понимаются охраняемые уголовным законом общественные отношения, которым преступлением причиняется вред или создается непосредственная угроза причинения вреда. Понятие же «криптовалютные отношения» не закреплено в действующем законодательстве, вследствие чего может иметь произвольное толкование и относиться к непосредственному объекту преступления. Как правило, при совершении таких преступлений криптовалюта выступает в качестве предмета преступления, так как целью лица, совершающего такие преступления, является получение криптовалюты. Но при этом действительно встает вопрос о необходимости дополнительной квалификации в соответствии с главой 28 Уголовного кодекса Российской Федерации.

Смешивание объекта и предмета преступления при осуществлении квалификации преступлений, совершаемых с использованием криптовалюты, происходит по причине присутствия правовой неопределенности самого понятия «криптовалюта», вследствие чего правоприменитель не всегда может разграничить объект и предмет таких преступлений и, соответственно, осуществить правильную квалификацию совершенного деяния.

Добросовестный участник любых не запрещенных законом экономических отношений имеет право на защиту его прав и законных интересов со стороны государства, в том числе и средствами уголовно-правового регулирования. В целях защиты прав и законных интересов добросовестных участников криптовалютного рынка необходимо внести

изменения в статью 128 Гражданского кодекса Российской Федерации, указав цифровую валюту в качестве объекта гражданских прав. Такие изменения не только позволят на законодательном уровне наиболее точно раскрыть понятие криптовалюты исходя из ее основных свойств, но и идентифицируют ее как самостоятельный объект гражданского права, что является необходимым условием функционирования регуляторно-правового механизма защиты прав добросовестных участников криптовалютного рынка путем использования регулятивной функции уголовного права.

Таким образом, можно констатировать, что криптовалюта в зависимости от способа совершения преступления может выступать:

1. Предметом хищений.
2. Предметом подкупа и взятки.
3. Предметом легализации (отмывания).
4. Средством финансирования незаконной деятельности.
5. Средством совершения других преступлений против личности, общественной безопасности и т.д. в качестве суррогатного средства платежа.

Учитывая, что способ совершения преступлений является элементом объективной стороны, разграничение преступлений с использованием криптовалюты будет осуществляться по их объективной стороне[44]. При это следует учитывать следующую особенность объективной стороны указанных преступлений: завладение имуществом в результате преступных действий, даже соединенных с насилием, предметом которых является криптовалюта, происходит не в реальном, а исключительно в виртуальном пространстве.

---

[44] См.: Санташов А.Л. Проблемы противодействия хищению денежных средств с банковских счетов, а равно в отношении электронных денежных средств // Пенитенциарная система России в современных условиях развития общества: от парадигмы наказания к исправлению и ресоциализации: Сборник материалов международной научно-практической конференции. В 3-х частях. Вологда, 09–11 декабря 2021 года / Под общей редакцией В.Н. Некрасова. Вологда, 2022. С. 111–115.

§ 1.2. Способы совершения преступлений с использованием криптовалюты как элемент объективной стороны преступления

По сравнению с другими факультативными признаками состава преступления именно способ совершения, то есть определенная совокупность и последовательность используемых при совершении преступления приемов, методов и последовательность совершения преступных действий и применения средств воздействия на предмет посягательства, чаще всего находит отражение в законодательных конструкциях уголовно-правовых норм. Говоря о средствах, всегда имеют в виду их материальное воплощение. Так, например, по мнению А.Б. Чугунка, применительно к уголовному праву, не может идти речи о нематериальных средствах, «поскольку средства совершения преступления рассматриваются как элементы объективной стороны состава преступления»[45]. К таковым можно отнести предметы, энергию, различные химические вещества, физические, химические или иные свойства которых используются для совершения преступления. Однако нельзя не отметить, что при совершении преступлений с использованием криптовалюты средства их совершения могут такими свойствами не обладать, так как не относятся к предметам материального мира, а существуют в виде цифрового компьютерного кода и не имеют общепринятого материального воплощения.

Как уже было сказано выше, конструкции составов преступлений, совершаемых с использованием криптовалюты, имеют определенную особенность, что непосредственно связано с совершением части действий, образующих объективную сторону состава таких преступлений, в виртуальной среде с использованием технологии блокчейн.

---

[45] Чугунок А.Б. Понятие и значение орудий и средств совершения преступления в уголовном праве // Вопросы юридической техники в уголовном и уголовно-процессуальном законодательстве. Сб. науч. ст. Ярославль, 1997. С. 101.

Таким образом, применение блокчейн-технологии при совершении преступлений с использованием криптовалюты и программные средства, с помощью которых такое использование происходит, относятся к признакам объективной стороны и непосредственно влияют на квалификацию преступления.

Можно полностью согласиться с мнением П.Н. Кобеца относительно того, что «объективная сторона – это внешнее проявление преступления, то есть проявление преступления вовне, представляющее собой совокупность внешних, объективных признаков (обстоятельств) преступления, характеризующих посягательство на его объект и поддающихся восприятию, установлению и доказыванию»[46].

Характерной особенностью объективной стороны преступлений, совершаемых с использованием криптовалюты, является совершение действий, которые поддаются восприятию, установлению и доказыванию в виртуальном пространстве, в том числе в блокчейн-сетях, технологическую основу функционирования которых образует совокупность определенных принципов, позволяющих отграничивать блокчейн-сети от других видов программного обеспечения.

Сам термин «Блокчейн» впервые появился в качестве названия распределённой базы данных, которая была реализована в криптовалюте «Биткойн». Термин «Блокчейн» происходит от англ. «Blockchain» («block» – блок, «chain» – цепочка) и означает цепочку блоков транзакций, выстроенную по строго определённым правилам, по которым каждый новый блок связан с предыдущим. Каждый блок содержит в себе определенный набор транзакций. Вновь сформированные блоки добавляются в конец цепи. Таким образом, вся история работы сети хранится в результирующем обобщенном блоке.

---

[46] См.: Кобец П.Н. О проблеме испытательного срока в механизме условного осуждения // Российская юстиция. 2009. № 9. С. 14.

Построение такой цепи основано на принципах распределённости, открытости и защищённости. Эти три принципа лежат в основе данной технологии и предполагают, что все пользователи блокчейн образуют между собой некую компьютерную сеть. На каждом из таких компьютеров хранится копия данных блокчейн. Как правило, это полная копия всех блоков, но в принципе могут храниться лишь нужные на данном компьютере сведения. Такой способ хранения данных практически исключает возможность их потери, так как для этого необходимо уничтожить данные на всех компьютерах данной цепи. Соответственно, каждый новый пользователь, расширяя данную сеть, укрепляет её неуязвимость.

Указанная технология направлена на максимальное недопущение совершения преступлений с криптовалютой в виртуальной сети, что в свою очередь является одной из составляющих ее привлекательности для пользователей. Кратко рассмотрим каждый из принципов, на которых данная технология основывается и которые являются определяющими для разграничения криптовалюты и других разновидностей цифровой валюты.

Принцип распределенности заключается в том, что все пользователи сети считаются полностью равноправными по отношению друг к другу вне зависимости от количества криптомонет, находящихся в его крипто-кошельке. Нет организаторов, модераторов сети, каких-либо иных контролеров, то есть присутствует независимость каждого конкретного пользователя. Все данные блоков блокчейн и их содержание являются открытыми, что позволяет любому прочитать соответствующую информацию, посмотреть цепочку и отследить информационные изменения, происходящие в ней.

Принцип защищенности реализуется в блокчейн последовательностью специальных ссылок, формируемых ХЭШ-функцией, то есть процессом преобразования входной информации свободной длины в исходящую битную строчку с конкретным размером через детерминированную схему. Криптографическая ХЭШ-функция представляет собой математический алгоритм, который отображает данные произвольного размера в битовый

массив фиксированного размера. Результат, производимый ХЭШ-функцией, называется «ХЭШ-суммой» или же просто «ХЭШем». ХЭШ, применительно к криптовалюте, — это зашифрованная информация (набор соответствующих символов), которая была преобразована по определённому алгоритму с введенной входной информации, то есть формируется информационный блок, не подлежащий дальнейшему изменению ни при каких условиях. Каждый блок ссылается на предыдущий и так далее вплоть до первого.

Исходя из действующего законодательства Российской Федерации, каждый сформированный блок, то есть каждую оконченную транзакцию, можно рассматривать как некий электронный документ, позволяющий сделать вывод об оконченном преступлении в случае совершения такового.

Так, пункт 11.1 статьи 2 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предусматривает, что электронный документ представляет собой документированную информацию, которая представлена в электронной форме, то есть в виде, пригодном для ее восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Как и документ на бумажном носителе, электронный документ имеет ряд реквизитов, подтверждающих его подлинность. ХЭШ или TxID (идентификационный номер, маркирующий каждую транзакцию в сети блокчейн), являясь уникальной для каждой криптовалютной транзакции последовательностью символов, основываясь на пункте 11.1 статьи 2 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» необходимо рассматривать как электронный документ. Данный электронный документ состоит из буквенно-цифровых символов и представляет собой идентификационный номер, указанный для каждой криптовалютной транзакции. Любая проведенная криптовалютная транзакция имеет такой уникальный идентификатор, позволяющей рассматривать его как

электронный документ, имеющий доказательственное значение по расследуемому уголовному делу. Используя TxID, можно проследить историю транзакций любой криптомонеты.

Принцип открытости предполагает возможность любого пользователя блокчейн увидеть любые транзакции, имевшие место в данной сети. Используя данный принцип, следователь имеет возможность визуально проследить любую интересующую его транзакцию, зафиксировав данную информацию любыми доступными ему средствами фиксирования (фото, видео, скриншот экрана). При этом увидеть данные владельцев анонимных криптокошельков не представляется возможным.

Сам процесс создания криптомонет, так называемый «майнинг», оставляет определенные «электронные» («цифровые», «виртуальные») следы в соответствующем блокчейне (например, в блокчейне биткоина). В совокупности данные следы, имея доказательное значение по уголовному делу, определяют тот или иной способ совершения преступления с использованием криптовалюты, могут быть выявлены, зафиксированы и использованы в процессе квалификации соответствующих преступлений.

В каждой транзакции обрабатываются два компонента. Первый компонент разблокирует биткоины, заблокированные в предыдущих транзакциях, используя для этого данные о получении ранее пользователем этих биткоинов, то есть тех, которые в данный момент он хочет переслать (inputs). Второй компонент транзакции состоит из данных об адресате, пересылаемых пользователем биткоинов (outputs). Выходы блокируют транзакцию для следующего получателя. Выходы содержат ХЭШ, полученный на основе открытого ключа. Таким образом, в каждой транзакции биткоины передвигаются от «входов к выходам». При этом «майнер» имеет право на получение комиссии, равной разнице между разблокированным входом (inputs), но не заблокированным в выходе (outputs). Эта комиссия предусмотрена самим пользователем, пересылающим биткоины, хотя она может и быть равной нулю. В последнем случае такие транзакции, как

невыгодные, могут надолго «зависнуть» в сети, то есть будут переданы позже транзакций с вознаграждением. Так называемые «пиры»[47] сети, принадлежащие «майнерам», определяют на основе своих алгоритмов правила отбора и обработки поступающих транзакций. Именно эта причина и заставляет пользователей включать комиссию – то есть делать «inputs» (входные ресурсы) больше «outputs» (выходных ресурсов). Таким образом, «майнеры» зарабатывают, создавая блоки и обрабатывая транзакции. Награда за это состоит из двух частей: первая – новые сгенерированные монеты (эмиссия), вторая – комиссия за транзакцию (transaction fee), то есть операционный сбор или комиссия за перевод.

«Майнер», получив транзакции от других участников сети, собирает их вместе, формирует заголовок будущего блока и рассчитывает ХЭШ блока, который также называется ключом блока. Ключ каждого блока рассчитывается с использованием данных всего блока и ключа предыдущего блока. Это значит, что в ключе любого блока закодированы не только записи данного блока, но и все предыдущие блоки. Блоков, созданных одновременно различными «майнерами», может быть несколько. В этом случае из представленных «майнерами» блоков выбирается «лучший». Если полученный блок является «лучшим», то его присоединяют в «хвост» блокчейна, если «не лучшим» – отбрасывают.

Теперь встает вопрос о критериях определения «лучшего» блока. Можно выделить три основные характеристики, анализируемые при формировании блокчейн.

Первой характеристикой является время представления блока. Эта характеристика направлена на увеличение производительности обработки данных в сети.

---

[47] Пир (англ. peer – соучастник) – общее название участника сети, построенной по принципу обмена файлами, который хранит на своем компьютере файлы, предоставляя к ним доступ другим участникам и взамен получая от них аналогичные файлы с компьютеров других участников такого обмена.

Второй характеристикой является размер блока. Чем больше транзакций он в себя включает, тем лучше. Эта характеристика также направлена на увеличение производительности обработки транзакций.

Третья характеристика определяется содержанием значения ХЭШ-функции. Если добавить в хэшируемые данные некоторое значение, называемое «nonce», то результат хэширования изменится. Поскольку результатом хэширования является некоторая последовательность нулей и единиц фиксированной длины, два представленных варианта значений ХЭШ-функции для различных значений «nonce» будут отличаться друг от друга. Их можно сравнить математически. В блокчейн выбран критерий минимального значения: лучше тот вычисленный ХЭШ, который меньше. Хотя, с математической точки зрения, с тем же успехом можно было бы принять и правило наибольшего ХЭШа. При этом определенное однажды правило уже не должно изменяться при функционировании сети. Эта характеристика направлена на обеспечение целостности, непротиворечивости и достоверности данных блокчейн. Введя соревновательный элемент, технология блокчейн, во-первых, стимулирует увеличение количества участников, во-вторых, направлена на исключение монополии реализации блоков, в-третьих, обеспечивает возможность проверки целостности данных любым пользователем.

В результате получаем следующее правило: если блок «лучший» и присоединен к блокчейну, то за эту работу «майнер» получит соответствующее вознаграждение в виде биткоинов (помимо комиссии). Если блок присоединен к блокчейну, то все транзакции, отраженные в блоке, считаются выполненными. После этого обычные пользователи получают новый блок и сохраняют его у себя с целью корректного создания своих записей и достоверной проверки новых чужих записей[48]. Считающийся официальным создателем Биткойна Сатоши (Сатоси) Накамото в своей статье

[48] См.: Самолысов П.В. Правовое регулирование майнинга криптовалют // Право и цифровая экономика. 2020. № 3(09). С. 13–20.

«Биткоин: цифровая пиринговая наличность»[49] пишет о том, что, по умолчанию, именно первая транзакция в блоке является специальной, которая создает новую монету, принадлежащую создателю данного блока. Такая схема является поощряющей для участников, стимулируя их к поддержанию работы сети, а также решает вопрос о начальном распределении криптомонет в отсутствие центрального эмитента. Равномерное увеличение числа монет в обращении можно сравнить с добычей золота, в которую золотоискатели тоже вкладывают свои ресурсы. В роли последних в нашем случае выступают процессорное время и электричество.

Необходимо привести и альтернативную точку зрения относительно осуществления «майнинга» и обращения криптовалют, тем более что данная точка зрения является официальной позицией Центрального банка Российской Федерации, выраженной им в официальном докладе для общественных консультаций: «Криптовалюты: тренды, риски, меры»[50]. Центральный банк Российской Федерации полагает, что деятельность, связанная с «майнингом» и оборотом криптовалюты, повышает вовлеченность населения страны и ее экономики криптовалютный рынок. Указанная деятельность несет существенные риски для экономики и финансовой стабильности государства, так как дополнительно создает непроизводительный расход электроэнергии, который ставит под угрозу энергообеспечение жилых помещений, зданий социальной инфраструктуры и предприятий, создает угрозу дополнительной криминализации экономики способствуя появлению новых способов хищения чужого имущества. Аналогичной точки зрения придерживаются и некоторые ученые. Так, например, А.А. Коренная выделяет способы хищения криптовалюты с использованием криптокошельков для ее хранения в самостоятельную группу преступлений, подчеркивая при этом, что

---

[49] См.: Накамото С. Биткойн: система цифровой пиринговой наличности. Режим доступа: https://opartnerke.ru/wp-content/uploads/2017/12/belaya_kniga_bitcoina_satoshi_nakamoto.pdf (дата обращения - 02.02.2021).

[50] См. Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 20.

фактически только некоторые преступные посягательства можно квалифицировать по ст. 159 УК РФ, то есть признавать мошенничеством[51]. С таким утверждением можно согласиться.

На сегодняшний день по способу функционирования и использования существующие криптокошельки можно разделить на две группы: онлайн или программные кошельки, то есть кошельки, существующие в виде определенной компьютерной программы, и аппаратные кошельки, существующие в виде микросхемы, работающей с определенной компьютерной программой-приложением.

В зависимости от места расположения криптокошельки можно разделить на четыре вида: локальные, мобильные, онлайновые и отличные от них аппаратные криптокошельки. Первые три вида криптокошельков относятся к группе программных, а последний является комбинированным или так называемым аппаратным (см. приложение № 3).

Если при совершении действий, получивших условные названия «Атака», «Атака-51», «Атака Финни», «Эгоистичный майнинг», «Атака Сибиллы», осуществлялся обман собственника криптомонет относительно характера вышеуказанных действий, то есть сообщением ему сведений, изначально не соответствующих действительности, содеянное следует квалифицировать как мошенничество, в остальных случаях как кражу, так как в данном случае обман не направлен непосредственно на завладение чужими криптомонетами, а используется только для облегчения доступа к чужому криптокошельку.

Необходимо также отметить, распространение такого сравнительно нового для России явления, как незаконный «майнинг» («криптоджекинг»). Суть данного явления состоит в следующем. «Майнинг» различного вида криптовалют становится достаточно популярным, но для осуществления такого рода деятельности требуется соответствующее оборудование. Далеко

---

[51] См.: Коренная А.А. Квалификация преступлений, совершаемых с использованием криптовалюты // Проблемы экономики и юридической практики. 2018. № 3. С. 221.

не всегда затраченные на приобретение оборудования для «майнинга» и электроэнергию денежные средства будут возвращены, а тем более возвращены с прибылью. То есть для осуществления беспроигрышного «майнинга» необходимо найти какой-либо способ, не требующий предварительных финансовых вложений. И такой способ есть. И даже два. Первый способ – это непосредственное использование сторонних мощностей для «майнинга» криптовалюты. При таком способе генерации криптовалюты «майнер» использует компьютерное оборудование иного лица без его согласия на совершение указанных действий. Использование сторонних мощностей для «майнинга» криптовалюты не образует состава преступления, предусмотренного действующим УК РФ, тем более что при этом не всегда такое использование приводит к невозможности решения непосредственных задач, для которых такое оборудование предназначено. Сам процесс «майнинга» может осуществляться с использованием, например, 30–50 % мощности компьютера или локальной сети, что не препятствует решению основных задач, для которых они предназначены[52]. То есть, по сути, отсутствует общественная опасность данного явления как такового, что в свою очередь не позволяет говорить о данном явлении как о преступлении. Тем не менее, при применении «криптоджекинга» могут быть совершены другие преступления, в том числе предусмотренные главой 28 УК РФ.

Случаи использования недобросовестного «майнинга» в качестве способа совершения преступления имели место на территории России. Так, по сообщению информационного издания РБК, сотрудники расположенного в Сарове Всероссийского научно-исследовательского института экспериментальной физики (РФЯЦ-ВНИИЭФ) были задержаны за попытку несанкционированного использования служебных вычислительных мощностей в личных целях, в том числе для «майнинга». В настоящее время городской суд города Сарова вынес приговор в отношении сотрудника

---

[52] См: Перов В.А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют // Безопасность бизнеса. 2018. № 2. С. 26.

Всероссийского научно-исследовательского института экспериментальной физики (РФЯЦ-ВНИИЭФ), который пытался осуществить «майнинг» криптовалюты биткоин, используя оборудование и электроэнергию предприятия, на котором он выполнял свои трудовые обязанности. На сайте Саровского городского суда имеется информация о том, что «обвинительный приговор вынесен по двум статьям Уголовного кодекса – ч. 1 ст. 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей) УК РФ и ч. 3 ст. 272 (неправомерный доступ к компьютерной информации) УК РФ»[53].

Использование для добычи криптовалют корпоративных мощностей является довольно распространенной практикой[54]. Так, например, Председатель правления Сбербанка Г. Греф характеризует инциденты, когда сотрудников банка уличают в «майнинге», как довольно частые[55].

Квалифицируя преступления, связанные с недобросовестным майнингом, необходимо выяснять мотивы субъекта преступления и цель, которую данный субъект хотел достигнуть. Использование «майнер-вируса»[56], то есть внесение изменений в компьютерную информацию для достижения способности к взаимодействию с другими программами, которые хранятся на данном компьютерном устройстве, необходимо квалифицировать по ч. 1 ст. 273 УК РФ. Если при этом собственнику или владельцу компьютерного устройства причинен крупный ущерб, то такое преступление необходимо квалифицировать по ч. 2 ст. 273 УК РФ. Аналогичные разъяснения содержатся в Постановлении Пленума Верховного Суда

---

[53] См.: Перов В.А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют // Безопасность бизнеса. 2018. № 2. С. 26.

[54] Там же.

[55] См.: Герман Греф уличил сотрудников Сбербанка в майнинге на рабочем месте. Режим доступа: https://www.kommersant.ru/doc/3541751 (дата обращения – 05.05.2023).

[56] «Майнер-вирус» – компьютерная программа, позволяющая осуществлять неправомерный доступ к информационно-телекоммуникационным сетям для модификации компьютерной информации.

Российской Федерации от 15 декабря 2022 года № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть ”Интернет”», в соответствии с которыми уголовную ответственность по ст. 273 УК РФ влекут действия по созданию, распространению, а также использованию именно вредоносных компьютерных программ либо иной компьютерной информации, которые заведомо для лица, совершающего указанные действия, предназначены для несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Осуществляя квалификацию по ч. 2 ст. 273 УК РФ необходимо выяснить, в чем данный ущерб выражается. В случаях когда компьютерное оборудование задействовано процессом «майнинга» полностью и не позволяет решать основные задачи по роду деятельности предприятия (организации), собственника такого оборудования, можно вести речь о неполученных или недополученных доходах, которые такое предприятие получило бы при обычных условиях использования данного оборудования, если бы его право не было нарушено использованием этого оборудования с целью «майнинга» в пользу третьих лиц. То есть имеет место упущенная выгода, но только в том случае, если результаты использования компьютерного оборудования могли повлиять на получаемой предприятием доход. Если же «майнинг» не препятствовал решению основной задачи, говорить об упущенной выгоде, конечно, нельзя. Однако сам процесс «майнинга» будет связан с расходованием дополнительной электроэнергии, то есть причинением собственнику имущественного ущерба в виде дополнительной оплаты электроэнергии, затраченной непосредственно на «майнинг». В этом случае необходима дополнительная квалификация по ст. 165 (причинение имущественного ущерба путем обмана или злоупотребления доверием) УК

РФ. Диспозиция указанной статьи предусматривает ответственность за причинение собственнику (владельцу) имущества имущественного ущерба путем обмана при отсутствии признаков хищения, совершенного в крупном размере, то есть в сумме не менее 250 000 руб. Указанный вывод соотносится с разъяснениями, которые даны в постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в соответствии с которыми от мошенничества следует отличать причинение имущественного ущерба путем обмана или злоупотребления доверием при отсутствии признаков хищения (ст. 165 УК РФ). В таком случае в своей совокупности либо отдельно отсутствуют такие обязательные признаки мошенничества, присущие любому виду хищения, как противоправное, совершенное с корыстной целью, безвозмездное изъятие либо обращение чужого имущества в пользу виновного либо других лиц.

При решении вопроса о том, имеется ли в действиях лица состав преступления, предусмотренного ст. 165 УК РФ, следует установить, действительно ли причинен собственнику или владельцу имущества реальный материальный ущерб или ущерб в виде упущенной выгоды, то есть неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено путем обмана или злоупотребления доверием, и превышает ли сумма ущерба двести пятьдесят тысяч рублей. Субъективная сторона преступления характеризуется прямым конкретизированным умыслом, направленным на причинение имущественного ущерба путем обмана с целью извлечения материальной выгоды в свою пользу или пользу третьих лиц за счет собственника (владельца) указанного оборудования. При этом признаки хищения отсутствуют.

Таким образом, на основании изложенного, учитывая умысел на причинение собственнику имущественного ущерба путем использования электроэнергии, им оплаченной, можно сделать вывод, что действия

подобного рода могут образовывать состав преступления, предусмотренного ст. 165 УК РФ.

Однако при этом проблема будет заключаться именно в определении размера причиненного ущерба. Каким образом можно рассчитать стоимость затраченной именно на «майнинг» электроэнергии пока не совсем понятно. Может быть использована методика, основанная на принципе исчислении разницы между затратной частью до установки «майнер-вируса» на компьютерное оборудование и после такой установки и начала его работы.

Второй способ недобросовестного «майнинга» – это использование вредоносной компьютерной программы-вируса, которая позволяет задействовать определенный процент вычислительной мощности зараженного компьютера для осуществления майнинга другим лицом.

В настоящие время уже существуют, и довольно успешно, так называемые «майнер-вирусы», позволяющие создавать целые компьютерные ботнет-сети[57]. Такие сети дают возможность определенным лицам удаленно управлять зараженными компьютерами и осуществлять, используя компьютерные мощности других лиц майнинг в своих интересах[58]. При этом заражение компьютера может произойти не только посредством просмотра сомнительных сообщений или сайтов. Так, например, некоторые смартфоны имеют уже предустановленные «скрипты» (программы, автоматизирующие некоторые задачи), посредством которых происходит автоматическая загрузка «вируса-майнера». Антивирус здесь, как правило, бессилен, хотя некоторые антивирусные программы все же распознают «программу-майнер», определяют ее как вирус и удаляют. Но это в итоге ни к чему не приводит. Установленный на устройстве «скрипт» обращается к соответствующему

[57] Ботнет (англ. Botnet) – компьютерная сеть, в которой каждое устройство, имеющее доступ в Интернет, заражено вредоносной программой, которая позволяет злоумышленнику выполнять определенные действия с использованием ресурсов заражённого компьютерного устройства.

[58] См.: Перов В.А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют // Безопасность бизнеса. 2018. № 2. С. 25–29.

ресурсу и загружает «вирус-майнер» вновь. Для того чтобы от этого избавиться, нужно полностью перепрограммировать («перепрошить») смартфон. Как показывают исследования Лаборатории Касперского, смартфон наиболее подвержен заражению вредоносными программами по причине более простой установки на него вредоносного программного обеспечения. Скрытый «майнер-вирус» можно установить на смартфон, запустив совершенно безобидное на вид приложение из официального магазина «Google Play»[59]. Также «майнер-вирус» может быть уже предустановлен в смартфонах, реализуемых через торговую сеть[60]. По принципу предустановки программы «майнер-вируса» работают некоторые смартфоны китайской сборки[61]. При этом кроме майнинга вирусная программа может самостоятельно обращаться к другим сервисам, подключать платные подписки, и такие случаи зафиксированы неоднократно. Признаками, позволяющими определить работу скрытого «вирус-майнера», являются постоянный нагрев батареи питания смартфона и резкое увеличение расходования интернет-трафика при том же режиме использования, что и ранее.

«Майнер-вирус», в отличие от других вредоносных программ, как правило, не мешает работе компьютера, если не считать замедления его скорости работы (быстродействия). Целью такой вирусной атаки является лишь установка программного обеспечения для майнинга и использования в указанном процессе части его вычислительных мощностей. «Вирус-майнер», являясь определенной компьютерной программой, после установки на компьютерное устройство получает возможность использовать системные

---

[59] См.: Нысанбаева С.Е., Нюсупов А.Т., Манас Ж.Б. Создание инструмента для выявления сетевых вирусов-майнеров на основе криптовалюты monero // Проблемы оптимизации сложных систем: материалы XIV Международной Азиатской школы-семинара (Алматы, 20–31 июля 2018 года). Алматы, 2018. С. 113–119.

[60] См.: Перов В.А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют // Безопасность бизнеса. 2018. № 2. С. 25–29.

[61] См.: Исаев А.С. Китай в мировом киберпространстве // Проблемы Дальнего Востока. 2020. № 4. С. 6–23.

ресурсы компьютера, которые задействуются при открытии программ и приложений, а также при автозагрузке. Также «вирус-майнер» получает доступ к оперативной памяти компьютера, его процессору, а в определенных случаях и к другому подключенному к компьютеру оборудованию, получая возможность использования данных ресурсов. Неправомерный доступ может быть осуществлен двумя способами: либо заставить жертву перейти по вредоносной ссылке в электронном письме, что приведет к загрузке вредоносного кода для осуществления майнинга на компьютер стороннего пользователя, либо внедрить на вебсайт или в интернет-рекламу вредоносного кода JavaScript, который автоматически запускается после загрузке в браузер компьютера. Такие скрипты (компьютерные программы, выполняющие определенную конкретную задачу, и применяющиеся, как правило, для автоматизации повторяющихся действий) отличаются от других вредоносных программ только тем, что не повреждают информацию, имеющуюся в компьютере пользователя, а модифицируют ее. При этом как в первом, так и во втором случае такое использование может привести к невозможности решения непосредственных задач, для которых такое оборудование предназначено, и значительному расходованию электроэнергии[62].

Так, например, в 2018 году «криптоджекинговой» атаке была подвергнута европейская система управления водоснабжением, что серьезно повлияло на способность операторов управлять всей системой и принесло довольно значительные убытки. Это был первый известный случай использования «криптоджекинга». В том же 2018 году был обнаружен код «криптоджекинга» на странице отчета об убийствах газеты Los Angeles Times. Когда посетители переходили на страницу отчета об убийствах, их устройства использовались для майнинга криптовалюты монеро (monero)[63]. Эту угрозу не удавалось обнаружить в течение длительного времени, поскольку

---

[62] См.: Черниговский А.В., Кривов М.В. Проблема майнинга в корпоративной среде // Вестник Ангарского государственного технического университета. 2021. № 15. С. 123.

[63] См.: Савицкий А.А. Судебная финансово-экономическая экспертиза операций с криптовалютой манейро // Вестник криминалистики. 2020. № 2(74). С. 75–80.

вычислительная мощность, которую использовал скрипт, была минимальной, и многие пользователи не осознавали, что их устройства скомпрометированы[64].

В июле — августе 2018 года в результате «криптоджекинговой» атаки было заражено более 200 000 маршрутизаторов MikroTik в Бразилии, в результате чего код CoinHive был внедрен в огромный объем проходящего через них веб-трафика[65].

В 2019 году из Microsoft Store было удалено восемь отдельных приложений, которые скрытно добывали криптовалюту за счет ресурсов загрузивших их пользователей. Потенциальные жертвы могли загрузить приложения для «криптоджекинга» при поиске приложений по ключевым словам в Microsoft Store либо из списка лучших бесплатных приложений. При загрузке и запуске приложений происходила загрузка кода JavaScript для «криптоджекинга». После этого на устройстве активировался «майнер-вирус» и начинался майнинг криптовалюты монеро с использованием значительной части ресурсов устройства, что замедляло его работу[66]. Замедление работы компьютерного устройства в ряде случаев не позволяло пользователю такого устройства решать определенные профессиональные задачи, для которых данное компьютерное устройство изначально предназначалось[67]. Если имеется целая сеть персональных компьютеров, зараженных «майнер-вирусом» (ботнет), то она может заменить целый «пул»[68], а это уже достаточно

---

[64] См.: Ивличев П. С. Незаконные методы снижения издержек в процессе криптовалютного майнинга // Математические методы и информационно-технические средства: Материалы XVI Всероссийской научно-практической конференции (Краснодар, 19 июня 2020 года). Краснодар, 2020. С. 57–60.

[65] См.: Пузиков Е.В., Лапсарь А.П. Вредоносный майнинг (криптоджекинг) – новая угроза информационной безопасности // Информационные системы, экономика и управление: ученые записки. Выпуск 24. Ростов-на-Дону, 2022. С. 70–77.

[66] См.: Лаборатория Касперского. Что такое криптоджекинг – определение и описание. Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cryptojacking (дата обращения – 06.05.2022).

[67] См.: Пузиков Е. В., Лапсарь А. П. Указ. соч. С. 71.

[68] Пул (англ. Pool) – объединение мощностей отдельных компьютеров для решения определенной задачи.

большой ресурс для майнинга за счет иных лиц, которые оплачивают электроэнергию, потребляемую на процесс майнинга их машинами. Такой незаконный «пул» может быть создан посредством последовательной установки вредоносной программы на компьютерные устройства одного собственника, например, организации, располагающей большими вычислительными мощностями.

Установленная на компьютерном оборудовании антивирусная программа как правило на такие действия не реагирует, а имеющиеся на компьютере или мобильном устройстве вредоносные объекты используют вычислительные ресурсы для «майнинга» соответствующего вида криптовалюты. «Криптоджекинг» активно развивается по всему миру и поражает любые типы устройств: компьютеры, ноутбуки, смартфоны и даже сетевые серверы[69].

Следует отметить, что некоторые разновидности «майнер-вирусов», помимо непосредственного использования мощностей чужого компьютерного устройства для генерирования криптовалюты, одновременно осуществляют сбор и отправку лицу, использующему такую вредоносную программу, сведений о сообщениях электронной почты владельца компьютера, его аудио-, фото-, видеофайлы, содержащие информацию о его частной жизни. В таком случае можно говорить о совершении преступлений, предусмотренных ст. 137 (нарушение неприкосновенности частной жизни), ст.138 (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений), ст. 273 (создание, использование и распространение вредоносных компьютерных программ) УК РФ.

В качестве примера можно привести преступление, обстоятельства совершения которого изложены в приговоре Собиинского городского суда Владимирской области. N был признан виновным в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ. Виновное лицо использовало

---

[69] См.: Лаборатория Касперского. Что такое криптоджекинг…

компьютерные программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, из корыстной заинтересованности. Реализуя возникший преступный умысел и корыстную цель, действуя умышленно, установил на свой компьютер вредоносные компьютерные программы, заведомо зная, что они предназначены для несанкционированной модификации компьютерной информации. После чего, используя вышеуказанные вредоносные компьютерные программы, предпринял попытку получения несанкционированного удаленного доступа к серверным ЭВМ в целях модификации содержащейся компьютерной информации путем установки компьютерной программы-майнера и использования вычислительных мощностей этих ЭВМ при осуществлении «майнинга» для извлечения имущественной выгоды. Суд квалифицирует действия подсудимого по ч. 2 ст. 273 УК РФ как использование компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенное из корыстной заинтересованности.[70] Необходимо отметить, что «криптоджекинг» является серьезной проблемой для юридических лиц, поскольку организации, подвергнувшиеся «криптоджекингу», несут дополнительные расходы, связанные как с заменой отдельных компонентов или компьютерных систем в целом, так и расходы по дополнительной оплате электроэнергии.

Таким образом, можно констатировать, что определенные способы майнинга представляют общественную опасность, но при этом процесс майнинга никак законодательно не урегулирован, в Уголовном кодексе

[70] См.: Приговор Собинского городского суда по уголовному делу № 1-1-276/2017 от 14 декабря 2017 г. [Электронный ресурс]. Режим доступа: https://sobinsky--wld.sudrf.ru (дата обращения – 16.02.2023).

отсутствует специальная норма, устанавливающая ответственность за выбор общественно опасного способа его (майнинга) осуществления, что подтверждается результатами исследования Банка России, изложенными в опубликованном им докладе для общественных консультаций.[71] Разрешая вопрос о наличии в действиях лиц, осуществляющих недобросовестный «майнинг», признаков состава преступления, необходимо исходить из того, на что был направлен умысел лица, осуществлявшего вышеуказанные действия.

Все представленные выше положения определяют правила установления формы вины в преступлениях, совершаемых с использованием криптовалюты. С целью снижения угроз, обусловленных распространением криптовалют, Банк России предлагает внести следующие изменения в законодательство:

- установить ответственность за нарушение законодательного запрета на использование криптовалют в качестве средства платежа за товары, работы и услуги, продаваемые и покупаемые юридическими и физическими лицами – резидентами Российской Федерации;

- ввести запрет на организацию выпуска и (или) выпуск, организацию обращения криптовалюты (в т.ч. криптобиржами, криптообменниками, P2P-платформами) на территории Российской Федерации и установить ответственность за нарушение данного запрета;

- ввести запрет на вложение финансовых организаций в криптовалюты и связанные с ними финансовые инструменты, а также на использование российских финансовых посредников и российской финансовой инфраструктуры для осуществления операций с криптовалютами и установить ответственность за нарушение данного запрета.

По некоторым видам криптовалют майнинг предполагает в том числе выпуск криптовалюты и/или получение криптовалюты в качестве вознаграждения за валидацию транзакций, что нельзя не учитывать при

---

[71] См.: Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М. 2022. С. 17–19.

рассмотрении предмета доклада, поскольку эта деятельность повышает вовлеченность населения и экономики в целом в криптовалютный рынок. Банк России считает, что текущий масштаб и дальнейшее распространение майнинга криптовалют на территории России несет существенные риски для экономики и финансовой стабильности, так как создает непроизводительный расход электроэнергии, ставящий под угрозу энергообеспечение жилых зданий, зданий социальной инфраструктуры и предприятий, а также реализацию экологической повестки Российской Федерации. Формируется спрос на инфраструктуру для проведения операций с криптовалютами, что усиливает негативные эффекты от распространения криптовалют и создает стимулы для обхода регулирования. В связи с этим, по мнению специалистов Банка России, оптимальным решением является введение в России запрета на майнинг криптовалют. При этом Банк России планирует совершенствовать систему регулярного мониторинга операций с криптовалютами, в том числе проводить совместную работу с финансовыми регуляторами стран, в которых зарегистрированы криптобиржи, чтобы получать информацию об операциях российских клиентов на зарубежных рынках криптовалют[72].

Таким образом, Центральный банк Российской Федерации констатирует в своем докладе значительную долю совершаемых различными способами преступлений с использованием криптовалют, как-то: различного вида мошенничеств при обороте криптовалют, легализация денежных средств или иного имущества, приобретенных другими лицами преступным путем, легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления обозначенным в докладе: отмывание доходов, уклонение от исполнения обязанностей по репатриации денежных средств в иностранной валюте или валюте Российской Федерации, так называемая наркоторговля, то есть преступления, предусмотренные главой 25 (преступления против здоровья

[72] См. Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 35.

населения и общественной нравственности) УК РФ, финансирование терроризма, а также мошенничество в сфере компьютерной информации. Так, например, при осуществлении криптовалютных транзакций одним из способов стимулирования их осуществления может быть комиссия за транзакции. Если входная сумма платежа больше выходной, то разница является комиссией за перевод и прибавляется к базовому значению награды за найденный блок в первой транзакции. Как только суммарный объем денежной массы достигнет заранее установленного максимума, единственным источником поощрения работы над блоками останутся комиссии, при этом избавленные от инфляции[73].

Такая форма стимулирования может также способствовать уменьшению случаев мошенничества, но не исключает их полностью. Мошенничество при этом совершается исключительно в виртуальной среде. Так, например, если злоумышленник способен выделить больше вычислительных мощностей, чем все честные участники, он может обманывать продавцов, аннулируя свои транзакции и возвращая средства, безвозмездно получая при этом товар, и его действия при этом будут квалифицированы как мошенничество в сфере компьютерной информации, то есть преступление, предусмотренное статьей 159^6 УК РФ. Также он может использовать данные мощности для генерирования новых «альтернативных» блоков цепи, однако в данном случае более выгодным для него является вариант «игры по правилам», который обеспечивает получение более половины всех новых криптомонет, чем вариант «саботажа системы» и поддержания своего капитала на постоянном уровне. Таким образом, кто нашел первым ключ, тот создал блок и заработал криптомонеты. Другие не получили ничего. После чего все вместе они снова принимаются за поиск ключа для нового блока.

---

[73] См.: Кочергин Д.А. Криптоактивы: экономическая природа, классификация и регулирование оборота // Вестник международных организаций: образование, наука, новая экономика. 2022. Т. 17. № 3. С. 88–90.

Созданные и присоединенные к цепочке блоки являются электронными следами, которые может увидеть любой желающий. Видя весь блокчейн и ключи, любой пользователь может проверить корректность любых данных, в том числе: верна ли последовательность блоков, не пропущен ли блок, не вставлен ли в середину цепи новый блок соответствие ключей блока хранимым в нем данным, то есть убедиться в отсутствии ложных сведений.

Конечно, подобная процедура расчета криптоключей усложняет создание блока, но еще больше усложняет его формирование поддельных блоков, делая создание практически невозможным. Следовательно, говорить о такой разновидности мошенничества в сфере компьютерной информации, как хищение криптомонет в виде создания путем обмана других пользователей блокчейна ложных блоков в цепи, нельзя. Хотя и полностью исключать такую возможность тоже нельзя. До тех пор, пока новая запись не внесена ни в один блок, она не может считаться достоверной и её использование участниками сети может осуществляться только, так сказать, на свой страх и риск, так как имеется вероятность её некорректности или подделки, вследствие чего запись может быть отменена, что сопряжено с финансовыми потерями лица, её использовавшего. Поэтому обычные пользователи сети просто пересылают новые записи, чтобы они рано или поздно дошли до «майнера», который включит их в блок. И лишь когда запись сохранена в блоке, можно быть уверенным, что она проверена и корректна. Отменить данную запись уже нельзя.

Исходя из представленной технологии блокчейн, с учетом требований национального законодательства, необходимо квалифицировать действия лиц, совершающих такие юридически значимые действия с использованием указанной технологии. Таким образом, можно полностью согласиться с мнением П.Н. Кобеца о том, что «в роли необходимых признаков некоторых

конкретных составов могут выступать также способ, орудия, средства, место, время или обстановка совершения преступления»[74].

Именно способ совершения преступлений с использованием криптовалюты как составная часть объективной стороны преступления позволяет при осуществлении процесса их квалификации производить разграничение со смежными составами преступлений, а в определенных случаях говорить о дополнительной квалификации по статьям главы 28 УК РФ. В свою очередь, способ совершения таких преступлений напрямую связан с принципами функционирования криптовалюты и соответствующих блокчейн-сетей. Невозможно избрать способ совершения преступления с использованием криптовалюты, не основанный на технологических принципах ее функционирования. Так же как нельзя произвести выстрел из оружия, предварительно не зарядив его соответствующим боеприпасом, невозможно совершить криптовалютную транзакцию, вопреки установленным системой принципам ее функционирования. И если данные принципы будут меняться, то, соответственно, будут изменяться и способы совершения преступлений с использованием криптовалюты и квалификация таких преступлений будет иной. Соблюдение принципов функционирования системы обеспечивается самой системой, и изменение таких принципов может быть осуществлено лишь извне путем изменения программного обеспечения системы функционирования технологии блокчейн и соответствующей криптовалюты. Но если такое произойдет, то речь будет идти уже не о сетях блокчейна и соответствующих им криптовалютах, а о некоем новом явлении в виртуальном пространстве и, соответственно, об иных отличных способах совершения преступлений в виртуальном пространстве (киберпространстве) и, соответственно, об иной квалификации таких преступлений.

---

[74] См.: Кобец П.Н. Общая характеристика объективной стороны преступления по действующему уголовному законодательству Российской Федерации // Символ науки: международный научный журнал. 2017. Т. 2. № 2. С. 187–189.

Таким образом, напрямую связанный с принципами функционирования блокчейн-сетей и соответствующих им криптовалют способ совершения данных преступлений как неотъемлемая часть объективной стороны преступления непосредственным образом влияет на их квалификацию. Без описания способа, как составной части объективной стороны преступления с использованием криптовалюты, невозможно выразить форму объективной стороны и, соответственно, правильно квалифицировать совершенное деяние либо провести разграничение со смежными составами преступлений. При этом, как уже было сказано выше, исходя из требований действующего законодательства Российской Федерации необходимо рассматривать криптовалюту как объект гражданского права в соответствии с требованиями ст. 128 ГК РФ, а также с учетом новеллы гражданского законодательства – статьи 141^1 ГК РФ. Именно исходя из этих позиций и требований Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» необходимо говорить о квалификации действий лиц, совершающих юридически значимые действия, используя блокчейн-технологии.

При выявлении и фиксации следов непосредственно в виртуальной сети необходимо учитывать, что сам процесс отбора криптовалютных транзакций не зафиксирован в виде каких-то однозначно определенных условий. «Майнеры» сами на основе своих алгоритмов выделяют из входного потока для обработки «нужные» транзакции. Основные критерии отбора при этом следующие:

— размер транзакции (чем он меньше, тем легче его обработать);

— комиссия за выполнение транзакции (чем больше комиссия, тем выгоднее ее выполнить);

— переводимая сумма (чем она больше, тем «лучше» при прочих равных условиях считается сгенерированный блок);

— приоритет (условное понятие, связанное с наличием денег в кошельке и временем их первоначального получения).

Если транзакция слаба с точки зрения критериев отбора, она может ждать подтверждения и несколько дней, вследствие чего нельзя не рассматривать такие незавершенные в течение определенного периода времени транзакции в качестве доказательств, имеющих значение для конкретного уголовного дела. Необходимо, используя «эксплорер», то есть вэбсайт для просмотра блокчейн и проверки транзакций (см. приложение № 1), периодическое обращение к данной транзакции на протяжении определенного периода времени, с конечной фиксацией ее завершения.

Как правило, если такая транзакция не подтверждается в течение недели, она вообще может быть удалена из пула памяти «майнеров». Такая транзакция не попала в блок и уже никогда в него не попадет. Тем не менее, при определенных условиях, фиксация попытки проведения подобной транзакции может являться доказательством по уголовному делу, так как в кошельке хранится информация о том, что транзакция отправлена, вследствие чего средства, которые должны были быть переведены, заблокированы. Через конкретно-неопределенное время данная транзакция может быть отменена и деньги сами возвратятся в кошелек. Но так бывает далеко не всегда (потому что это никому, кроме пользователя, не нужно). Средства на счете блокируются кошельком, поэтому требуется получить доступ к счету вне текущего кошелька. В этом случае пользователю самому потребуется произвести ряд достаточно сложных действий, чтобы вернуть деньги обратно в кошелек (нужно получить приватный ключ от нужного счета, подставить публичный номер счета, на котором лежат заблокированные средства, получить приватный ключ данного счета, переименовать кошелек, создать новый кошелек, в него импортировать полученные ранее ключи, после чего в него должны начать обратно импортироваться деньги), что сможет далеко не каждый.

Необходимо отметить, что неподтвержденные транзакции являются значимой проблемой в блокчейн. Вышеуказанные технологические аспекты непосредственно влияют на процесс квалификации преступлений, совершаемых с использованием криптовалюты. Так, в том случае, когда имеет место незавершенная транзакция, при доказанной попытке ее незаконного проведения при отсутствии волеизъявления собственника криптомонет будут иметь место умышленные действия лица, непосредственно направленные на совершение такого преступления, как мошенничество в сфере компьютерной информации. При этом преступление не будет доведено до конца по не зависящим от этого лица обстоятельствам, так как транзакция не была подтверждена системой (блокчейн-сетью), вследствие чего такие действия необходимо квалифицировать по части 3 статьи 30 и соответствующей части статьи 159^{6} Уголовного Кодекса Российской Федерации, так как, согласно диспозиции указанной нормы, в данном случае имеет место вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации, что позволяло бы виновному лицу незаконно завладеть чужим имуществом в виде криптомонет.

В том случае, если такое мошенничество в сфере компьютерной информации будет совершено с использованием вредоносной компьютерной программы, содеянное требует дополнительной квалификации по ст. ст. 272, 273 или ст. 274^{1} УК РФ в зависимости от способа использования и вида вредоносной программы.

Следующей проблемой реализации блокчейн, как уже было сказано выше, является анонимность его пользователей. Необходимо отметить, что решение данной проблемы, кроме прочего, напрямую зависит от технической оснащенности и наличия специальных знаний у лиц, совершающих преступления в указанной области. Анонимность при использовании криптовалют делает их привлекательными для использования в преступной деятельности. Согласно отчету Центрального банка Российской Федерации, «на текущий момент не существует подходов, позволяющих

деанонимизировать всех участников операций с криптовалютами, что создает вызов для действующей глобальной системы ПОД/ФТ (противодействие отмыванию доходов и финансированию терроризма) и обусловливает необходимость её совершенствования»[75]. Сохранение анонимности при обороте криптовалюты предоставляет возможность как мошенникам, так и лицам, осуществляющим реализацию товаров, запрещенных или ограниченных в гражданском обороте, значительно осложнить работу правоохранительных органов.

Согласно отчету Центрального банка Российской Федерации, «чаще всего в России (по части незаконной деятельности) криптовалюты используют для преступлений, связанных с незаконным оборотом наркотиков и выплатой вознаграждений за их реализацию. Для этого используют теневые обменные сервисы, работающие в анонимных сетях «даркнет» (darknet)»[76]. С целью сокрытия реального получателя денежных средств, поступивших от совершения преступлений с использованием криптовалюты, отмывания и обналичивания денежных средств, полученных преступным путем, «злоумышленники часто используют счета и банковские карты, открытые на подставных третьих лиц»[77]. С целью обеспечения дополнительного сокрытия информации используется метод перевода криптовалюты между множеством криптокошельков с изменением количества переводимых криптомонет, в результате чего конечному получателю необходимая ему сумма криптомонет приходит по частям с различных криптокошельков. С этой целью также используются криптомиксеры, дробящие поступающие криптомонеты на более мелкие и не позволяющие использовать их для идентификации криптокошельков, с которых они были отправлены.

Непосредственно в блокчейн-сетях для обеспечения анонимности пользователей блокчейн применяется асимметричная система шифрования с

---

[75] См.: Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 15–27.
[76] Там же.
[77] Там же.

открытыми и закрытыми ключами. Анонимность пользователей достигается следующими факторами:

1. Адреса биткойн кошельков не связываются с личностью пользователей и не хранят персональные данные.

2. Каждый пользователь в любой момент может создать себе новый случайно сгенерированный биткойн-адрес, с которым связывается секретный ключ. При этом нет необходимости предоставлять системе информацию о своей личности.

3. Транзакции включаются майнерами в блок исходя из случайных, ситуативных или прагматических обстоятельств. То есть, сами транзакции также не привязываются к личности пользователей.

4. Сеть P2P[78] состоит из множества узлов (компьютеров, смартфонов, иного компьютерного оборудования), которые объединены в единую систему и взаимодействуют посредством P2P-протокола. Сети P2P построены по принципу передачи данных случайно выбранным узлам. Это может быть передача данных между «трекерами» (устройствами, которые предназначены для записи координат маршрута с заданной периодичностью), между «пирами» или между «трекером» и «пиром». «Пир» хранит на своем компьютере файлы или размещает сервисы и предоставляет к ним доступ другим участникам. Взамен такой «пир» получает аналогичные файлы или услуги сервисов с компьютеров других участников обмена. Узел «не знает» о том, создана ли полученная им информация или она просто транслируется дальше. Вследствие этого любой желающий может увидеть, какая сумма имеется у определенного лица, скрытого за шифрованным обозначением. При этом, нельзя узнать, кто непосредственно скрывается за таким обозначением, пока владелец криптокошелька не передаст специальный пароль (виртуальный ключ), с помощью которого он подтвердит, что данная сумма

[78] P2P (англ. peer-to-peer — равный к равному) – одноранговая сеть или сетевой протокол, который обеспечивает возможность создания и функционирования сети равноправных узлов и их взаимодействие друг с другом.

принадлежит именно ему. Однако, как отмечает, например, Аарон Ван Вирдум, полная анонимность пользователей криптокошельков биткойна в сети блокчейн может быть поставлена под сомнение ввиду нижеследующего:

— хотя транзакции случайным образом передаются через сеть P2P, эта система не является полностью неуязвимой. Если злоумышленник, к примеру, имеет возможность подключить несколько узлов к сети биткойна, собранной ими информации может оказаться достаточно, чтобы определить источник конкретной транзакции;

— биткойн-адрес можно связать с конкретными людьми, если их личная информация была каким-либо образом связана с таким биткойн-адресом. Имеются в виду адреса, использованные для депозитов или снятия денег с регулируемой биржи или кошелька, находящиеся в открытом доступе адреса для пожертвований, или просто адреса, использованные для отправки биткойнов с использованием личной информации (например, платеж в онлайн-магазине);

— все транзакции в сети биткойна, равно как и в сети любой криптовалюты, полностью прозрачны для любого интересующегося. Это позволяет аналитику связать несколько биткойн-адресов и соотнести их с конкретным пользователем. Таким образом, если всего один из этих связанных адресов «привязан» к определенной личности одним из вышеописанных способов, все адреса будут деанонимизированы[79].

Такая деанонимизированность может быть осуществлена путем построения логически связанных аналитических цепочек транзакций. В различных публикациях, в частности в упомянутой статье Аарона Ван Вирдума, можно встретить термин «кластеризация», то есть логическое сведение определенных транзакций в определенные группы (кластеры) для их

[79] См.: Van Wirdum, A. IS BITCOIN ANONYMOUS? A COMPLETE BEGINNER’S GUIDE // Bitcoin Magazine. Nov. 18, 2015. Цит. по: Анонимность в сети Биткоин. Мифы и реальность. [Электронный ресурс]. Режим доступа: https://cryptor.net/bitkoin-dlya-chaynikov/anonimnost-v-seti-bitkoin-mify-i-realnost (дата обращения - 15.05.2022).

последующего анализа с использованием результатов проведенных оперативно-разыскных мероприятий и результатов автоматизированными информационными системами (далее — АИС) или автоматизированными информационно-поисковыми системами (далее — АИПС). Анализируя самостоятельно либо используя АИС, необходимо обнаружить нескольких выходов, которые объединены в одну транзакцию, так называемый «батчинг», используемый, как правило, для экономии комиссии за перевод. Данное обстоятельство может свидетельствовать о том, что все они (выходы), даже в случае происхождения от разных адресов, могут контролироваться одним и тем же пользователем.

Аналогичным образом, путем построения аналитических блок-схем, могут быть установлены устойчивые связи между отдельными участниками блокчейна. Построение указанных блок-схем дает возможность путем анализа установить, по крайней мере, общие связи между пользователями определенного блокчейна (см. Приложение № 2). В дальнейшем, установив IP-адреса электронных устройств, с которых осуществлялся выход в сеть, через предоставляющего услуги провайдера возможно установление владельца данного электронного устройства.

К условиям неочевидности совершения таких преступлений, безусловно, необходимо отнести возможность использования криптовалюты с помощью «анонимайзеров»[80] в сети Даркнет. Как уже отмечалось, Даркнет – частная сеть, интернет-соединения которой устанавливаются только между доверенными лицами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. Соответственно, Даркнет, по общему мнению, является полностью анонимным сегментом сети Интернет, к которому нельзя подключиться через обычный браузер. Однако степень анонимности Даркнета все-таки вызывает определенные споры, в основном в

[80] Анонимайзер (от англ. «anonymize») – общее название программных средств, которые используются для сокрытия информации о компьютере и его IP-адресе.

части того, могут ли его разработчики тем или иным способом контролировать его пользователей.

При использовании криптовалюты с помощью анонимайзера «Тор» риск утечки персональных данных существенно возрастает, обнаружили исследователи И. Пустогаров и А. Бирюков из исследовательской лаборатории CryptoLUX Люксембургского университета, определившие, «что с помощью определенных манипуляций возможно определить персональные данные биткойн-пользователя, работающего через «Тор». Подключаясь к сети «Тор», люди ожидают полной анонимности, но ее несложно обойти»[81]. И. Пустогаров и А. Бирюков выявили возможность подобной манипуляции, сфокусировав внимание на малоизвестном аспекте протокола биткойн – встроенной защите от DoS-атак (атака отказа в обслуживании). В целях самозащиты биткойн-серверы присваивают баллы пользователям, генерирующим проблемные транзакции. В том случае, если количество баллов превышает 100, сервер блокирует пользователя на 24 часа. Авторы поясняют, что, когда пользователь сети «Тор» подсоединяется к биткойну, его IP-адрес никак не фигурирует в сети. Вместо этого адреса биткойн-сеть видит только адреса выходного узла «Тор». Таким образом, злоумышленники могут заблокировать все выходные узлы «Тор», инициировав большое количество невалидных транзакций. Благодаря принципу работы защитной системы на серверах биткойна через какое-то время после начала спам-атаки все выходные узлы «Тор» попадут в «черные списки». Когда жертва начнет использовать «Тор» для подключения к биткойну, ей ничего не остается, кроме как подсоединиться к тем биткойн-серверам, которые уже захвачены взломщиком, так как все остальные заблокированы. С этого момента вся информация о биткойн-транзакциях жертвы проходит через руки злоумышленника. В результате атаки те транзакции и блоки, которые были запущены истинным владельцем биткойн-

[81] См. об этом: Александров А.Г., Сафронов А.А. Использование сети Даркнет при подготовке и совершении преступлений // Вестник Санкт-Петербургского университета МВД России. 2021. № 1(89). С. 156–160.

адреса, тоже подвергаются рискам, поскольку взломщик может отложить их или вовсе отменить. Принимая во внимание, что атаки данного вида могут представляет серьезную опасность для продавцов на теневом интернет-рынке, чей бизнес существует только при условии полной анонимности, данные атаки могут быть использованы именно как способ определенного противодействия указанной деятельности [82].

В настоящее время, как правило, не оспаривается тот факт, что заложенные в основу концепции «Tor» принципы маршрутизации разработаны в исследовательской лаборатории Военно-морских сил США[83]. Разработкой руководил сотрудник указанной лаборатории П. Сиверсон[84]. Из-за этого существует мнение, что код браузера наверняка включает в себя «бэкдор» (от англ. back door – «черный ход»), то есть намеренно встраиваемый разработчиком дефект алгоритма, позволяющий получать тайный доступ к данным или удаленному управлению компьютером пользователя. Однако до настоящего времени чего-либо, напоминающего такой «бэкдор», в системе не найдено.

В отличие от обычного Интернета, как такового отдельного Даркнета не существует. Есть несколько не связанных между собой сетей определенной направленности и с определенными признаками, которые объединяют общим названием «Даркнет» (см. Приложение № 2).

Основными признаками сетей Даркнет являются:

1. Децентрализация сети, так как отсутствуют привычные серверы и DNS (англ. Domain Name System – система доменных имён) и данные передаются между случайными узлами.

---

[82] См.: Вепрев С.Б., Перов В.А. Вопросы информационной безопасности при использовании криптовалют // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2017. № 2. С. 66–68.

[83] Нуркаева М.К. «Темная сеть» Интернета как инструмент для совершения преступлений и обеспечения преступной деятельности // Вестник Дальневосточного юридического института МВД России. 2021. № 4(57). С. 120–130.

[84] Мамонтов С.С. История появления термина «луковая маршрутизация» // Язык науки и техники в современном мире: материалы V международной научно-практической конференции (Омск, 14 апреля 2016 года). Омск, 2016. С. 132–135.

2. Передача информации осуществляется по защищённым каналам в зашифрованном виде.

Соответственно, такие сети дают возможность пользователю скрыть свой реальный IP-адрес, скрыть географическое место нахождения компьютера (его геолокацию), с помощью которого осуществляется выход в сеть.

Войти в Даркнет можно, используя определенные браузеры, самыми известными из которых являются уже упоминавшийся выше «Tor», «I2P» и «Freenet».

Используя анонимный криптокошелек, в сетях Даркнет пользователь, полностью сохраняя свою личную анонимность, получает возможность осуществления расчетов криптовалютой по любым заключаемым им сделкам вне зависимости от их законности. Степень раскрытия при этом его личности и сбора доказательств, подтверждающих преступность его деяния, приближается к нулю. Так, например, если лицо А договорилось передать лицу Б взятку в виде определенной суммы криптомонет, то с использованием криптокошельков в одной из сетей Даркнета такая операция может быть осуществлена полностью анонимно, без раскрытия личностей отправителя и получателя криптовалюты при невозможности установления реальных IP-адресов их компьютеров и места их нахождения. В дальнейшем получатель в зависимости от своего желания может либо осуществлять расчеты, используя полученную криптовалюту, либо, используя биржи криптовалют или так называемые обменные пункты криптовалют, произвести ее обмен на фиатные деньги, подчас с высокой степенью анонимности.

Приведенную чем схему можно легко усложнить, что приведет к дополнительным трудностям в процессе выявления лиц, совершивших преступление с использованием криптовалюты. Криптовалюту можно переводить с разных криптокошельков разными суммами. При этом можно увидеть, с каких анонимных криптокошельков на другие, также анонимные

криптокошельки какие именно криптомонеты были перечислены, но их владельцы остаются анонимными.

Последующие варианты обмена криптовалюты на фиатные деньги также не представляют сложности. Так, например, чтобы произвести обмен того же биткойна на рубли с использованием электронной платежной системы (далее — ЭПС) «Киви» (Qiwi) нужно выполнить всего лишь несколько последовательных действий. Такому обмену может предшествовать ряд действий, направленных на дробление полученных в результате совершения преступления криптомонет (см. Приложение № 5 рисунок 1, рисунок 2). Количество анонимных криптокошельков взяткодателя и взяткополучателя с целью дробления передаваемой суммы может быть различным, вследствие чего передаваемое в виде взятки количество криптомонет может быть раздроблено на несколько частей, вследствие чего возможно отследить перемещение криптомонет между криптокошельками, но нельзя определить, кому они принадлежат.

Сегодня к наиболее часто выявляемым и расследуемым преступлениям[85] с использованием криптовалюты можно отнести незаконное приобретение наркотических средств или психотропных веществ, либо их частей, содержащих наркотические средства или психотропные вещества, мошенничество в сфере компьютерной информации, а также получение взятки. Необходимо отметить, что квалификация таких преступлений будет напрямую зависеть от выявленных и зафиксированных электронных следов.

Так, например, диспозиция статьи 290 (получение взятки) УК РФ предусматривает получение должностным лицом или иностранным должностным лицом или должностным лицом публичной международной организации взятки в виде денег, а также иного имущества, которым в данном случае является криптовалюта. Исходя из требований действующего законодательства России (Федеральный закон № 259-ФЗ), криптовалюта,

[85] Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. Т. 10. № 6. С. 147–154.

являющаяся предметом взятки, может рассматриваться только как «иное имущество в виде цифровой валюты», вследствие чего в соответствующих процессуальных документах данное деяние отражается как «получение должностным лицом взятки в виде имущества цифровой валюты (название криптовалюты) в количестве (число) криптомонет». Учитывая, что криптовалюта имеет определенное стоимостное выражение, ее можно рассматривать как предмет взятки[86]. Однако, как следует из вышеуказанной диспозиции ст. 290 УК РФ, специальным субъектом данного преступления является также иностранное должностное лицо либо должностное лицо публичной международной организации. При этом в настоязее время в некоторых странах мира криптовалюта выполняет функцию денег, то есть является платежным средством и именно в этом качестве выступает предметом взятки.

Соответственно, получение или дача взятки, а равно незаконного вознаграждения при коммерческом подкупе, будут являться оконченными с момента принятия должностным лицом либо лицом, выполняющим управленческие функции в коммерческой либо иной организации, хотя бы части передаваемых ему ценностей (например, с момента передачи их лично должностному лицу, зачисления с согласия должностного лица на указанный им электронный или криптовалютный кошелек). При этом не имеет значения, получили ли указанные лица реальную возможность пользоваться или распоряжаться переданными им ценностями по своему усмотрению. Аналогичные разъяснения содержатся и в Постановлении Пленума Верховного Суда Российской Федерации от 09 июля 2013 года № 24 (ред. от 24 декабря 2019 года) «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях». Если же иностранное должностное лицо либо должностное лицо публичной международной организации

---

[86] См.: Долгиева М.М. Квалификация деяний, совершаемых в сфере оборота криптовалюты // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2019. № 1(88). С. 18.

получило в качестве предмета взятки криптовалюту именно как платежное средство, то в процессуальных документах может быть указано «получение должностным лицом взятки в виде цифровой валюты в сумме (количество и наименование криптомонет)».

Сложность при решении вопросов квалификации многократно увеличивается, если предметом взятки является криптовалюта, так как не только возникает вопрос о правовом режиме криптовалюты в различные временные периоды ее функционирования на территории Российской Федерации, но и вопрос о экономической ценности различного вида криптовалют в различные временные периоды. Разрешение указанных вопросов напрямую связано с квалификаций действий лица, получившего (давшего) взятку криптовалютой.

Также, исходя из изложенного, можно сделать вывод, что любой способ совершения преступлений с использованием криптовалюты предполагает использование виртуального пространства, что значительно снижает риск привлечения к уголовной ответственности за содеянное при возможности извлечения лицом, такие преступления совершающим, дохода в крупном и особо крупном размере.

К сказанному следует добавить, что, когда криптовалюта выступает предметом разбоя, грабежа, вымогательства, взяточничества и т. п., нет необходимости вмешательства в деятельность информационно-телекоммуникационных сетей. В данном случае криптовалюта изымается в виде информации — пароля доступа к криптокошельку или же в виде флеш-карты, на которой записан код доступа к такому кошельку.

Так, например, к умышленным преступлениям, совершаемым в блокчейн-сети, можно отнести преступления, различные по способу совершения, но совершаемые с целью хищения криптомонет путем обмана, то есть совершение мошеннических действий. Наличие прямого умысла, направленного на хищение криптомонет путем обмана, должно подтверждаться характером совершаемых в виртуальной среде действий.

Ниже приведены способы совершения мошенничества в виртуальной среде с использованием криптовалюты. При этом не всегда совершение определенных действий имеет своей целью совершение преступления, так как при этом большую роль будет играть наличие у лица специальных знаний, позволяющих предположить наиболее вероятную реакцию блокчейн-сети на характер совершаемых им в данной сети действий.

К таким способам мошенничества можно отнести:

1. Способ, получивший название «Атака» или «Атака одного подтверждения», при использовании которого «атакующий» осуществляет транзакцию А, оплачивая покупку, например, в магазине. Одновременно он выполняет транзакцию Б, переводящую те же деньги, но уже на другой счет злоумышленника, коим сам же атакующий может и являться. При этом в случае, если магазин не дожидается прихода денег и производит доставку (отгрузку, передачу) купленных товаров, то половины денежной суммы за них он может так и не получить, так как с вероятностью 50 % транзакция Б может попасть в цепочку блоков без каких-либо усилий со стороны мошенника. При этом мошенник может увеличить эту вероятность, выбирая узлы сети для передачи той или иной транзакции[87].

2. «Атака Финни» или «двойная трата». Мошенник, имеющий доступ к некоторой части мощностей майнинга сети, пытается найти обычный блок, который может содержать его транзакцию Б. Суть в том, что ни транзакция А, ни транзакция Б еще не отправлены. В зависимости от мощностей сети такой блок рано или поздно обнаруживается, после чего он отправляет транзакцию А. Мошенник приобретает товары в магазине, который ждет появления блока с транзакцией А в сети. Как только блок обнаруживается, магазин отпускает оплаченные товары, после чего появляется блок с транзакцией Б, найденный мошенником. Это приводит к так называемой развилке, то есть ситуации, при

[87] См.: Риски цифровизации: виды, характеристика, уголовно-правовая оценка: монография / отв. ред. Ю.В. Грачева. М., 2022. С. 57.

которой «майнеры» должны выбрать один из двух блоков для продолжения цепочки.

При этом, если выбор осуществляется неслучайным образом, мошенник может увеличить свои шансы на 50 %. Лицо, совершающее такие действия для достижения преступной цели завладения чужими криптомонетами, должно заранее выстроить всю схему преступных действий с учетом особенностей реагирования на такие действия блокчейн-цепи[88]. Только при таких условиях можно говорить о наличии у него прямого умысла на совершение мошеннических действий. Другими словами, каждый индивид, совершая определенные деяния, стремится к определенной цели и пытается ее достичь определенным способом. При непонимании особа достижения цели отсутствует возможность ее достижения, а значит прямой умысел, направленный на совершение мошеннических действий[89].

Продолжая рассматривать способ совершения мошенничества под названием «Атака Финни», необходимо отметить, что в случае наличия у мошенника доступа к большим мощностям майнинга (достигающим мощностей 51 % от общего количества, используемых в блокчейн-сети мощностей), он может подготовить не один блок, а сразу несколько, для того чтобы обогнать «хорошую» цепочку. Вероятность такой ситуации не слишком велика, но такая атака будет на 100 % успешной и в данном случае, учитывая правильную последовательность действий[90], направленных на преступный результат, можно говорить о наличии у лица прямого умысла, направленного на совершение мошенничества определенным способом. Если у мошенника имеется 10 % «ХЭШрейта» (единица измерения вычислительной мощности) на каждые 100 блоков, то есть чаще, чем раз в сутки, он может находить два

---

[88] См.: Риски цифровизации. С. 56–58.
[89] Там же.
[90] Семибратов И.В., Фомичев В.М. Оценка вероятности успешной атаки нарушителя в блокчейн-сети // Прикладная дискретная математика. Приложение. 2019. № 12. С. 169–172.

«быстрых» блока подряд и начинать свою атаку[91]. В данном случае такие действия будут квалифицироваться по ст. 159[6] УК РФ (мошенничество в сфере компьютерной информации), так как умысел лица был направлен на завладение чужими денежными средствами путем модификации компьютерной информации, хранящейся в блокчейн-сети[92], пользователем которой является каждый из ее участников[93], вследствие чего осуществляется хищение чужого имущества путем модификации компьютерной информации и вмешательства в функционирование средств хранения компьютерной информации.

3. «Эгоистичный майнинг»[94]. При избрании данного сценария целью мошенника будет являться не только совершение одно эпизодного мошенничества, а контроль над сетью при наличии менее чем 50 % мощностей. Схема действий при этом такова. «Пул» (специализированная веб-служба), которым владеет мошенник, заявляет, что «майнинг» здесь выгоднее, чем в других «пулах». Майнеры входят в данный пул и начинают «майнинг». В результате «пул»[95] мошенника может получить 51 % мощностей и использовать схему мошенничества под названием «Атака 51».

Следует отметить, что каждый «майнер» отдает себе отчет в том, что, присоединяясь к крупному пулу, он может способствовать совершению мошенничества, тем самым подвергая опасности систему, предоставляющую ему возможность извлечения прибыли.

---

[91] См.: Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Режим доступа: https://nakamotoinstitute.org/bitcoin/ (дата обращения –18.04.2023).

[92] См.: Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: учебно-методическое пособие. М., 2017. С. 83.

[93] Черепнев М. А. Децентрализованная схема защищенного создания и хранения баз данных // International Journal of Open Information Technologies. 2020. Т. 8, № 7. С. 109–115.

[94] См.: Полпудников С.В., Степанова А.С. Атака 51% в системе биткоин // European Scientific Conference: сборник статей VIII Международной научно-практической конференции: в 3 ч. (Пенза, 7 января 2018 года). Часть 1. Пенза, 2018. С. 139–141.

[95] Здесь и далее термин «пул» используется для наименования объединения нескольких ЭВМ или другого компьютерного оборудования в единую сеть, находящуюся под контролем одного администратора.

4. «Атака Сибиллы» – данный способ получил наибольшие распространение в P2P-сетях. Мошенник пытается «окружить» узел жертвы, то есть завладеть всеми соседними узлами сети. Получив доступ к узлам, он начинает контролировать все входящие и исходящие данные. Мошенник может передавать жертве ложную информацию или препятствовать передаче потерпевшим какой-либо информации по сети. Кроме того, атакующий мошенник имеет возможность идентифицировать транзакции, отправленные узлом жертвы[96].

Следует отметить, что такой способ совершения мошеннических действий является достаточно сложным по причине того, что коды криптовалют написаны таким образом, что узел выбирает соединение с другими узлами практически случайно. Даже в случае, если взломщик контролирует 80 % всех узлов в сети и нам требуется установить 8 случайных исходящих соединений, вероятность оказаться полностью окруженным составляет всего 0,88 = 16,77 %[97].

Сами по себе указанные действия, совершенные человеком, то есть вменяемым физическим лицом, достигшим возраста привлечения к уголовной ответственности, могут свидетельствовать о наличии у него умысла на завладение чужим имуществом (криптомонетами) путем обмана, то есть мошенничества. Хотелось бы еще раз отметить, что во всех указанных выше способах совершения мошенничества речь идет только об обмане человека, но никак не компьютерных программ, используемых как средство совершения преступления.

В постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве,

---

[96] См.: Тороев А.С., Колованов А.В. Классификация и анализ атак на блокчейн-системы // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. 2019. № 1(10). С. 189–196.

[97] См.: Ярыгин П.К. Анализ эффективности применения комбинированной атаки на сети Bitcoin // Информатизация и связь. 2023. № 1. С. 98–104.

присвоении и растрате» указывается, что обман как способ совершения хищения или приобретении права на чужое имущество может состоять как в сознательном сообщении заведомо ложных сведений, которые не соответствуют действительности, так и в умолчании об истинных фактах. Также обман может состоять в определенных умышленных действиях, направленных на введение владельца имущества или иного лица в заблуждение. То есть обманутым или введенным в заблуждение может быть только определенное физическое лицо.

Соответственно, в том случае, если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа.

В случаях, когда лицо похитило криптовалюту, воспользовавшись при этом необходимой для получения доступа к криптокошельку конфиденциальной информацией держателя такого кошелька (паролем), переданной виновному лицу владельцем криптокошелька под воздействием обмана или злоупотребления доверием, действия виновного должны быть квалифицированы по соответствующей части ст. 158 УК РФ как кража. Также необходимо отметить, что в том случае, когда хищение криптовалюты осуществляется с использованием вредоносной компьютерной программы, такое деяние по смыслу ст. 159^6 УК РФ будет являться вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, то есть целенаправленным воздействием программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры) или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом, в данном случае криптомонетами, или приобрести право на него.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 273 УК РФ. Представляется обоснованным говорить о том, что обманутым или введенным в заблуждение может быть только человек, но никак не компьютерная программа, либо взятое отдельно или в комплексе компьютерное оборудование.

На основании вышеуказанного можно сделать вывод о том, что такие действия, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества, независимо от способа получения доступа к таким данным, подлежат квалификации как кража, если виновным не было оказано незаконное воздействие на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии криптокошелька, происшедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием.

§ 1.3. Анализ преступлений, совершаемых с использованием криптовалюты

Эффективность борьбы с любым видом преступлений зависит от уровня и качества информационного обеспечения деятельности правоохранительных и следственных органов. Учитывая, что часть преступлений, совершаемых с использованием криптовалюты, относится к категории тяжких и особо тяжких, а значит к подследственности Следственного комитета Российской Федерации, анализируя указанные преступления, необходимо применение практико-ориентированного подхода, состоящего в том, что в результате такого анализа должны быть выявлены:

1. Степень распространенности и общественной опасности преступлений, совершаемых с использованием криптовалюты.

2. Тенденций состояния преступности, ее социально-правовых характеристик, раскрывающих механизм ее порождения и функционирования с целю выработки наиболее эффективных мер, направленных на профилактику, выявление и эффективное расследование преступлений, совершаемых с использованием криптовалюты.

К указанным характеристикам можно отнести характеристику всей совокупности преступлений с использованием криптовалюты, совершенных за определенных временной период в различных странах мира и в Российской Федерации, структуру преступности, обстоятельства совершения преступлений с использованием криптовалюты и их последствия.

Таким образом, анализ преступлений, совершаемых с использованием криптовалюты, призван не только выявить основные детерминанты, повышающие латентность указанных преступлений, но и способствовать разработке мер противодействия преступности в указанной сфере.

Согласно исследованию, проведенному аналитической компанией Chainalysis[98] в 2020 году, в котором отражены тенденции развития в мире так называемых «киберпреступлений»[99], при совершении которых используются различные виды криптовалют, составлен рейтинг преступлений, наиболее часто совершаемых в мире. Компания Chainalysis занимается анализом блокчейнов, а также разрабатывает программное обеспечение, проводя исследования для государственных учреждений, бирж, финансовых учреждений, страховых и компаний по кибербезопасности в более чем 50 странах мира. Исследовались преступления, совершенные со следующими видами криптовалют и токенов: «BAT» (сокр. от англ. Basic Attention Token, токен, который был создан на основе технологии «Ethereum»), «BCH» (сокр. от англ. Bitcoin Cash – биткойн кэш, разновидность криптовалюты, созданной с использованием кода программы «биткойн»), «BTC» (криптовалюта биткойн), «ETH» (криптовалюта Эфириум), «LTC» (криптовалюта Лайткойн), «MKR» (Макер – разновидность стейблкоина), «OMG» (аббревиатура разновидности криптовалюты), «PAX» (разновидность стейблкоина, курс которого зависит от курса доллара США), «TUSD» (разновидность стейблкоина, курс которого зависит от курса доллара США), «USDC» (разновидность стейблкоина, курс которого зависит от курса доллара США), «USDT» (разновидность стейблкоина, курс которого зависит от курса доллара США). В данный список попали такие виды преступлений, как отмывание (легализация) денежных средств или иного имущества, приобретенных преступным путем, финансирование терроризма, вымогательство.

---

[98] Chainalysis — это аналитическая компания, предоставляющая правоохранительным органам и иным заинтересованным в этом государственным учреждениям инструменты отслеживания операций в блокчейне, а также оказывающая помощь криптобиржам в выявлении лиц, совершающих преступления в данной сфере и используемых ими криптокошельков.

[99] См.: The Chainalysis 2021 Crypto Crime Report. Цит по: Chainalysis: отчет по криптопреступлениям, 2021. Режим доступа: https://vc.ru/finance/251237-chainalysis-otchet-po-kripto-prestupleniyam-2021 (дата обращения - 22.04.2022).

Так называемое отмывание (легализация) денежных средств или иного имущества, приобретенных преступным путем, является важнейшим элементом во многих преступных схемах, реализуемых с использованием криптовалюты, на что указывают данные, полученные при анализе работы сетей блокчейн. Преступникам достаточно проблематично использовать крупные криптобиржи с их уже устоявшимися «процедурами комплаенса»[100]. Вместо этого они пользуются так называемыми криптообменными пунктами, для которых отмывание средств либо основной вид деятельности, либо способ дополнительного заработка. К таковым можно отнести: игровые платформы, миксеры, а также другие сервисы, использующие криптовалюту и находящиеся в регионах со слабым регулированием отношений, связанных с оборотом криптовалюты. Криптовалюты, задействованные в незаконных схемах, оседают в основном на 5 сайтах, на которые пришлось 55 % всех незаконных средств за 2020 год[101].

По мнению аналитиков Chainalysis, «отмывание денег – ключ к криптовалютной преступности»[102]. И с таким утверждением можно согласиться, так как конечной целью большинства преступлений, предметом которых является криптовалюта, – то ее легализация либо легальная конвертация криптовалюты в фиатные деньги, которые можно на законном основании хранить в кредитных организациях и использовать по своему усмотрению. Соответственно, такие преступления совершаются с прямым умыслом и имеют своей конечной целью легализацию криптовалюты, полученной в результате совершения преступлений либо обращения ее в фиатные деньги.

Данный вывод подтверждается материалами расследованных в Российской Федерации уголовных дел.

---

[100] Комплаенс (англ. compliance) – комплекс мер, направленный на строгое соблюдение требований действующего законодательства и отраслевых стандартов.
[101] См.: The Chainalysis 2022 Crypto Crime Report. Цит по: Chainalysis – Криптопреступность 2022. Режим доступа: https://is-systems.org/blog_article/11647251410 (дата обращения – 11.05.2023).
[102] Там же.

Так, например, приговором Октябрьского районного суда г. Кирова лицо было признано виновным в совершении преступлений, предусмотренных ч. 3 ст. 30, п. п. «а», «г» ч. 4 ст. 228^1, ч. 3 ст. 30, ч. 5 ст. 228^1, ч. 1 ст. 174^1 УК РФ. Преступления совершены при следующих обстоятельствах. Используя свой сотовый телефон и информационно-телекоммуникационную сеть Интернет, виновное лицо конвертировало полученную им в результате сбыта наркотических средств криптовалюту биткоин в российские рубли, с целью придания правомерного вида владения, пользования и распоряжения указанными денежными средствами организовывал их перевод на банковскую карту, оформленную на имя иного лица. Используя указанную банковскую карту для различных операций, виновное лицо смогло по своему усмотрению распоряжаться денежными средствами, которые в результате совершения вышеперечисленных финансовых операций теряли связь с ранее совершенными особо тяжкими преступлениями в сфере незаконного оборота наркотических средств, и лицом, их совершившим. Таким образом, своими действиями виновное лицо легализовало денежные средства, приобретенные в результате совершенного преступления, путем осуществления финансовых операций в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами[103].

Следующий пример показывает совершение аналогичных преступлений организованной группой.

Так, приговором Советского районного суда г. Липецка N признан виновным в совершении преступлений, предусмотренных ч.3 ст.30, п.п. «а», «г» ч.4 ст.228^1, ч.3 ст.30, п.п. «а», «г» ч.4 ст.228^1, п. «а» ч.4 ст.174^1, ч.3 ст.327 УК РФ, совершенных им в составе организованной группы. Структура организованной группы состояла из организаторов, руководителей, а также иных участников, разделявшихся в соответствии с возложенными на них

[103] См.: Приговор Октябрьского районного суда г. Кирова по уголовному делу № 1-44/2020 от 13 февраля 2020 г. [Электронный ресурс] / Октябрьский районный суд г. Кирова. Режим доступа: https://oktyabrsky--kir.sudrf.ru (дата обращения – 26.02.2023).

функциональными обязанностями на «кураторов-операторов» и «закладчиков». Неустановленными следствием лицами – организаторами и руководителями организованной группы – был положен в основу совершения преступлений бесконтактный способ незаконного сбыта наркотических средств путем производства закладок (тайников) с активным использованием при этом сети Интернет для обмена информацией о совершаемых преступлениях между соучастниками, общения с покупателями наркотических средств и получения электронных платежей за реализованные наркотические средства в качестве оплаты противоправных действий соучастников.

Неустановленные организаторы и руководители организованной группы взяли на себя следующие функции: разработка общего плана деятельности организованной группы, ее структуры, планов действий (специализации) каждой из структур, распределение между ними обязанностей по подготовке и совершению конкретных особо тяжких преступлений, по совершению действий, в том числе используя сеть Интернет, направленных на достижение общей цели, поставленной перед участниками организованной группы, в частности: осуществление подбора и вербовки участников организованной группы, определяя им преступные роли и обязанности, обеспечивая их материально-техническими и финансовыми средствами, упаковочными материалами, весами, оплатой проживания в местах дислокации, разъясняя разработанные ими методы сокрытия совершаемых преступлений, меры безопасности и конспирации; осуществляли распределение денежных средств, полученных от преступной деятельности между участниками организованной группы, при этом осуществляли легализацию указанных денежных средств путем приобретения криптовалют и дальнейшего использования интернет-ресурсов для имитации происхождения преступного дохода из легальных источников; осуществляли общее руководство организованной группой и по поддержанию связей между ее участниками, координируя их преступные действия и создавая для них

условия совершения преступлений, через соответствующие программы персональной связи в телекоммуникационной сети Интернет, в целях незаконного сбыта наркотических средств лицам, пожелавшим их приобрести. При этом неустановленными организаторами и руководителями организованной группы для ее функционирования привлечены в качестве участников организованной группы неустановленные в ходе следствия лица, так называемые «кураторы-операторы», которые за денежное вознаграждение дистанционным способом, посредством общения через электронную программу персональной связи «Телеграмм», в сети Интернет осуществляли функции по более детальному инструктажу лиц, так называемых «закладчиков», непосредственно размещающих наркотические средства в закладки (тайники), по выполнению ими своих обязанностей, координации деятельности «закладчиков», указывая вид и количество наркотических средств, которые необходимо расфасовать и разместить в закладки тайники) в определенных районах города, после чего получают от «закладчиков» сообщения с адресами и описаниями местонахождения закладок (тайников) с наркотическими средствами. Также проводился инструктаж по осуществлению функции по связи с приобретателями наркотических средств, которым после подтверждения произведенной в безналичной форме оплаты наркотических средств сообщали местонахождение закладок (тайников) с оплаченными наркотическими средствами. Виновное лицо совместно с участниками организованной группы осуществляло легализацию денежных средств, полученных от преступной деятельности, путем приобретения цифровых криптовалют и дальнейшего использования интернет-ресурсов для имитации происхождения преступного дохода из легальных источников[104]. Полученная в результате совершения преступлений, аналогичных описанному выше, криптовалюта обменивается на фиатные деньги на криптовалютных

[104] См.: Приговор Советского районного суда г. Липецка по уголовному делу № 1-259/2020 от 29 июля 2020 г. [Электронный ресурс] / Советский районный суд г. Липецка. Режим доступа: http://sovetsud.lpk.sudrf.ru (дата обращения – 26.02.2023).

биржах. В 2020 году выросла доля всей криминальной криптовалюты, получаемой такими биржами (см. Приложение № 5, рис. 3).

Данный факт говорит о возросшей в мире криминальной активности в сфере оборота криптовалют и увеличении количества преступлений с целью противоправного завладению ею.

Значительный рост транзакций происходит с так называемых «криминальных кошельков», то есть тех криптокошельков, которые уже ранее использовались преступниками на сервисах, которые относятся к категории «рискованных». Это биржи с высоким риском, онлайн-казино, миксеры и сервисы, которые базируются в юрисдикциях с высоким уровнем риска[105].

Согласно аналитическим исследованиям Chainalysis, наибольший объем криптовалюты с так называемых криминальных кошельков на основе разбивки мест расположения пользователей для услуг, получающих эти средства, поступает в следующие страны: Соединенные Штаты Америки, Россия, Китай, Южно-Африканская Республика, Великобритания, Украина, Южная Корея, Вьетнам, Турция, Франция.

В приложении № 5 (см. рисунок 4) указаны страны-получатели криптовалюты с учетом типа криминальной деятельности, за счет которой криптовалюта была получена. Объем подсчитан на основе web-трафика сервисов – получателей нелегальных средств[106].

Анализ преступности в странах-получателях криптовалюты с учетом видов преступлений, в результате совершения которых она была получена, позволяет сделать вывод, что Россия находится на втором месте после США в данном рейтинге, что свидетельствует о росте на ее территории количества умышленных преступлений с использованием криптовалюты.

Данные вышеназванного аналитического исследования свидетельствуют о том, что к преступлениям с использованием криптовалюты, наиболее часто совершаемым в Российской Федерации, можно отнести

---

[105] См.: The Chainalysis 2022 Crypto Crime Report…
[106] Там же.

вымогательство. Применительно к Российской Федерации это преступления, предусмотренные ст. 163 УК РФ. Проведенный компанией Chainalysis анализ преступлений, совершенных в сетях блокчейн за 2020 год, показывает рост криптовалютных платежей от жертв вымогателей на 311 %»[107]. В том же отчете компании Chainalysis указано, что при росте криптовалютных платежей от жертв вымогателей общая сумма таких платежей составила 350 миллионов долларов США. Таков общий ущерб от совершения вышеуказанных преступлений[108].

Количество программ-вымогателей может говорить о том, что преступных групп, создающих и использующих данные программы с целью вымогательства, довольно много. Chainalysis указывает в своем аналитическом отчете на возможности существования модели RaaS[109], сервиса, предусматривающего возможность аренды у лиц, создавших данную модель, компьютерной программы, которая представляет собой инструмент, используемый для преступной деятельности, в данном случае — для координации атак программ-вымогателей. По самым скромным оценкам, общая сумма потерь от использования программ-вымогателей с середины 2019 по середину 2020 года составила более 1 миллиарда долларов США[110]. Доступное для продажи программное обеспечение RaaS, как правило находится в «Даркнете». Программисты, создающие такого рода программы-вымогатели, продают их для широкого использования. Некоторые из них предоставляют техническую поддержку при использовании такой программы, создают форумы пользователей и осуществляют регулярное обновление программы.

---

[107] См.: The Chainalysis 2021 Crypto Crime Report…

[108] Там же.

[109] Модель RaaS (ransomware as a service) – это программа-вымогатель, которая может быть создана с уникальным набором определенных функций (по желанию клиента).

[110] См.: Бойченко О.В. Инновации противодействия атакам программ-вымогателей // Теория и практика экономики и предпринимательства: труды XVIII Всероссийской с международным участием научно-практической конференции (Симферополь-Гурзуф, 27–29 апреля 2021 года). Симферополь, 2021. С. 13–14.

Программы-вымогатели можно настраивать. Покупателям таких программ предоставляются интерфейсы, в которых они могут настраивать свои вредоносные программы. При этом некоторые панели интерфейса позволяют пользователям просматривать информацию о том, где, например, впервые была запущена данная вредоносная программа, какое количество файлов было зашифровано с использованием именно этой программы, общая сумма заплаченного выкупа.

Необходимо отметить, что диспозиция ст. 163 УК РФ предусматривает, что вымогательство — это требование передачи чужого имущества или права на имущество либо совершения иных действий имущественного характера под угрозой применения насилия, а также уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких. В рассматриваемом случае при использовании вредоносной программы RaaS происходит блокирование компьютерной информации, вследствие чего пользователь лишается возможности пользоваться своим имуществом (компьютером) одновременно с требованием передачи чужого имущества в виде криптовалюты для его разблокирования. Можно ли рассматривать данную ситуацию как повреждение чужого имущества вопрос оценки. Видится, что в данном случае необходимо исходить из следующего. Блокирование персонального компьютера лишает его пользователя возможности использования своего имущества по его прямому назначению, что равносильно физическому уничтожению такого имущества (ПК). Указанное деяние охватывается диспозицией ст. 163 УК РФ и должно быть квалифицировано как вымогательство. Аналогичной точки зрения придерживаются и некоторые российские ученые[111].

---

[111] Безручко Е.В., Ходусов А.А. Преступления, совершаемые с использованием информационно-телекоммуникационных средств: философско-правовое конструирование эффективных классификаций // Философия права. 2020. № 3(94). С. 89–95; Митряев И.С.

Также криминальные даркнет-рынки в России помимо программ-вымогателей предлагают также услуги по реализации наркотиков и огнестрельного оружия. Применительно к законодательству Российской Федерации это преступления, предусмотренные ст. 222 (незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение оружия, основных частей огнестрельного оружия, боеприпасов), ст. 228 (незаконные приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их аналогов, а также незаконные приобретение, хранение, перевозка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества), ст. 228^{1} (незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества) УК РФ. Рынки Даркнета, осуществляющие незаконную реализацию предметов, ограниченных или запрещенных в гражданском обороте, установили рекорд по количеству собранной криптовалюты за 2020 год. Её объем составил 1,7 миллиардов долларов США[112].

Также с использованием Даркнета реализуются различные виды мошеннических схем. Даркнет в данном случае облегчает совершение различного вида мошенничества, обеспечивая анонимность. Применительно к законодательству Российской Федерации это преступления, предусмотренные ст. 159 (мошенничество), ст.159^{3} (мошенничество с использованием электронных средств платежа), ст. 159^{6} (мошенничество в сфере компьютерной информации) УК РФ. Согласно отчету Chainalysis, в 2020 году

Тенденции применения кибератак программ-вымогателей // Инновации. Наука. Образование. 2021. № 47. С. 985–991.

[112] См.: The Chainalysis 2021 Crypto Crime Report….

на данный вид преступлений пришлось 54 %[113] от общего количества преступлений, совершенных с использованием криптовалюты.

Следующей по количеству совершаемых преступлений следует кража криптомонет из криптовалютных кошельков пользователей. Применительно к законодательству Российской Федерации это преступления, предусмотренные ст. 158 (кража) УК РФ.

Осуществляя тайное хищение криптомонет из биржевого криптокошелька потерпевшего, злоумышленники собирают похищенные криптомонеты, как правило, на нескольких сервисах. Процент нелегальных средств, направляемых на 5 сайтов, которые использовали криптовалюту, полученную в результате совершения преступлений, позволяет сделать вывод, что в целом в 2020 году эти пять сайтов получили 55% от всех средств, отправленных с нелегальных кошельков[114] (См.: Приложение № 5, рисунок 5).

К сожалению, в аналитический отчет Chainalysis не вошли такие преступления, при совершении которых криптовалюта использовалась в качестве платежного средства при финансировании терроризма и экстремизма. Применительно к законодательству Российской Федерации это преступления, предусмотренные ст. 282^3 (финансирование экстремистской деятельности), ст. 205^1 (содействие террористической деятельности) УК РФ. По информации агентства «Интерфакс», директор Росфинмониторинга заявил, что криптовалюты используются не только в спекулятивных сделках, но и для финансирования терроризма и экстремизма[115]. Анонимность использования криптовалют, не требующих идентификации, как, например, при использовании банковских счетов, глобальная доступность криптовалюты, предполагающая возможность ее использования в любой

---

[113] См.: The Chainalysis 2021 Crypto Crime Report…
[114] Там же.
[115] См.: Красинский В.В. Финансирование терроризма с использованием криптовалют: опыт контроля и пресечения // Мировой политический процесс: информационные войны и «цветные революции»: Сборник материалов Международной научно-практической конференции (Москва, 27–29 октября 2021 года). М., 2022. С. 68.

точке мира при наличии телекоммуникационной сети Интернет и относительная простота использования делают криптовалюту притягательной для использования экстремистскими и террористическими организациями.

Полученные на основании исследований, проведенных компанией Chainalysis, данные использовались для раскрытия наиболее резонансных уголовных дел в мире, связанных с непосредственным использованием криптовалюты[116] в том числе и преступлений, совершенных на территории Российской Федерации.

Так, например, приговором Сургутского городского суда Ханты-Мансийского автономного округа — Югры признаны виновными в совершении преступлений, предусмотренных ч. 3 ст. 272, ч. 3 ст. 159 УК РФ, группа лиц, совершивших вышеуказанные преступления при следующих обстоятельствах: действуя в группе лиц по предварительному сговору из корыстной заинтересованности совершили неправомерный доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации, а также вступив в сговор с целью хищения чужого имущества, а именно криптовалюты «биткойн», посредством телекоммуникационной сети Интернет, путём незаконного получения доступа к учетным записям под предлогом обмена BTC-e кодов (биткоинов). Осознавая преступный характер своих намерений, совместно, умышленно, из корыстных побуждений спланировали действия, направленные на неправомерный доступ к компьютерной информации и совершение мошеннических действий[117].

Таким образом, совершая определенное деяние с криптовалютой, лицо должно осознавать незаконность такого деяния и желать наступление неких

---

[116] См.: Поздышев Р. С. Криптовалюта как угроза финансово-правовому механизму надзора в сфере противодействия легализации преступных доходов и финансированию терроризма // Наука среди нас. 2019. № 8(24). С. 125–128.

[117] См.: Приговор Сургутского городского суда Ханты-Мансийского автономного округа — Югры по уголовному делу № 1-762/2017 от 3 ноября 2017 г. [Электронный ресурс] / Сургутский городской суд Ханты-Мансийского автономного округа — Югры. Режим доступа: http://surggor.hmao.sudrf.ru/ (дата обращения – 26.02.2023).

общественно опасных последствий. Конечно, данное утверждение можно отнести к материальному составу преступления. При совершении преступления с использованием криптовалюты с материальным составом необходимо учитывать относительную автономность блокчейн-сетей, осуществляющих свою работу в соответствии с используемыми ими алгоритмами и не всегда реагирующими на действия человека в соответствии с его желаниями, то есть не позволяя ему достичь тех целей, которые он преследует, совершая соответствующее деяние. Другими словами, можно сказать, что в данном случае мы говорим о симбиозе мира виртуального и реального, при котором сеть в определенных условиях может по-разному реагировать на одни и те же действия определенного лица. Кроме того, не следует забывать, что психика каждого человека индивидуальна и не всегда разум отдельного индивида в силу целого ряда причин, например наличия (отсутствия) специальной подготовки, различного образа мышления, способен осознать и спрогнозировать последствия своих действий в блокчейн-сетях.

Отсутствие истинного отражения реалий виртуального мира у отдельно взятого индивида может быть выражено в виде его заблуждения или неведения, что проявляется в волевых поступках, к которым относятся и преступные действия. В силу указанных обстоятельств роль заблуждения и неведения при установлении вины представляется достаточно значимой для квалификации преступлений с использованием криптовалюты и требует детального изучения.

Содержание понятия неведения в современной науке принято раскрывать как незнание лицом каких-либо фактических условий деятельности или недостаток представлений, соответствующих действительности. Такую трактовку термина можно встретить во многих толковых словарях, определяющих неведение как незнание или неосведомленность о чем-либо.

Относительно последствий совершения преступлений с использованием криптовалюты необходимо отметить, что в соответствии со статьей 140

Гражданского кодекса Российской Федерации к законному платежному средству, обязательному к приему по нарицательной стоимости на всей территории Российской Федерации, относится рубль, соответственно величина причиненного ущерба либо стоимость предмета взятки должна быть выражена в рублях.

Аналогичным образом должен быть оценен ущерб при совершении различных видов хищений криптовалюты.

Неопределенность характеристики содержания ущерба, обусловленная отсутствием законодательно закрепленных критериев его оценки в составах преступлений, совершаемых с использованием криптовалюты, детерминировала неоднозначность подходов к его определению, что создает квалификационные сложности при уголовно-правовой оценке данного деяния.

Отсутствует и как таковая методология оценки. Оценивая причиненный потерпевшему ущерб вследствие хищения принадлежащих ему криптомонет либо оценивая стоимость криптомонет, являвшихся предметом взятки, правоприменитель исходит из индивидуально-субъективных критериев, как правило, не несущих в себе какой-либо правовой или экономической составляющей, обосновывающей подобную оценку[118].

Законодательно определено, что противоправное изъятие у собственника любого принадлежащего ему имущества, в том числе криптовалюты, причиняет ему убытки, эквивалентные стоимости данного имущества, то есть реальный ущерб, связанный с утратой потерпевшим данного имущества (ч. 2 ст. 15 ГК РФ).

Таким образом, для правильной квалификации хищений криптовалюты необходимо использование соответствующей методики расчета ущерба,

[118] См.: Лошкарев А.В., Крылова А.Е. Возмещение ущерба причиненного преступлением с использованием криптовалют // Международный журнал гуманитарных и естественных наук. 2020. № 10–3(49). С. 127–130.

причиненного потерпевшему в результате действий по незаконному изъятию у него данной криптовалюты, которая основывается на следующем.

Учитывая, что криптовалюта обладает высокой волатильностью (изменчивостью цены) при оценке ее стоимостных показателей в рублевом эквиваленте следует исходить из ее стоимости в конкретный временной период, соответствующий совершению преступного деяния. Данное положение применимо и к стоимостной оценке криптовалюты как предмета взятки.

При этом, если имело место незаконное завладение криптовалютой, находящейся в криптокошельке потерпевшего на криптовалютной бирже, то стоимость криптомонет определяется в соответствии с стоимостью их покупки данной биржей на время совершения противоправных действий.

В случае если имели место противоправные требования к потерпевшему о приобретении криптовалюты и ее последующей передаче, стоимость необходимо определять исходя из фактических затрат на ее приобретение.

В случаях, когда противоправное завладение криптовалютой осуществляется из принадлежащего потерпевшему программного или аппаратного криптокошелька, стоимость похищенного определяется путем вычисления среднестоимостного показателя соответствующих криптомонет, согласно курсовой стоимости действующих криптовалютных бирж, либо, исходя из принципа презумпции невиновности, ее минимального биржевого значения на указанный временной период. Указанная методика применима и для определения стоимости криптовалюты, полученной в качестве предмета взятки.

Следует отметить, что взяточничество можно отнести к одному из самых распространенных преступлений коррупционного характера, причем не только в России, но и в мире. Оно посягает на основы любой государственной власти, дискредитируя ее в глазах населения, создает помехи в управленческой деятельности государственных и муниципальных органов и учреждений, подрывает их авторитет, деформирует правосознание граждан,

создавая у них представление о возможности удовлетворения личных и коллективных интересов путем подкупа должностных лиц, препятствует конкуренции, затрудняет экономическое развитие, создавая черный рынок по оказанию незаконных услуг, частично переводя незаконно полученные должностными лицами денежные средства в теневой сектор экономики. Использование при даче взятки криптовалюты увеличивают общественную опасность данного деяния путем повышения его латентности[119], так как такое преступление значительно реже выявляется[120] и регистрируется. Предметом взяточничества наряду с деньгами, ценными бумагами может быть иное имущество, к которому на сегодняшний день можно было отнести разновидность цифровой валюты – криптовалюту. Соответственно, с учетом вступившего в законную силу 1 января 2021 года Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» в Российской Федерации с указанного периода времени необходимо в процессуальных документах использовать понятия, предусмотренные статьей 1 вышеуказанного закона. Данное положение должно применяться и при соответствующей оценке собранных по расследуемому уголовному делу доказательств, в том числе в виде электронных следов, и последующей квалификации образующих объективную сторону действий.

Учитывая, что получение и дача взятки, посредничество во взяточничестве в виде непосредственной передачи взятки считаются оконченными с момента принятия должностным лицом хотя бы части передаваемого ему имущества, необходимо устанавливать момент поступления криптомонет в электронный кошелек взяткополучателя.

---

[119] См. об этом подробнее: Усачева Е.А., Филимонов А.Д. Криптовалюта как предмет взятки и коммерческого подкупа: проблемы регулирования // Искусство правоведения. 2023. № 1(5). С. 84.

[120] См. об этом подробнее: Качалов В.В. Получение взятки криптовалютой: вопросы квалификации // Союз криминалистов и криминологов. 2020. № 2. С. 22.

Вышеизложенное свидетельствует о том, что латентность взяток с использованием криптовалюты значительно выше по сравнению с иными формами взяточничества, и связано это, в первую очередь, «с проблемами понимания фактической и юридической сущности криптовалют и со спецификой механизма передачи такой взятки»[121].

Таким образом, из изложенного можно сделать вывод о том, что анонимность использования криптовалют, не требующих идентификации, ее глобальная доступность, предполагающая возможность использования в любой точке мира при наличии телекоммуникационной сети Интернет, и относительная простота применения делают криптовалюту притягательной как для совершения с ее помощью преступлений имущественного характера, так и для использования организациями экстремистской и террористической направленности. Такая тенденция будет сохраняться и далее, если законодателем не будут внесены соответствующие изменения в Уголовный кодекс Российской Федерации, направленные на введение уголовной ответственности за несоблюдение порядка генерации («майнинга») криптовалюты и ее оборота.

[121] Качалов В.В. Указ. соч. С. 22.

Глава 2. АКТУАЛЬНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

§ 2.1. Квалификация неоконченных преступлений, совершаемых с использованием криптовалюты

Все преступления представляют собой некий поведенческий акт человека, совершаемый во временных границах и имеющий свое начало и окончание. Правильное установление таких временных границ имеет важное значение как для квалификации преступлений, так и для разграничения оконченных и неоконченных преступлений. Как справедливо полагают многие ученые, «для того чтобы констатировать наличие в деянии состава преступления, необходимо определить, достигнут ли момент окончания преступления, под которым обычно понимается момент, когда в деянии получают свое отражение все признаки, содержащиеся в составе преступления»[122]. Данное положение законодательно закреплено в ч. 1 ст. 29 УК РФ.

Момент окончания присущ всем без исключения преступлениям, в том числе совершаемым с использованием криптовалюты, несмотря на то что определенный временной период их совершения охватывает и действия, осуществляемые без участия человека. Анализируя уголовные дела о преступлениях, совершенных с использованием криптовалюты, можно сделать вывод, что в определенных случаях момент их окончания является сложно определяемым в силу специфики оборота криптовалюты и технологических особенностей блокчейн-сети и связан непосредственно с

[122] См.: Хорошилова О. С. Классификация составов преступлений по моменту окончания преступления // Вестник Кемеровского государственного университета. 2015. № 2 (62). Т. С. 223.

технологическими возможностями блокчейн-сети, в которой осуществляется оборот соответствующей криптовалюты.

Данное обстоятельство необходимо учитывать при квалификации действий лиц, совершающих такие преступления, определяя момент окончания преступления в материальных, формальных и усеченных составах, отграничивая тем самым покушение от оконченного преступления и разграничивая смежные составы.

В зависимости от конструкции составы преступлений в науке уголовного права принято разделять на материальные, формальные и усеченные. Конструкция каждого из составов преступлений представляет собой набор конкретных признаков каждого элемента состава преступления, которые закреплены в диспозиции соответствующей уголовно-правовой нормы. Такая юридическая конструкция является одним из средств законодательной техники. Указанные процессы обусловлены как структурированностью отдельных уголовно-правовых норм, так и нормами права в целом.

Характерной особенностью преступлений, совершаемых с использованием криптовалюты, является частичная автономность действий блокчейн-сети, в которой осуществляется криптовалютный оборот. Такие действия сети хотя и являются порождением волевого человеческого начала и совместно с действиями человека образуют объективную сторону соответствующего преступления, предусмотренного Особенной частью Уголовного кодекса Российской Федерации, но на волевое человеческое начало отвечают совершением (или несовершением) определенных действий вне зависимости от воли человека. Конечный результат уже не всегда зависит от действий человека. Так, при совершении разновидностей виртуального мошенничества при наличии прямого умысла на завладение чужим имуществом или правом на такое имущество путем обмана, то есть совершении преступлений с материальным составом, момент их окончания, то есть наступления общественно опасных последствий, зависит не от воли

человека, а от того, как на совершаемые им действия среагирует сеть. Например, когда сетью будет сформирован и закрыт соответствующий блок. Исходя из требований ст. 29 УК РФ к неоконченному преступлению относят приготовление к преступлению, при котором осуществляется приискание или приспособление лицом средств или орудий совершения преступления и покушения на преступление. В преступлениях с использованием криптовалюты средством их совершения будет являться различное компьютерное оборудование, которое в процессе совершения преступления предоставляет человеку возможность использовать так называемое виртуальное пространство, то есть увеличивающие его физические возможности. Разумеется, вышеизложенное будет относиться к той части объективной стороны преступления, которая совершается в так называемом виртуальном пространстве. Средством совершения преступления будут являться соответствующие компьютерные программы, используемые для совершения преступления.

Из отчета Центрального банка Российской Федерации следует, что криптовалютные биржи часто являются объектом хакерских атак, при которых в том числе используются и описанные в предыдущей главе способы совершения мошенничества «Атака-51», «Атака Финни», «Эгоистичный майнинг», «Атака Сибиллы», а также ряд других способов. При этом «объёмы украденных криптовалют в результате мошеннических действий за 2019 год составили 4,52 млрд. долларов США, что на 160 % больше, чем в 2018 году. В 2020 году объёмы сократились до 1,9 млрд. долларов США. По отношению к среднегодовому значению капитализации криптовалютного рынка объёмы хищений составили 0,6 % в 2018 году, 2,1 % в 2019 году, 0,6 % в 2020 году. Доля подобных операций в общем объёме операций в 2020 году составила 0,00117 % (в 2019 году – 0,00089 %)»[123].

[123] См.: Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 25.

Еще большую актуальность вопрос определения начала неоконченного преступления приобретает при совершении преступлений с использованием криптовалюты. Необходимо признать, что уголовно-правовые параметры приготовления к преступлению (описание приготовительных действий в законе) являются весьма специфичными, что можно установить на примере относительной неопределенности границы между приготовлением к преступлению и стадией обнаружения умысла.[124] Часть 3 статьи 30 УК РФ определяет покушение на преступление как совершение умышленных действий (бездействие) лица, которые непосредственно направлены на совершение преступления, если при этом преступление не было доведено до конца по обстоятельствам, не зависящим от данного лица.

Применительно к преступлениям, совершаемым с использованием криптовалюты, как покушение не всегда можно рассматривать начало определенных действий лица в виртуальном пространстве. Вряд ли уместным будет рассматривать как начало преступного посягательства действия лица, направленные на включение компьютерного устройства, вход в сеть Интернет или сети блокчейн, если указанные действия не охватывались умыслом лица на совершение определенного преступления, то есть если данные действия не были связаны с началом выполнения объективной стороны преступления. В данном случае под началом преступления следует понимать начало таких действий, которые напрямую были направлены на достижение преступного результата и преследовали цель совершения определенного преступления.

Выделение стадий совершения умышленного преступления имеет как теоретическое, так и практическое значение, так как в соответствии с требованиями ч. 2 ст. 30 УК РФ уголовная ответственность наступает лишь за приготовление только к тяжкому и особо тяжкому преступлениям.

---

[124] См.: Решетников А.Ю. Приготовление к преступлению и покушение на преступление: вопросы дифференциации ответственности // Вестник Краснодарского Университета МВД России. 2015 № 4 (30). С. 72–76.

Само по себе недоведение преступления до конца также еще не дает оснований для оценки указанного преступления в качестве неоконченного[125]. По этому признаку происходит разграничение неоконченного преступления с добровольным отказом от совершения преступления, который происходит при осознании лицом возможности доведения начатого преступления до его логического завершения.

Осуществляя квалификацию преступлений с использованием криптовалюты, необходимо учитывать то обстоятельство, что часть объективной стороны таких преступлений состоит из непосредственных действий человека в сети блокчейн и наступления в результате указанных действий последствий, вызванных реакцией сети на такие действия. При этом сеть не всегда реагирует таким образом, как рассчитывал человек. Возникает естественный вопрос, можно ли квалифицировать как неоконченное преступление реакцию блокчейн-сети, направленную на блокировку действий человека (отрицательную реакцию), рассчитанных в последующем на осуществление хищения криптовалюты из криптокошелька, например невозможность подбора ключа от криптокошелька, без которого невозможно осуществить последующую кражу криптомонет. Совершение подобного рода действий может рассматриваться лишь как приготовление к преступлению, то есть приискание лицом пусть и виртуальных, но средств совершения преступления, и то лишь в том случае, если бы попытка лица приискать такие средства закончилась удачно. Указанное полностью согласуется с требованиями ст. 30 УК РФ, согласно которой приготовлением к преступлению признаются приискание, изготовление, а также приспособление лицом средств или орудий совершения преступления, приискание соучастников преступления, сговор на совершение преступления, а также иные умышленно созданные условия для совершения преступления,

[125] См.: Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. М., 2010. С. 28–35.

если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.

В противном случае вообще нельзя утверждать, что такие действия несут в себе общественную опасность, так как приготовление характеризуется умышленной формой вины, а в данном случае речь идет об абстрактной возможности получения средств доступа к чужому криптокошельку.

Любое приготовление к совершению преступления характеризуется объективными и субъективными признаками.

К объективным признакам относят создание условий для совершения преступления, которое не доведено до конца по независящим от лица обстоятельствам. В свою очередь к субъективным признакам относят умышленный характер создания условий для совершения преступления.

В данном случае, равно как и при осуществлении мошеннических действий в блокчейн-сети, указанные признаки отсутствуют, так как лицо не может заранее предсказать реакцию сети на его действия и предвидеть результат таких действий.

Таким образом, квалификация деяния как покушения на преступление допустима при наличии в поведении лица соответствующей фактической ошибки.

К таким ошибкам могут быть отнесены неправильный подбор блокчейн-приложения, то есть приложения, каждый экземпляр которого хранит свой экземпляр блокчейна, идентичный цепочке блоков всех остальных участников сети, и синхронизируется с ними при помощи алгоритма консенсуса[126]. Вопрос правильности выбора соответствующего блокчейн-приложения требует специальных знаний, но является обязательным к разрешению на предмет наличия фактической ошибки при совершении мошеннических действий под условными наименованиями «Атака», «Атака Финни», «Эгоистичный

[126] См.: Галкин Р.Е., Старолетов С.М. О методах тестирования блокчейн-приложений // Высокопроизводительные вычислительные системы и технологии. 2021. Т. 5. № 1. С. 98–106.

майнинг», «Атака Сибиллы». Неправильно выбранное лицом блокчейн-приложение, то есть его ошибка относительно природы средства совершения преступления, используемого им для достижения преступного результата, приведет к невозможности осуществления им дальнейших действий, направленных на окончание преступления и достижение цели его совершения. Соответственно, при этом ответственность в соответствии с ч. 3 ст. 30 УК РФ наступает за покушение на совершение задуманного им преступления. Необходимо отличать действия, совершенные с ошибкой относительно природы средства совершения преступления, от действий, когда в силу определенных причин, например боязни потерять соответствующее вознаграждение за вычисление нового блока, лицо добровольно отказывается от совершения дальнейших действий, направленных на достижения преступного результата. Так, например, блокчейны на базе «Эфириум» (Ethereum), «Криптон» (Krypton) и «Шифт» (Shift) стали жертвами атак 51 % в августе 2016 года[127]. После указанного случая разработчики проектов внедрили дополнительные системы защиты. Так, например, в базе «Криптон» было увеличено число подтверждений, необходимых для одобрения транзакции, до одной тысячи[128]. В случае если система предусматривает защиту от мошенничества, совершенного способом «Атака 51», и лицо, совершающее указанную атаку, может потерять соответствующее вознаграждение или получить соответствующий «штраф», лишившись имеющихся у него криптомонет[129], вследствие чего отказывается от продолжения совершения действий, направленных на совершение мошенничества, такие действия рассматриваются как добровольный отказ от совершения преступления, так как лицо имело возможность совершить

[127] См.: Галкин Р.Е., Старолетов С. М. Указ. соч. С. 98–106.
[128] Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 5–18.
[129] См.: Петров С. Уничтожаем криптомифы. Можно ли защитить монету от атаки 51 процента? [Электронный ресурс]. – Режим доступа: https://2bitcoins.ru/mozhno-li-zashhititsya-ot-ataki-51/ (дата обращения – 29.04.2022).

преступление, но из-за опасений возможных негативных для себя последствий отказалось от их совершения.

Ученые полагают, что организация атак на ведущие мировые криптовалюты является дорогостоящим мероприятием, которое требует больших денежных вложений[130]. Согласно результатам исследования «Безопасность протокола Биткойн», проведенного профессором С. Вижайакумараном, «атака 51% на сеть биткойна экономически бесполезна для злоумышленников, так как требует «значительных расходов» и не несет никакой «финансовой отдачи»[131]. Опасения лишиться при совершении мошеннических действий средств, затраченных на окончание данного преступления, может являться мотивом добровольного отказа от совершения дальнейших действий, направленных на окончание преступления. Могли ли при этом в силу технических возможностей соответствующей сети блокчейн наступить такие последствия, которых намеревалось достичь лицо, совершающее преступление, значения для квалификации его действий не имеет. При этом мотивы, по которым лицо отказалось от совершения преступления, никакой роли не играют, вследствие чего до тех пор, пока досрочное завершение преступления зависит только от самого лица, речь идет о добровольном отказе от совершения преступления с использованием криптовалюты.

Аналогичного мнения придерживаются А.Ю. Решетников и Е.А. Русскевич, полагающие, что «добровольным отказом, безусловно, следует признавать случаи, когда лицо самостоятельно прекращает действия, направленные на преодоление средств информационной защиты»[132].

---

[130] См.: Попандопуло И. Д., Аникин А. В. «Атака 51 %» в криптовалютных системах: сущность, прецеденты, затратность // Научно-методический электронный журнал «Концепт». 2019. № 1. С. 205—211.

[131] См.: Костюкова Е. Н. Криптовалюта и риски ее функционирования. – 2019. – № 1(5). – С. 42–46.

[132] Решетников А.Ю., Русскевич Е.А. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации // Уголовное право. 2018. № 2. С. 23.

Не может быть признан добровольным отказ, который вызван невозможностью дальнейшего продолжения преступных действий, например, в силу отрицательного на них реагирования блокчейн-сети.

Для определения содержания в содеянном признаков приготовления к преступлению необходимо установить, были ли созданы соответствующие условия для совершения преступления, имелось ли у лица соответствующее компьютерное оборудование и программное обеспечение, обладало ли оно необходимыми специальными знаниями для работы в блокчейн-сети. Именно создание таких условий характеризует приготовительную деятельность.

Учитывая децентрализованность сети блокчейн, местом начала преступления будет то место географического нахождения объекта (физического лица), где данное лицо с помощью технических средств осуществило противоправные действия, используя блокчейн-технологию. В преступлениях с формальным составом это же место будет и местом окончания данного преступления, так как формальный состав преступления предполагает, что оно будет считаться оконченным с окончанием действий, совершение которых запрещено под угрозой уголовного наказания.

Относительно преступлений с материальным составом, предусматривающим наступление общественно опасных последствий, необходимо отметить, что такое преступление с использованием криптовалюты будет считаться оконченным, когда создан блок, подтвердивший противоправную транзакцию, и криптомонеты незаконным способом выбыли из правообладания их первоначального владельца, поступив в иной криптокошелек.

Постановлением Пленума Верховного Суда Российской Федерации от 29 июня 2021 года № 22 (ред. от 29 июня 2021 года) «О судебной практике по делам о краже, грабеже и разбое» даны разъяснения (п. 25.2), в соответствии с которыми кражу, ответственность за которую предусмотрена п. «г» ч. 3 ст. 158 УК РФ, следует считать оконченной с момента изъятия денежных средств с банковского счета владельца указанных средств или электронных денежных

средств, в результате которого владельцу этих средств причинен ущерб. Местом окончания такой кражи является место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета.

Однако к краже криптомонет из криптокошелька данные разъяснения неприменимы ввиду нижеследующего:

1. Из технологических принципов функционирования технологии блокчейн следует, что не может существовать банк или иная организация, в которых имеется криптокошелек потерпевшего, из которого было осуществлено хищение принадлежавших ему криптомонет. Все криптокошельки находятся в сети блокчейн, то есть в системе распределенной базы данных, и не имеют привязки к какому-либо серверу или иному устройству их электронного хранения, то есть они хранятся на всех компьютерных устройствах участников данной сети.

2. Закрытие блока и транзакция криптомонет происходит в распределенной сети данных без участия человека и контроля с его стороны или стороны созданных им организаций или учреждений, вследствие чего изъятие криптомонет из криптокошелька потерпевшего произойдет только после закрытия сетью соответствующего блока. До закрытия блока и фактического изъятия криптомонет из криптокошелька потерпевшего такое хищение будет считаться неоконченным преступлением, то есть имеет место покушение на совершение соответствующего вида хищения. Кража критовалюты должна квалифицироваться по общему правилу по ст. 158 УК РФ, когда, например, преступник любым способом тайно похищает флеш-карту с учетными данными, либо совершает аналогичные действия с использованием компьютерных программ, такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. Если хищение чужого

имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по статье 159, а не 159^6 УК РФ). В случаях, когда такое деяние сопряжено с обманом или злоупотреблением доверием, когда преступник вынуждает обманом сообщить пароль или перечислить криптовалюту, даже если при этом преступник использует общедоступные компьютерные программы, деяние должно быть квалифицировано по ст. 159 УК РФ. Если хищение совершено с целенаправленным воздействием специальных программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники, деяние должно быть квалифицировано по ст. 159^6 УК РФ. Вследствие того, что криптовалюта не является электронным средством платежа, квалификация вышеуказанных преступлений по ст. 159^3, также, как и по ст. 187 УК РФ, производиться не может.

Таким образом, при определении времени и места окончания преступления, совершенного с использованием криптовалюты, необходимо учитывать указанные технические особенности функционирования криптовалюты в соответствующей распределенной блокчейн-сети, не позволяющей говорить о конкретном месте закрытия блока и проведенной транзакции, так как местом начала и окончания транзакции и соответственно местом начала и окончания хищения криптомонет будет являться вся распределенная блокчейн-сеть, находящаяся одновременно по всему миру. Преступление будет считаться оконченным с момента создания нового блока, подтверждающего произведенную транзакцию. Так, субъект описанных в предыдущем параграфе мошеннических действий с использованием криптовалюты, получивших условное название «Атака», «Атака 51», «Атака Финни», «Эгоистичный майнинг», выполняя объективную сторону, по сути,

никогда не знает, в какой момент система сформирует соответствующий блок и перечислит криптомонеты, которыми он пытается завладеть в контролируемый им криптокошелек. Более того, алгоритм действий данной системы в каждом конкретном случае, если можно так сказать, известен только ей самой. Иными словами, система осуществляет действия в соответствии с определенными алгоритмами, созданными человеком, но каким образом используются такие алгоритмы, не понимает даже разработчик таких систем. Можно говорить о том, что человек совершает определенные действия, последствия совершения которых ему заранее достоверно не известны, но при этом он все же надеется, используя специальные знания и навыки работы с блокчейн-сетями, достигнуть запланированного им преступного результата.

Характерной особенностью таких преступлений является то обстоятельство, что часть объективной стороны состава преступления по команде человека выполняет машина, и выполняет она эти действия на основании определенных математических алгоритмов, а не желания человека, подавшего команду машине на совершение данных действий.

Мошенничество, то есть хищение чужого имущества либо приобретение права на чужое имущество путем обмана или злоупотребления доверием, может быть признано оконченным с того момента, когда соответствующий блок был окончательно сформирован и закрыт системой, а криптомонеты поступили в незаконное владение виновного лица либо других лиц, и они получили реальную возможность ими распоряжаться. То есть криптомонеты, незаконно выбывшие из владения их собственника, должны быть «зачислены» в криптокошелек виновного либо других лиц, что позволит им пользоваться и распоряжаться данными криптомонетами по своему усмотрению.

Необходимо отметить, что существует иная точка зрения по данному вопросу, основанная на том, что в случае когда предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений п. 1 примечаний к

ст. 158 УК РФ и ст. 128 ГК РФ содеянное должно рассматриваться как кража. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Необходимо отметить, что в случаях с криптовалютой как одну из форм хищения можно рассматривать мародерство, ответственность за которое предусмотрено ст. 356.1 УК РФ. Диспозиция указанной статьи предусматривает совершенные с корыстной целью в периоды военного положения, военного времени, а также в условиях вооруженного конфликта или ведения боевых действий и не связанные с вынужденной необходимостью противоправные безвозмездное изъятие и (или) обращение в пользу виновного или других лиц чужого имущества (в том числе имущества, находящегося при убитых или раненых, имущества гражданского населения). Учитывая, что криптовалюта относится к иному имуществу, представляется фактически возможным совершить ее противоправное, безвозмездное изъятие у собственников в указанные в диспозиции ст. 356.1 УК РФ периоды.

В том случае, если мошенничество совершено в форме приобретения права на чужое имущество, преступление считается оконченным с момента возникновения у виновного юридически закрепленной возможности вступить во владение или распорядиться чужим имуществом, как своим собственным. Указанная точка зрения отражена в постановлении Пленума Верховного Суда РФ от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», однако неприменима к мошенничеству, совершенному с криптовалютой в блокчейн-сети, так как при непринятии блока сетью криптовалюта останется в кошельке предполагаемой жертвы, в отличие от других электронных денежных средств. Таким образом, вышеприведенные разъяснения неприменимы к совершению мошенничества с криптовалютой в блокчейн-сети, так как лицо, совершающее действия, направленные на приобретение права на чужое имущество (криптовалюту) путем обмана, фактически такое право не получает, пока блокчейн-сеть не

закроет соответствующий блок, что и будет являться подтверждением такого права.

Соответственно, в тех случаях, когда мы говорим о мошенничестве, при наличии прямого умысла субъекта на завладение чужим имуществом (криптомонетами) путем обмана и совершении им действий, образующих объективную сторону данного преступления, можно говорить об уголовной ответственности за неоконченное преступление, предусмотренное ч. 3 ст. 30 УК РФ, так как завладение чужим имуществом (либо получением права на такое имущество) не произошло в результате наличия обстоятельств, не зависящих от воли данного лица. Таким образом, при разграничении оконченного и неоконченного преступления в любом виде хищения криптомонет должна быть учтена описанная особенность блокчейн- сетей, при закрытии которыми сформированного блока происходит одномоментное изъятие криптомонет из кошелька потерпевшего и зачисление их в кошелек злоумышленника или других лиц. То есть два эти действия совпадают по времени и образуют оконченную транзакцию, что и отличает такие транзакции от электронных платежей, в которых момент изъятия денежных средств со счета потерпевшего и зачисление их на другой счет могут быть разнесены по времени.

При этом если лицо самостоятельно не осуществляло попыток воздействия на блокчейн-сеть, а требовало таких действий от другого лица, например от потерпевшего, не совершившего таких действий под влиянием обстоятельств от злоумышленника не зависящих, такие действия будут квалифицироваться как покушение на совершение преступления.

Так, например, следственным управлением Следственного комитета Российской Федерации по Чувашской Республике было расследовано уголовное дело в отношении 31-летнего нигде не работающего жителя города Чебоксары. Ему было предъявлено обвинение в совершении преступления, предусмотренного ч. 3 ст. 30, ч. 4 ст. 159 УК РФ (покушение на мошенничество в особо крупном размере). По версии следствия, в июне-июле

2017 года в городе Чебоксары обвиняемый, находясь у себя дома, при помощи компьютера дистанционно пытался похитить денежные средства в размере 50000 долларов США, что эквивалентно сумме около 3 000 000 рублей, у одного из предпринимателей, осуществляющих свою деятельность в сфере ресторанного бизнеса. Посредством электронной переписки со специально созданной для этих целей электронной почты он ввел его в заблуждение относительно того, что якобы некие третьи лица намереваются совершить его убийство, а за указанную сумму он предоставит информацию, которая могла бы предотвратить якобы возникшую для потерпевшего угрозу жизни. При этом он требовал конвертировать эти деньги в криптовалюту биткоин и перевести на указанный им криптокошелек. Однако он не смог довести свои преступные действия до конца, поскольку потерпевший своевременно обратился в Следственный комитет России. Причастность обвиняемого к инкриминируемому деянию была подтверждена его признательными показаниями, показаниями свидетелей, результатами обыска, проведенного по месту жительства обвиняемого, а также заключением судебной компьютерно-технической экспертизы[133]. Данный пример показательно демонстрирует совершение неоконченного преступления с использованием криптовалюты. В случае если криптовалюта использовалась при совершении преступлений, предусмотренных главой 30 действующего УК РФ, например, получение взятки, то переданное в качестве взятки имущество, которым, с точки зрения действующего законодательства, является криптовалюта, должно получить денежную оценку, что может быть осуществлено также путем получения следователем сведений с одной из криптовалютных бирж, где указанная криптовалюта была приобретена. Такую информацию можно получить на соответствующем сайте криптовалютной биржи. Данная информация является открытой, общедоступной и не требует наличия специальных знаний.

[133] См.: В Чувашии перед судом предстанет местный житель, обвиняемый в покушении на мошенничество в особо крупном размере с криптовалютой [Электронный ресурс] // Официальный сайт Следственного комитета Российской Федерации. http://sledcom.ru/news/item/1197736/ (дата обращения – 21.04.2023).

Соответственно, она может быть получена любым заинтересованным лицом, и для определения стоимости криптовалюты не требуется назначение экспертизы.

При этом можно полностью согласиться с мнением ученых, полагающих, что «передача криптовалюты в качестве предмета взятки не подпадает под указанные признаки неоконченных преступлений, наоборот, данные обстоятельства будут свидетельствовать о том, что виновное лицо выполнило в полном объеме объективную сторону преступления, доведя до конца свой умысел, равно как и лицо, получившее криптовалюту. Как покушение данное преступление можно было бы квалифицировать в случае, если в момент передачи (или перевода) криптовалюты действия виновных были бы пресечены сотрудниками правоохранительных органов»[134]. В данном случае нужно исходить из того обстоятельства, что до тех пор, пока соответствующий блок не подтверждён сетью и не осуществлено его закрытие, должностное лицо никоим образом не может получить предназначавшуюся ему криптовалюту в силу технологии ее (криптовалюты) оборота. Соответственно, нельзя говорить о применении к таким случаям разъяснений, данных в постановлении Пленума Верховного Суда Российской Федерации от 9 июля 2013 года № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» относительно окончания коррупционных преступлений с момента принятия должностным лицом или лицом, выполняющим управленческие функции в коммерческой или иной организации, хотя бы части передаваемых ему ценностей, так как в случаях с криптовалютой транзакция (перевод) не был осуществлен ни в какой части.

В том случае, если передача криптовалюты была осуществлена посредством передачи взяткополучателю пароля от криптокошелька, преступление будет считаться оконченным вне зависимости от возможности

---

[134] Долгиева М.М. Квалификация деяний, совершаемых в сфере оборота криптовалюты // Вестник Восточно-Сибирского института МВД России. 2019. № 1(88). С. 18.

воспользоваться указанным паролем и открыть соответствующий криптокошелек, так как в этом случае имеющаяся в кошельке криптовалюта поступила в полное распоряжение взяткополучателя.

Учитывая, что получение, дача взятки или незаконного вознаграждения при коммерческом подкупе, посредничество во взяточничестве в виде непосредственной передачи взятки считаются оконченными с момента принятия должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации, хотя бы части передаваемого ему имущества, а в случаях использования криптовалюты — с момента поступления в его криптокошелек соответствующих криптомонет, вопрос доказывания указанных обстоятельств, то есть подтверждения соответствующей транзакции и принадлежность криптокошелька определенному лицу, является первостепенным.

Резюмируя изложенное, можно прийти к следующему выводу. Часть объективной стороны большинства преступлений с использованием криптовалюты всегда совершается дистанционно с использованием блокчейн-сети, что лишает правоприменителя возможности определить момент окончания такого преступления, если это преступление с материальным составом (например, разновидность хищения). При этом правоприменитель также лишен возможности определить юрисдикцию государства, на территории которого данное преступление было окончено, если не признавать окончанием преступления место нахождения виновного лица в момент совершения преступления. Более того, при любом виде хищения криптомонет преступление будет считаться оконченным только лишь при закрытии блокчейн-сетью соответствующего блока определенной транзакции. Сеть при этом является децентрализованной, то есть не находится на территории конкретного государства, а существует на компьютерах пользователей, расположенных в разных странах мира. Данное обстоятельство не позволяет осуществить должное уголовное преследование лиц, совершающих преступления с использованием криптовалюты. В целях устранения

указанного препятствия уголовного преследования лиц, совершивших преступления с использованием криптовалюты, необходимо усиление трансграничного сотрудничества в части надзора за оборотом криптовалюты и применения ограничительных мер, в том числе уголовно-правового характера, направленных на пресечение таких преступлений и привлечение лиц, их совершивших, к уголовной ответственности.

Преступления, предусмотренные статьями 174 и 174^1 УК РФ, совершенные путем финансовых операций, следует считать оконченными с момента, когда лицо, действуя с указанной в данных статьях целью, непосредственно использовало преступно полученные от реализации криптовалюты денежные средства в целях маскировки связи легализованного имущества (денежных средств) с преступным источником его происхождения (основным преступлением).

В тех случаях, когда названные преступления совершались путем сделки, их следует считать оконченными с момента фактического исполнения виновным лицом хотя бы части обязанностей или реализации. Ответственность по ст. 174 или ст. 174^1 УК РФ наступает и при совершении одной финансовой операции или сделки с денежными средствами или иным имуществом, приобретенными преступным путем (в результате совершения преступления), если будет установлено, что такое деяние было совершено с целью придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами либо иным имуществом. Таким образом, сам по себе факт покупки или продажи криптовалюты, полученной преступным путем, не образует составы преступлений, предусмотренных ст. 174 или ст. 174^1 УК РФ.

На признание преступления оконченным не влияет то обстоятельство, что финансовые операции или сделки осуществлялись в условиях оперативно-разыскного мероприятия, проводимого в соответствии с Федеральным законом от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности». В данном случае необходимо учитывать, что понятие

«финансовая операция» не имеет однозначного общепризнанного толкования и не закреплено в действующем законодательстве, вследствие чего толкование термина может быть различным. Так, например, А.А. Краюшкин, обобщивший мнения различных ученых по данному вопросу, полагает, что к финансовым относятся такие операции по движению капитала, как, например, зачисление денежных средств на чей-либо счет или осуществляется какое-либо иное движение денежных средств[135]. Таким образом, обмен криптовалюты на фиатные деньги может быть отнесен к финансовым операциям, вследствие чего, например, финансированием терроризма следует признавать, наряду с оказанием финансовых услуг, предоставление или сбор не только денежных средств (в наличной или безналичной форме), но и криптовалюты для финансирования организации, подготовки или совершения хотя бы одного из преступлений, предусмотренных статьями 205, 205^1, 205^2, 205^3, 205^4, 205^5, 206, 208, 211, 220, 221, 277, 278, 279 и 360 УК РФ, либо для финансирования или иного материального обеспечения лица в целях совершения им хотя бы одного из этих преступлений. Данный вывод полностью соотносится с разъяснениями, данными в постановлениях Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» и Пленума Верховного Суда Российской Федерации от 9 февраля 2012 года № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности».

При совершении преступления с материальным составом или покушении на совершение такого преступления с использованием криптовалюты, при любой разновидности хищения возникает вопрос о

---

[135] См.: Краюшкин А.А. Понятие финансовой операции как вида деятельности, образующей легализацию преступных доходов // Вестник Московского университета МВД России. 2009. № 10. С. 113–115.

необходимости дополнительной квалификации такого деяния по соответствующей статье главы 28 (преступления в сфере компьютерной информации) УК РФ, так как любое хищение криптомонет осуществляется непосредственно в виртуальной блокчейн-сети и почти всегда связано с компьютерной информацией, которая при этом изменяется или модифицируется. Изменению или модификации должна быть подвергнута информация определенного пользователя, владеющего такой информацией на законных основаниях, что в принципе неприменимо к блокчейн-сетям, не принадлежащим конкретному пользователю или пользователям и не контролируемым с чьей-либо стороны. Кроме того, к охраняемой законом компьютерной информации относятся сведения, доступ к которым ограничен в соответствии с Федеральным законом от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне», Федеральным законом от 28 ноября 2011 года № 335-ФЗ «Об инвестиционном товариществе», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Законом Российской Федерации от 20 июля 2012 года № 125-ФЗ «О донорстве крови и ее компонентов», Федеральным законом от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 25 июля 1998 года № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации», Федеральным законом от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 28 декабря 2022 года № 555-ФЗ «О гарантировании прав участников негосударственных пенсионных фондов в рамках деятельности по негосударственному пенсионному обеспечению», Федеральным законом от 2 декабря 1990 года № 395-1 «О банках и банковской деятельности», Федеральным законом от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», Федеральным законом от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Закона Российской Федерации от 2 июля 1992 года № 3185-1 «О психиатрической помощи и гарантиях прав граждан

при ее оказании», Закона Российской Федерации от 22 декабря 1992 года № 4180-1 «О трансплантации органов и (или) тканей человека», Основ законодательства Российской Федерации о нотариате от 11 февраля 1993 года № 4462-1, Федеральным законом от 31 мая 2002 года № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации», Федеральным законом от 30 декабря 2008 года № 307-ФЗ «Об аудиторской деятельности», Федеральным законом от 24 июля 1998 года № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний», Федеральным законом от 7 июля 2003 года № 126-ФЗ «О связи», Семейным кодексом Российской Федерации и другими федеральными законами Российской Федерации, относящими определенные сведения к ограниченной категории доступа. Пленум Верховного Суда Российской Федерации в постановлении «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» от 15 декабря 2022 года № 37 разъяснил, что по смыслу ч. 1 ст. 272 УК РФ в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен соответствующий специальный режим ее правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности. Применительно к ст. 272 УК РФ неправомерным доступом к компьютерной информации будет являться получение или использование такой информации без согласия обладателя информации лицом, которое не наделено

необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа).

Исходя их вышеизложенного, можно констатировать, что используемая при осуществлении оборота криптовалюты технология блокчейн в определенных случаях оказывает непосредственное влияние на момент окончания преступлений с использованием криптовалюты, совершаемых в виртуальном пространстве. При совершении указанных преступлений не всегда представляется возможным четко разграничить стадии приготовления к совершению преступления и покушения на его совершение, что в свою очередь приводит к спорам относительно места совершения преступления.

Полагаем, что местом совершения преступления с использованием криптовалюты (с учетом того, что такое преступление будет считаться оконченным с момента закрытия блока в децентрализованном реестре) необходимо считать географически определенную точку в пространстве, обозначающую место использования преступником компьютерного оборудования в целях совершения преступления.

§ 2.2. Особенности соучастия в преступлениях, совершаемых с использованием криптовалюты

Преступления, совершаемые группой лиц, то есть двумя и более лицами, как правило, обладают большей степенью общественной опасности, чем преступления, совершаемые единолично, так как объединение усилий группы для достижения преступного результата облегчает совершение действий, образующих объективную сторону преступления. Данное утверждение в полной мере относится и к преступлениям, которые совершаются с использованием криптовалюты, так как такие преступления совершаются, как правило, группой лиц по предварительному сговору, в которой участвуют лица, заранее договорившиеся о совместном совершении преступления, либо организованной группой, то есть устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений с использованием криптовалюты. Это детерминировано рядом условий.

Первым условием следует считать наличие у лица специальных технических знаний в IT-сфере, позволяющих работать с криптовалютой с максимальной степенью анонимности. И хотя криптовалютная отрасль получает все большее распространение во всем мире, количество специалистов, имеющих специальные знания о работе блокчейн-сетей, крайне ограничено. Большинство людей осуществляют свою работу с криптовалютой на уровне пользователей, либо вообще не имеют представления об информационной безопасности, либо их знания носят разрозненный характер и не позволяют противостоять потенциальным угрозам. Наличие у специалистов знаний в IT-сфере предоставляет им возможность как противостоять преступным посягательствам, так и совершать преступления с использованием криптовалюты. Соответственно, востребованность таких специалистов возрастает и в криминальных кругах, так как позволяет совершать преступления с высоким уровнем латентности.

Такие случаи на территории Российской Федерации фиксировались неоднократно. Так, следователем Следственной части Следственного управления МВД России по Республике Крым было возбуждено уголовное дело в отношении подозреваемого по признакам состава преступления, предусмотренного п. «а» ч. 4 ст. 174^1 УК РФ. В период с 21 августа по 12 декабря 2016 года подозреваемый, осуществляя в составе организованной группы на территории Республики Крым незаконный сбыт наркотических средств, используя счета в биткойн-кошельке и в электронной платежной системе QIWI, получил в качестве оплаты за выполнение своей функции в преступной группе денежные средства, которые затем перевел на принадлежащие ему банковские карты, впоследствии обналичил их и распорядился по своему усмотрению[136]. В данном случае не представляется возможным дополнительно квалифицировать действия подсудимого по ст. 174^1 УК РФ, так как его действия не были направлены на придание законности полученным в результате обмена криптовалюты денежным средствам.

Указанный пример демонстрирует наличие в составе организованных преступных групп исполнителей, обладающих специальными знаниями. Такие лица не только непосредственно выполняют объективную сторону преступлений с использованием криптовалюты, но и принимают меры к сокрытию следов совершенного преступления.

При таких обстоятельствах для вменения квалифицирующего признака «организованная группа» необходимо наличие устойчивости такой группы и общность целей.

Организаторы таких групп, осуществляя общее руководство и планирование преступных действий, могут выполнять часть объективной стороны преступления, а могут и не принимать непосредственного участия в выполнении объективной стороны преступлений с использованием

---

[136] Приговор Железнодорожного районного суда г. Симферополя (Республика Крым) по уголовному делу по делу № 1-200/2020 от 29 июля 2020 г. [Электронный ресурс] Режим доступа:http://zheleznodorozhniy.krm.sudrf.ru/modules.php?name=press_dep&op=12&arc_list=2019-07 (дата обращения – 25.04.2023).

криптовалюты, при этом пользоваться результатами преступной деятельности, то есть фиатными денежными средствами, полученными в результате обмена криптовалюты, полученной в результате совершения таких преступлений. В том и другом случае их действия необходимо рассматривать как соисполнительство.

Так, например, Следственной частью Главного следственного управления Главного управления МВД России по Волгоградской области расследовалось уголовное дело по признакам преступлений, предусмотренных ч. 4 ст. 159^{6}, п. «а» ч. 4 ст. 174^{1} УК РФ, в отношении N и неустановленных лиц по факту хищения организованной преступной группой денежных средств, принадлежащих пользователям услуг дистанционного банковского обслуживания, путем вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации. А также по факту совершения N и неустановленными лицами, в составе организованной преступной группы, финансовых операций по обналичиванию похищенных денежных средств в целях придания правомерного вида владению, пользованию и распоряжению данными денежными средствами.

В ходе предварительного расследования было установлено, что в неустановленное время N, являясь активным пользователем сети Интернет, вступил в состав организованной преступной группы с целью совершения хищения денежных средств пользователей услуг дистанционного банковского обслуживания путем вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации, а именно путем заражения устройств под управлением операционной системы «Андроид» вредоносным программным обеспечением и «перехвата» личной информации о банковских картах пользователей.

Организованная группа действовала следующим образом. Неустановленное лицо, являясь организатором организованной преступной группы, при помощи вредоносных компьютерных программ получало

учетные данные банковских карт, которые предоставляло и аккумулировало их на интернет-ресурсах, доступ к которым имели только вовлеченные им члены преступной группы, в том числе и N. В дальнейшем исполнители преступления, а именно N и неустановленные лица, действуя согласно отведенным ролям, получив и использовав учетные данные персональных банковских карт, без ведома их владельцев, используя персональные электронные устройства, осуществляли переводы денежных средств потерпевших иным лицам, включенным в состав преступной группы, задача которых заключалась в совершении финансовых операций по обналичиванию похищенных денежных средств в целях придания правомерного вида владению, пользованию и распоряжению ими. В дальнейшем путем перевода обналиченных денежных средств в криптовалюту биткоин на специальных теневых ресурсах в сети Интернет похищенные денежные средства переводились N на подконтрольные ему биткойн-кошельки[137]. Необходимо отметить, что включать в организованную группу неустановленных лиц возможно только лишь при условии наличия доказательств, подтверждающих совершение преступления определенным лицом в составе организованной группы.

Данный пример подтверждает факт того, что организованные преступные группы используют для совершения преступлений специалистов в сфере IT-технологий, отводя им роль технических специалистов, выполняющих объективную сторону указанных преступлений в виртуальном пространстве, то есть непосредственных исполнителей. В определенных случаях, например, при совершении разбоя, грабежа или вымогательства, предметом которых является криптовалюта, указанные специалисты не только скрывают следы преступления, используя, например, в целях невозможности

[137] Шепель Н.В. Некоторые особенности доказывания при расследовании преступлений, связанных с использованием криптовалют и других виртуальных активов // Право: ретроспектива и перспектива. 2022. № 3(11). С. 96.

идентификации лиц, завладевших криптовалютой потерпевшего, криптовалютные миксеры, то есть содействуя совершению преступления.

Согласно исследованию американской компании Cipher Trace, оказывающей помощь правоохранительным органам в поиске нелегальных операций с криптовалютой в блокчейн-сети, в 2018 году было похищено криптовалюты на сумму около 1,7 млрд. долларов США (в 3,6 раза больше, чем в 2017 году). Из них более 950 млн. долларов США были похищены с криптовалютных бирж и криптовалютных обменных сервисов[138]. Объемы хищений криптовалюты позволяют говорить о наличии соответствующих организаций, оказывающих услуги по отмыванию (легализации) средств, полученных в результате совершения преступления, то есть придающих законность полученной в результате совершения преступлений криптовалюте. Такой вывод можно сделать исходя из принципов работы сетей блокчейн, позволяющих отслеживать любую криптомонету с момента ее создания (генерации), что в свою очередь позволяет применять санкции к лицам такие криптомонеты использующие. Тем не менее вышеуказанные объемы ущерба в результате хищения криптомонет, позволяют говорить о наличии организаций, специализирующихся на придании вида законности похищенным криптомонетам либо путем использования криптомиксеров, либо иными способами, в том числе обменом криптовалюты на фиатные деньги в странах со слабо регулирующим данную область законодательством.

Согласно представленному компанией Chainalysis аналитическому отчету «Крипто-преступность 2021», большая часть отправленных с криминальных криптокошельков средств попадает на депозитные кошельки крупных крипто-бирж с правилами, не обеспечивающими комплексную систему мер безопасности криптовалютных транзакций, построенными с учетом требований действующего национального законодательства или

---

[138] См.: Cryptocurrency Anti-Money Laundering Report (Report-AML-20180703) / Cipher Trace, 2018. [Электронный ресурс]. Режим доступа: https://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf (дата обращения – 02.05.2022).

специальных сервисов анонимизации, усложняющими отслеживание криптовалютных транзакций в соответствующей блокчейн-сети. Такие сервисы используют технологию, позволяющую раздробить средства клиента на мелкие части, после чего смешивают их в случайном порядке с частями средств других клиентов. В результате указанных операций к конечному получателю приходит заданное количество криптовалюты, но разными транзакциями от разных случайно выбранных адресов из общего пула, принадлежащего сервису, онлайн-казино или сервисов, расположенных в юрисдикциях с высоким уровнем риска[139]. Часть таких кошельков-получателей могут контролироваться самими отправителями, то есть фактически проводят транзакции между принадлежащими им же криптокошельками. Другая часть принадлежат сторонним сервисам, предоставляющим преступникам услуги по отмыванию денег, полученных в результате совершения преступления. Такие сторонние сервисы, работающие внутри крупных бирж, заимствуют у них ликвидность и торговые пары крипто-валют (комбинация двух криптовалют для облегчения торговли на криптовалютной бирже). Так, например, клиент такой криптобиржи может создать свой собственный счет на бирже и предлагать различные услуги неопределенному кругу лиц через свой личный счет или заниматься так называемым «криптовалютным арбитражем» (перепродажа криптомонет по более выгодному курсу).

Исходя из технологии функционирования блокчейн, операции вложенных сервисов будут отображаться как проведенные через базовую платформу, на которой размещен вложенный сервис. Распространенные примеры вложенных сервисов – брокеры внебиржевых сделок и мгновенные «обменники», то есть интернет-сайты, предлагающие мгновенный обмен криптовалюты на фиатные деньги с сохранением анонимности лица, совершающего подобную сделку, что в свою очередь может образовывать

[139] См.: The Chainalysis 2021 Crypto Crime Report…

состав преступления, предусмотренного ст. 172 УК РФ (незаконная банковская деятельность). Такие сервисы осуществляют свою деятельность в различных странах, но доступ к ним может быть осуществлен и с территории Российской Федерации. Возможность использования больших объемов полученных в результате совершения преступлений наличных денежных средств, которые могут быть переведены через вложенные сервисы[140], некоторые из которых соответствуют требованиям, предъявляемым регуляторами к основным биржам, позволяет говорить о том, что часть из вложенных сервисов целенаправленно обслуживает именно лиц, совершающих преступления в сфере высоких технологий, в том числе и преступления с криптовалютой[141]. Такой способ совершения преступлений используется в том числе крупными компаниями, для которых незаконная деятельность составляет лишь небольшую долю от общего объема сделок, что в свою очередь позволяет предположить, что нелегальные средства попадают в законный оборот вследствие пробелов национального законодательства. Часть таких, если их так можно назвать, «депозитных» криптокошельков, аккумулируют криптовалюту, поступающую с других кошельков, используемых при совершении преступлений. Указанные сервисы просто не смогут работать, не обслуживая преступников, совершающих преступления в сфере высоких технологий, что в свою очередь может свидетельствовать о совершении преступлений, предусмотренных ст. 172 (незаконная банковская деятельность), ст. 172^2 (организация деятельности по привлечению денежных средств и (или) иного имущества), ст. 172^3 (невнесение в финансовые документы учета и отчетности кредитной организации сведений о размещенных физическими лицами и индивидуальными предпринимателями денежных средствах) УК РФ. Таким образом, на основании сведений представленного аналитического отчета можно сделать вывод о том, что в

[140] Термином «вложенные сервисы» обозначается наличие на одном сайте различных функциональных приложений.
[141] См.: См.: The Chainalysis 2021 Crypto Crime Report…

данном случае имеет место организованная преступная группа со строгим распределением ролей. Имеется организатор, который планирует совершение преступлений с использованием криптовалюты и осуществляет контроль за деятельностью остальных участников группы, имеются исполнители, непосредственно осуществляющие действия в зависимости от ранее определенной им роли, и имеются пособники из числа лиц, обладающих специальными знаниями в сфере блокчейн-технологий, осуществляющие соответствующую техническую и консультативную поддержку преступной деятельности. Часть членов такой группы могут не знать друг друга в лицо, но по характеру совершаемых ими действий и ранее достигнутой с организатором договоренности выполняют отведенную им роль в организованной преступной группе и осуществляют свою деятельность для достижения общего преступного результата. Использование современных средств связи, в том числе программ, позволяющих оперативно обмениваться сообщениями, осуществлять звонки через Интернет (мессенджеры), обеспечивать анонимность в Интернете (анонимайзеров), предоставляет возможность членам такой организованной группы не вступать в непосредственный визуальный контакт друг с другом. При этом постоянное поддержание связей внутри группы может свидетельствовать о ее устойчивости, сплоченности и наличии общих целей.

Как следует из представленного аналитического отчета, связи между членами группы могут иметь не только устойчивый характер, но и обладать определенной иерархичностью, что в случаях использования вышеуказанного преступного способа крупными компаниями позволяет говорить о наличии преступного сообщества (преступной организации), то есть совершении преступления, предусмотренного ст. 210 УК РФ (организация преступного сообщества (преступной организации) или участие в нем (ней)). Такое преступное сообщество будет обладать более сложной многоступенчатой внутренней структурой (иерархией), позволяющей совершать тяжкие и особо тяжкие преступления, такие, как мошенничество, совершенное

организованной группой либо в особо крупном размере с последующей легализацией полученных от преступной деятельности денежных средств, то есть прямым получением финансовой выгоды путем совершения одного или нескольких тяжких либо особо тяжких преступлений.

При этом, в зависимости от конкретной ситуации на рынке криптовалют, существует возможность объединения двух или более организованных групп с аналогичной целью.

Необходимо отметить то обстоятельство, что лица, обладающие специальными знаниями, привлекаются также и к осуществлению таких преступлений, как незаконный сбыт наркотических средств, совершаемый с использованием криптовалюты. Роли в таких группах, как правило, также четко распределены.

Так, например, приговором Октябрьского районного суда г. Кирова лицо было признан виновным в совершении преступлений, предусмотренных ч. 3 ст. 229^1, ч. 2 ст. 228, п. «а» ч. 4 ст. 228^1, ч. 3 ст. 30 п. «а, г» ч. 4 ст. 228^1, ч. 1 ст. 174^1 УК РФ. Действуя в составе группы, организованной из корыстных побуждений, совершил незаконный сбыт наркотических средств с использованием сети Интернет группой лиц по предварительному сговору, а также совершил покушение на незаконный сбыт наркотических средств с использованием сети Интернет группой лиц по предварительному сговору в крупном размере. Кроме этого, в составе той же группы он совершал финансовые операции и другие сделки с денежными средствами или иным имуществом, приобретенными лицом в результате совершения им преступления в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом, совершенное группой лиц по предварительному сговору[142].

---

[142] См.: Приговор Октябрьского районного суда г. Кирова по уголовному делу № 1-44/2020 от 13 февраля 2020 г. [Электронный ресурс] / Октябрьский районный суд г. Кирова. Режим доступа: https://oktyabrsky--kir.sudrf.ru (дата обращения – 26.02.2023).

Второе условие совершения преступлений с использованием криптовалюты — это наличие у лица специального компьютерного оборудования, позволяющего использовать его мощности для совершения действий в виртуальном пространстве, направленных на совершение мошенничества, в том числе способами, получившими названия «Атака», «Атака-51», «Атака Финни», «Эгоистичный майнинг», «Атака Сибиллы», а также других преступлений в виртуальной среде, таких, как вымогательство, или преступления, предусмотренные главой 28 УК РФ (преступления в сфере компьютерной информации).

Для совершения преступлений в виртуальном пространстве необходимо наличие специального оборудования, предоставляющего лицу соответствующие способу совершения мошенничества мощности. Естественно, что при отсутствии такого оборудования и специальных знаний лицо не в состоянии реализовать ни один из вышеперечисленных способов совершения виртуального мошенничества с криптовалютой. Для этого ему необходимо объединить свои усилия с лицом (лицами), не только имеющими специальные знания в области функционирования блокчейн-сетей, но и располагающими соответствующим оборудованием. Сам же он при этом выполняет роль организатора преступления, распределяя роли остальных участников такой группы, то есть имеет место создание организованной преступной группы с распределением ролей.

Более сложной для квалификации представляется ситуация, при которой для совершения виртуального мошенничества с использованием криптовалюты используется «пул», то есть объединение нескольких мощностей для решения определенных задач, как правило майнинга. Между тем «пул» вполне может быть использован для совершения виртуального мошенничества. Можно полностью согласиться с общепринятым мнением о том, что «модель классического компьютерного преступления – это хищение денежных средств или криптовалюты из электронных кошельков пользователей, посредством модификации компьютерной информации, и

квалифицироваться такие деяния должны по ст. ст. 272 и (или) 273 УК РФ либо в совокупности с нормами о мошенничестве».

Как правило, «пул», то есть собрание участников, предоставивших свои мощности, назначает координатора, который отвечает за организацию «пула» и осуществление им деятельности. При этом координатор может иметь возможность использовать «пул» и для других, в том числе преступных целей. Наличие таких «пулов» в блокчейн-сетях наиболее популярных криптовалют — явление широко распространенное. Распределение «пулов» в сети криптовалюты биткоин представлено в Приложении № 5 (см.: рис. 5). Как следует из диаграммы, на четыре крупнейшие площадки — F2Pool, Poolin, AntPool и BTC.com — приходится 60,1 % вычислительных мощностей всей сети. Это свидетельствует о том, что наличие «пулов» в сети биткойн — явление достаточно распространенное.

Такие «пулы» можно использовать в том числе и для совершения мошенничества. Каждый такой «пул», по сути, представляет собой группу людей, объединенных общими интересами и преследующих общую цель — генерацию криптовалюты. Если же помимо «майнинга» администратор соответствующего «пула» по согласованию с другими участниками принимает решения использовать находящиеся в его распоряжении вычислительные мощности группы лиц для совершения мошенничества в виртуальной среде и совершает или пытается совершить его, возникает вопрос о квалификации указанных действий всей группы участников такого «пула». С одной стороны, участник такого «пула» контролирует свою часть мощностей, представленных в общем «пуле», и должен понимать, для какой цели используются его мощности и пул в целом и за счет чего он получает денежное вознаграждение. С другой стороны, полный контроль над «пулом» возможен только лишь при наличии соответствующих специальных знаний, которыми лицо, участвующее в «пуле», может не обладать, вследствие чего не может должным образом оценить эффективность и цели использования такого «пула», в котором он является непосредственным участником. В таком случае

было бы уместно расценивать данную деятельность участника «пула» при наличии соответствующего умысла, как прикосновенность к преступлению, так как он фактически не содействует совершению преступления, по причине использования представленных им мощностей в преступных целях без его фактического согласия.

Под термином «прикосновенность к преступлению» понимают такую деятельность, которая непосредственно связана с преступлением, но при этом не считается соучастием, так как не содействует совершению данного преступления и не находится в причинной с ним связи.

Действующее уголовное законодательство предусматривает ответственность за прикосновенность к преступлению в виде несообщения о преступлении (статья 205^6 УК РФ). При этом диспозиция данной статьи предусматривает перечень конкретных преступлений, за несообщение о которых наступает уголовная ответственность. К таким преступлениям относятся преступления террористической направленности, предусмотренные статьями 205, 205^1, 205^2, 205^3, 205^4, 205^5, 206, 208, 211, 220, 221, 277, 278, 279, 360, 361 УК РФ. Кроме того, ст. 316 УК РФ предусматривает ответственность за укрывательство тяжких и особо тяжких преступлений.

Конечно, необходимо отметить тот факт, что криптовалюта используется в том числе и для финансирования терроризма, экстремистской деятельности, организованной преступной группы, незаконного вооруженного формирования, преступного сообщества. Данное обстоятельство связано с определенной анонимностью криптовалютных транзакций, то есть сложностью определения личности первоначального плательщика.

Вопрос квалификации соучастия в таких преступлениях стоит особенно остро[143]. Необходимо устанавливать, охватывалось ли умыслом лица,

[143] См.: Родыгин Р. А., Орлов Б. А. К вопросу об особенностях совершения преступлений в сфере незаконного оборота наркотиков с использованием сети Интернет // Право: ретроспектива и перспектива. 2022. № 4(12). С. 65–72.

осуществившего соответствующую транзакцию, совершение общественно опасного деяния, запрещенного УК РФ под угрозой наказания, то есть преступления, либо лицо, в силу своей технологической осведомленности, оказывало услуги по приобретению криптовалюты и перечислению ее соответствующему получателю, не зная при этом истинных целей данных операций.

Но если одно из перечисленных в статье 205^6 УК РФ преступлений и было совершено координатором «пула», другие его участники никоим образом не могли ему содействовать или воспрепятствовать, то есть не имели возможности его предотвратить, так как координатор «пула» самостоятельно распоряжается предоставленными ему мощностями. Следовательно, говорить в данном случае о соучастии в таких преступлениях, равно как и о прикосновенности к ним, не представляется возможным.

Как справедливо полагают В.А. Очередько, Н.К. Кустова и др., в качестве криминологической, то есть непосредственно не поставленной под уголовный запрет формы прикосновенности к преступлению можно рассматривать непредотвращение преступления, к которому можно отнести как попустительство, так и укрывательство[144].

Приведенные в настоящем диссертационном исследовании примеры преступлений, совершенных с использованием криптовалюты, позволяют говорить о том, что возникают определенные сложности при решении вопросов, относящихся к институту соучастия в таких преступлениях.

В ряде случаев при квалификации преступлений с использованием криптовалюты не всегда правильно определяется функциональная роль, которую выполняют лица при совместном совершении таких преступлений.

---

[144] Кустова Н.К. Прикосновенность к преступлению и ее соотношение с соучастием в преступлении и иными формами совместной преступной деятельности // Социально-экономические и гуманитарные науки: сборник избранных статей по материалам Международной научной конференции (Санкт-Петербург, 28 октября 2021 г.). СПб., 2021. С. 90–92.

Так, например, использование вредоносных программ, которые позволяют осуществлять копирование данных клиентов криптобирж с последующим выдвижением требований о передаче имущества (криптомонет) под угрозой блокирования криптокошельков, квалифицируются по ст. 273 УК РФ. Однако при такой квалификации не учитывается, что целью лица, такие действия совершающего, является совершение более тяжкого преступления, предусмотренного ст. 163 УК РФ, то есть вымогательство криптовалюты. Такое вымогательство осуществляется под угрозой невозможности пользоваться своим имуществом (криптовалютой), так как невозможность доступа к криптокошельку автоматически лишает собственника доступа и к принадлежащим ему криптомонетам.

Тем не менее, правоприменитель подобные деяния не квалифицирует по ст. 163 УК РФ, поскольку угроза уничтожения компьютерных программ или компьютерной информации не является признаком состава данного преступления[145], а сама принадлежащая потерпевшему криптовалюта уничтожена быть не может в силу технологических особенностей ее функционирования. Однако если на ряду с вышеуказанными действиями в адрес потерпевшего поступали угрозы применения к нему насилия, то действия всех участников такой группы необходимо квалифицировать по совокупности преступлений, предусмотренных ст. ст. 163, 273 УК РФ, вне зависимости от того, от кого конкретно из членов преступной группы такие угрозы исходили.

Соответственно, речь идет о множественности преступлений, совершаемых группой лиц ради достижения ранее обусловленной преступной цели. В зависимости от роли каждого члена такой группы в совершении указанных преступлений должен быть определен его вид соучастия.

---

[145] См.: Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалют [Электронный ресурс] Режим доступа: https://epp.genproc.gov.ru/web/proc_11/sections?section=25924455 (дата обращения – 21.04.2023).

От соучастия в деятельности таких преступных групп необходимо отличать эксцесс исполнителя, которым признается совершение исполнителем преступления, не предусмотренное умыслом других соучастников. В соответствии со ст. 36 УК РФ за эксцесс исполнителя, то есть совершение применительно к рассматриваемой группе лиц преступления, которое не охватывалось умыслом других участником группы, остальные соучастники преступления уголовной ответственности не подлежат.

При эксцессе исполнитель может выйти за рамки согласованного преступного посягательства, совершив однородное с задуманным преступление. Так, например, после завладения паролем от криптокошелька один из участников группы по собственной инициативе с целью сокрытия совершенного преступления, осуществляет убийство потерпевшего, о чем остальные члены группы не были осведомлены заранее и их умыслом совершение данного преступления не охватывалось.

При квалификации таких действий соучастника, которые включают в себя признаки подстрекателя и организатора, необходимо иметь в виду, что основное отличие организатора от подстрекателя заключается в том, что последний не планирует совершение преступления и не руководит подготовкой преступления или его совершением. Подстрекатель в совершении преступлений, может подать идею завладения чужими криптомонетами с целью последующего материального обогащения, но при этом не заниматься разработкой плана совершения преступления, оставляя себе роль «технического консультанта» или же непосредственно соучаствуя в выполнении объективной стороны в виртуальной среде. В последнем случае такой соучастник будет рассматриваться как соисполнитель. В случае когда лицо не только склонило другое лицо к совершению преступления, но впоследствии выполнило и организационные действия, такие действия соучастника следует оценивать только как организационные, поскольку по своей сути они являются более опасными, чем подстрекательские.

Организация преступления включает в себя действия, направленные на склонение другого лица к совершению преступления, приискание и подготовку исполнителя, в данном случае обладающего соответствующими специальным знаниями относительно принципов работы блокчейн-сетей и навыками работы с криптовалютой, а также составление плана совершения преступления, приискание орудий и средств совершения преступления.

В частности, следует помнить, что соучастие в преступлении с субъективной стороны характеризуется умышленной виной соучастников. Данная форма психической деятельности соучастников проявляется в их отношении ко всем признакам состава преступления, в том числе и квалифицирующим.

Квалифицирующие признаки состава преступления могут вменяться соучастникам только при условии установления у них умысла в отношении этих признаков.

Так, например, совершение насильственных действий, образующих объективную сторону соответствующих преступлений и направленных на противоправное получение от собственника (владельца) криптокошелька соответствующего пароля, не могут вменяться лицу, не участвующему в их совершении совместно с другими лицами членами преступной группы.

Так, Петроградским районным судом г. Санкт-Петербурга рассмотрено уголовное дело в отношении N, совершившего преступления, предусмотренные п. «б», ч. 2 ст. 163 УК РФ, ч. 2 ст. 325 УК РФ, при следующих обстоятельствах. Он, обладая информацией о том, что потерпевший осуществляет операции с криптовалютой, путем обмана похитил у него криптовалюту на сумму не менее 1 000 000 рублей, которой в последующем распорядился по своему усмотрению, осуществив обмен криптовалюты на наличные деньги. Для достижения своих целей злоумышленник дважды встречался с потерпевшим, представляясь ему сотрудником ФСБ России, сообщал ложную информацию о якобы грозящей потерпевшему уголовной ответственности за его деятельность с криптовалютой, а также о возможности

избежать уголовной ответственности, если потерпевший переведет на его криптокошелек криптовалюту в указанном им количестве. На последней встрече с потерпевшим виновное лицо, поняв, что потерпевший ему не верит и у него не получится мошенническим путем завладеть желаемым имуществом, решил завладеть данным имуществом путем совершения иного преступления – вымогательства, и начал реализовывать свой преступный умысел совместно с иным лицом. Под видом сотрудников ФСБ указанные лица, применяя к потерпевшему физическое насилие, не опасное для жизни, и угрожая введением в его организм химических веществ психотропного действия, потребовали от последнего перевести принадлежащую ему криптовалюту на указанные ему криптокошельки, что и было им выполнено[146].

В преступлениях, совершаемых с применением насилия, криптовалюта может выступать как в качестве фактического средства платежа при совершении таких преступлений по найму, так и являться непосредственно предметом преступного посягательства, например при разбое с целью завладения криптомонетами потерпевшего. Можно согласиться с разъяснениями, данными в постановлении Пленума Верховного Суда Российской Федерации от 17 декабря 2015 года № 56 «О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации)» относительно того, что при разрешении вопроса об отграничении грабежа и разбоя от вымогательства, соединенного с насилием, необходимо учитывать, что при грабеже и разбое насилие является средством завладения криптовалютой либо ее удержания, тогда как при вымогательстве оно подкрепляет угрозу. Завладение криптомонетами при грабеже и разбое происходит сразу после их совершения, а при вымогательстве умысел виновного направлен на получение требуемых криптомонет в будущем. В том

[146] См.: Приговор Петроградского районного суда г. Санкт-Петербурга по уголовному делу № 1–95/2020 от 30 июня 2020 г. [Электронный ресурс] / Петроградский районный суд г. Санкт-Петербурга. Режим доступа: http://pgr.spb.sudrf.ru (дата обращения – 16.02.2023).

случае, когда вымогательство сопряжено с непосредственным изъятием криптомонет потерпевшего, при наличии реальной совокупности преступлений, эти действия в зависимости от характера примененного насилия должны дополнительно квалифицироваться как грабеж или разбой.

Криптовалюта – явление наднациональное, а ее оборот осуществляется вне зависимости от территориальной юрисдикции государств. С экономической точки зрения криптовалюта представляет собой некий финансовый актив, имеющий котировочную стоимость, то есть представляющий определенную ценность, и в качестве такового рассматривается большинством стран мира. Исходя из требований ст. 11 УК РФ (действие уголовного закона в отношении лиц, совершивших преступление на территории Российской Федерации), предусматривающей, что лицо, которое совершило преступление на территории Российской Федерации, подлежит уголовной ответственности по УК РФ, и все требования уголовного закона подлежат применению к виновному лицу, совершившему преступления в блокчейн-сетях с использованием криптовалюты, но физически при этом находящегося на территории России. Вышеизложенное относится к преступлениям с формальным составом. В материальных составах местом преступления является место наступления общественно опасных последствий, так как само действие, как правило, не наказуемо. При наступлении последствий на территории иностранного государства юрисдикция Российской Федерации, как правило, не распространяется на такие преступления, то есть они не направлены против интересов Российской Федерации или гражданина Российской Федерации.

Таким образом, соучастники, совершая преступления с использованием криптовалюты в соответствующих блокчейн-сетях, физически могут находиться в различных местах, но при этом, используя компьютерные устройства, действовать согласованно, преследуя при этом единую цель и действуя согласно ранее достигнутой договоренности.

Следует особо отметить, в качестве соучастников не могут рассматриваться лица, не осведомленные о преступном происхождении криптовалюты либо денежных средств, которые были получены от реализации криптовалюты, для совершения преступлений, предусмотренных ст. ст. 174, 174[1], 175 УК РФ. Их исполнителями должны признаваться лица, которые фактически контролировали соответствующие криптовалютные транзакции, финансовые операции, сделки и руководили действиями вышеуказанных лиц.

Не могут признаваться соучастниками лица, осуществлявшие криптовалютные транзакции с криптовалютой, полученной ранее в результате совершения преступления иными лицами, по поручению которых они действуют, но при этом не осведомленных о цели совершаемых ими по поручению транзакциях.

Необходимо отличать понятие легализации от приобретения или сбыта криптовалюты, заведомо добытой преступным путем. Легализация – это придание правомерности владению имуществом, полученным от совершения преступлений. Сами по себе покупка или продажа криптовалюты легализацией не являются, но могут образовывать состав преступления, предусмотренного ст. 175 УК.

При совместной легализации криптовалюты, денежных средств, полученных от ее реализации, либо иного имущества, приобретенных в результате совершения преступления, участвующее в совершении такой сделки лицо, которое до этого непосредственно приобрело указанное имущество в результате совершения им преступления, должно нести ответственность по ст. 174[1] УК РФ, а лицо, которое данное имущество в результате совершения основного преступления не приобретало, – по ст. 174 УК РФ.

В организованную группу, предусмотренную п. «а» ч. 4 ст. 174[1] УК РФ, могут входить лица, не обладающие признаками специального субъекта преступления, предусмотренного статьей 174[1] УК РФ. В случае признания совершения названного преступления организованной группой действия всех

ее членов, принимавших участие в подготовке и совершении этого преступления, независимо от того, выполняли ли они функции исполнителя, организатора, подстрекателя или пособника, подлежат квалификации по п. «а» ч. 4 ст. 174^1 УК РФ без ссылки на ст. 33 УК РФ.

Приобретение или сбыт криптовалюты, равно как и иного имущества, заведомо добытого преступным путем, могут быть признаны соучастием в преступлении в том случае, если эти действия были обещаны исполнителю такого преступления до или во время его совершения либо по иным причинам (например, в силу систематического их совершения) давали основание исполнителю преступления рассчитывать на подобное содействие.

В отличие от группы лиц, заранее договорившихся о совместном совершении преступления, в организованную группу по смыслу ч. 3 ст. 35 УК РФ могут входить также лица, не обладающие признаками специального субъекта, предусмотренными ч. 5, 6 либо 7 ст. 159, ст. 159^1 или ст. 160 УК РФ, которые заранее объединились для совершения одного или нескольких преступлений.

Таким образом, в случае признания мошенничества с использованием криптовалюты, присвоения или растраты денежных средств, полученных от реализации криптовалюты, которые совершены организованной группой, действия всех ее членов, принимавших участие в подготовке или в совершении преступления, независимо от их фактической роли в совершении указанных преступлений следует квалифицировать по соответствующей части ст. ст. 159, 159^1, 159^2, 159^3, 159^5, 159^6, 160 УК РФ без ссылки на ст. 33 УК РФ. Данный вывод обосновывается следующим.

Совершение мошенничества либо растраты с использованием криптовалюты, как правило, невозможно либо крайне затруднительно без участия лиц, обладающих специальными знаниями в области функционирования блокчейн-сетей и навыками работы с криптовалютой. Навыки работы с криптовалютой подразумевают не просто возможность использования криптокошелька и осуществление соответствующих

транзакций, но наличие знаний относительно максимально возможной анонимизации произведенных транзакций в блокчейн-сети (использование соответствующих P2P-платформ, криптомиксеров и т.п. средств анонимизации). Указанные члены преступной группы формально осуществляют только «техническую поддержку», работая в виртуальном пространстве, но фактически выполняя часть объективной стороны преступления, так как их умысел, равно как и других членов преступной группы, направлен на конечный преступный результат.

Разрешая вопрос о квалификации действий лиц, совершивших мошенничество, присвоение или растрату в составе группы лиц по предварительному сговору либо организованной группы по признаку «причинение значительного ущерба гражданину» или по признаку «в крупном размере» либо «в особо крупном размере», необходимо исходить из общей стоимости криптовалюты, а также иного имущества, похищенного всеми участниками такой преступной группы.

В тех случаях, когда криптовалюта используется в целях создания или функционирования экстремистского сообщества, при совершении участником такого экстремистского сообщества конкретного преступления его действия должны квалифицироваться по совокупности преступлений, предусмотренных ч. 2 ст. 282^1 УК РФ и соответствующей частью (пунктом) с учетом квалифицирующего признака «организованная группа». Если состав совершенного лицом преступления не предусматривает в качестве квалифицирующего признака совершение его организованной группой, то действия лица подлежат квалификации только по ч. 2 ст. 282^1 УК РФ и соответствующей части (пункту) статьи УК РФ, которая предусматривает квалифицирующий признак «группой лиц по предварительному сговору», а при его отсутствии – по признаку «группой лиц». Использование криптовалюты в данном случае позволяет максимально скрытно осуществлять финансирование экстремистского сообщества, также, как и том случае, когда состав совершенного лицом преступления с использованием криптовалюты не

предусматривает в качестве квалифицирующего признака совершение его организованной группой, группой лиц по предварительному сговору или группой лиц. По общему правилу действия лица необходимо квалифицировать по ч. 2 ст. 282^1 УК РФ и соответствующей статье УК РФ. При этом совершение участниками экстремистского сообщества конкретного преступления в составе организованной группы в соответствии с пунктом «в» ч. 1 ст. 63 УК РФ признается в качестве обстоятельства, отягчающего наказание.

В отношении лиц, признанных виновными в совершении преступлений, предусмотренных ст. ст. 282^1, 282^2 и 282^3 УК РФ, в соответствии с пунктами «а», «б», «в» ч. 1 ст. 104^1 УК РФ необходимо также разрешение вопроса относительно конфискации как непосредственно криптовалюты, так и денежных средств, которые были получены в результате совершения преступлений с использованием криптовалюты, а также и любых доходов от их использования, предназначенных для финансирования терроризма, экстремистской деятельности, организованной группы, незаконного вооруженного формирования, преступного сообщества (преступной организации).

Необходимо отметить, что в целях конфискации криптовалюты, полученной в результате совершения преступлений, необходимо наложение ареста на криптовалютные кошельки, что в настоящее время является достаточно проблематичным, но необходимым условием последующей конфискации.

Имеется два возможных варианта, каждый из которых может быть использован по усмотрению следователя, исходя из фактических обстоятельств конкретного уголовного дела.

Первый вариант представляет собой возможность перевода криптомонет из криптокошелька обвиняемого на специально открытый для этих целей под контролем следователя криптокошелек для хранения арестованного имущества в виде криптовалюты. Конечно, при этом возникает вопрос, кто конкретно должен совершать такие действия. Может ли следователь либо иное

должностное лицо открывать и контролировать данный криптокошелек, то есть быть ответственным за хранение криптомонет. Данный вопрос не урегулирован. Тем не менее, учитывая отсутствие запретов на совершение указанных действий, при том что криптомонеты признаются вещественным доказательством, открывать такой криптокошелек и быть ответственным за хранение арестованного имущества вполне может быть следователь. В данном случае необходимо исходить из требований ст. 82 УПК РФ, предусматривающей, что вещественные доказательства должны храниться при уголовном деле до вступления приговора в законную силу либо до истечения срока обжалования постановления или определения о прекращении уголовного дела и передаваться вместе с уголовным делом.

В случае использования аппаратного криптокошелька такой кошелек в обязательном порядке изымается и хранится с уголовным делом в качестве вещественного доказательства, в определенных случаях подтверждающего связь его владельца с другими участниками преступной группы, а также способствовать выявлению других участников такой группы.

По смыслу ст. 35 УК РФ, организованная группа будет характеризоваться устойчивостью и организованностью, что в свою очередь предполагает распределение ролей, наличие организатора и (или) руководителя такой группы. Именно к такой организованной группе можно отнести так называемый «пул», когда несколько участников не только предоставляют свои компьютерные мощности для совершения заранее разработанных руководителем такой группы преступлений, но и роль каждого из членов такой организованной группы четко определена. Такой «пул» не может функционировать без согласованности действий всех его участников и координации их действий одним руководителем.

Преступление признается совершенным организованной группой, если оно совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Организованной группой могут быть совершены и так называемые коррупционные преступления, в тех случаях, когда дача, получение взятки, коммерческий подкуп осуществляются с использованием криптовалюты. В таком случае, признавая получение взятки либо предмета коммерческого подкупа организованной группой, действия всех ее членов, принимавших участие в подготовке и совершении этих преступлений, независимо от того, выполняли ли они функции исполнителя, организатора, подстрекателя или пособника, подлежат квалификации по соответствующей части ст. 290 либо ст. 204 УК РФ без ссылки на ст. 33 УК РФ. Преступление признается оконченным с момента принятия незаконного вознаграждения, в данном случае криптомонет, любым членом организованной группы. В данном случае криптовалюта также используется в целях достижения максимальной анонимности лиц, совершающих указанные преступления.

Разрешая вопрос о квалификации получения взятки либо предмета коммерческого подкупа в составе группы лиц по предварительному сговору или организованной группы, следует исходить из общей стоимости конкретного вида криптовалюты, предназначавшейся всем участникам преступной группы. Стоимостные критерии криптомонет, полученных в виде взятки или коммерческого подкупа должны быть определены исходя из их биржевой стоимости на момент передачи каждому из членов группы.

Таким образом, большая часть преступлений с использованием криптовалюты совершается в соучастии, так как требует наличия определенных знаний и навыков работы с блокчейн-сетями, при этом необходима не только общая координация действий всех членов преступной группы, объединенных единым умыслом, но и предварительное распределение ролей между всеми членами такой группы в зависимости от их навыков и компетенций.

Деятельность всех участников организованной преступной группы определяется едиными правилами, включающими требования соблюдения конспирации. Для целей конспирации участники осуществляют все контакты

между собой посредством телекоммуникационной сети Интернет, например, используя шифрованную программу мгновенного обмена сообщениями «Телеграмм» либо используя временную электронную почту и даркнет-сети. Также могут быть использованы вымышленные имена (ники). Соучастники при этом могут быть лично друг с другом не знакомы.

В качестве примера действий организованной преступной группы можно привести незаконную реализацию наркотических средств с использованием криптовалюты[147].

Реализация наркотических средств на всех стадиях осуществляется на основе постоянной, однотипной и выработанной схемы: бесконтактным способом, путем размещения в тайниках, о месте нахождения которых сообщается через сеть Интернет. Расчеты за проданные наркотики и иные финансовые операции осуществляются с использованием криптовалюты[148]. Между членами организованной преступной группы существует субординация, предусмотрена система штрафов и иных наказаний за невыполнение или некачественное выполнение заданий, существует возможность, если так можно сказать, карьерного роста. Вербовка и привлечение новых членов организованной преступной группы, а также реклама «магазина» осуществляются посредством дачи объявлений в социальных сетях и на других интернет-ресурсах, ориентированных на потребителей наркотических средств, а также на лиц, желающих иметь стабильный высокий доход при минимальных рисках задержания правоохранительными органами, ввиду вышеуказанных конспиративных мер[149]. Организованная преступная группа отличается сложной

---

[147] См.: Ализаде В.А., Волеводз А.Г. Судебная практика применения ст. 174[1] УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты // Наркоконтроль. 2017. № 4. С. 8–14.

[148] См.: Дворянкин О.А., Клочкова Е.Н. Криптовалюта – новый инструмент наркобизнеса // Наркоконтроль. 2018. № 4. С. 19–22.

[149] См.: Яшин А.В., Шикшеев В.Р. Проблемы противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемым посредством сети интернет // Вестник Пензенского государственного университета. 2020. № 3(31). С. 108.

организационно-иерархической структурой, характеризуется организованностью, масштабностью, длительностью периода преступной деятельности, отработанной системой совершения преступлений, сплоченностью и устойчивостью состава соучастников на основе единого преступного умысла, направленного на сбыт наркотических средств, и четким распределением ролей между ними.

Схемы распределения ролей в такой организованной преступной группе на примере торговых площадок по незаконной торговле наркотическими средствами и сильнодействующими веществами, расчеты за которые осуществляются в криптовалюте, может быть следующей:

- «руководитель» – непосредственный организатор «интернет-магазина», осуществляющий общее руководство организованной преступной группой, определяющий общие цели, способы совершения и сокрытия преступлений. Руководитель определяет меры конспирации, роли и состав участников, меры безопасности и конспирации, распределяет доходы и организовывает материально-техническое, финансово-хозяйственное обеспечение организованной преступной группы, принимает «кадровые решения» и обеспечивает оплату денежного вознаграждения участникам, а также иные платежи, связанные с организационными расходами. Организует доставку партий наркотиков, обмен поступающей в качестве оплаты криптовалюты на фиатные деньги;

- «куратор» получает от руководителя организованной преступной группы сведения о месте нахождения оптовой партии наркотических средств и осуществляет обмен информацией между членами организованной преступной группы о количестве наркотиков, подлежащих сбыту, их фасовке и месте нахождения тайников. Также лично или при помощи автоматизированных программ передает покупателям информацию о виде и стоимости наркотиков, получает оплату в криптовалюте за реализованные наркотические средства и сообщает местонахождении тайников, принимает «кадровые» решения;

- «перевозчик» по указанию руководителя организованной преступной группы обеспечивает поставку наркотических средств в особо крупных размерах, обеспечивая бесперебойную деятельности такой группы;

- «склад-фасовщик» получает, хранит, фасует, доставляет и размещает в тайниках оптовые партии наркотических средств для сбыта «мини-складом» или «закладчиками (курьерами)»;

- «мини-склад» получает, хранит, фасует, доставляет и размещает в тайниках мини-оптовые партии наркотических средств для сбыта «закладчиками (курьерами)»;

- «закладчик» или «курьер», координируя свои действия с «оператором» и «куратором», получает от «склада» или «мини-склада» оптовые партии наркотиков и осуществляет их непосредственный сбыт потребителям путем оборудования тайников с разовыми дозами наркотика;

- «отдел кадров» рассылает рекламу «магазина», отбирает для работы новых лиц[150].

«Прием на работу» осуществляется после предоставления копий документов, удостоверяющих личность либо внесения денежного залога в сумме от 5000 до 15000 рублей (в зависимости от количества наркотиков, получаемых для реализации на первоначальном этапе), выступающими гарантами возможных убытков вследствие утраты членом организованной преступной группы партии наркотических средств, подлежащих сбыту[151]. Действия членов организованной преступной группы взаимосвязаны и дополняют друг друга, преследуя единую цель.

Потребители наркотических средств в чате мессенджера, используемом «интернет-магазином», при непосредственном участии «оператора»,

---

[150] См.: Детков А.А., Стародубцева М.А. Бесконтактный сбыт наркотических средств посредством сети Интернет: криминогенная обстановка в Алтайском крае // Уголовно-исполнительное право. 2021. Т. 16. № 4. С. 512–521.

[151] См.: Приговор Якутского городского суда Республики Саха (Якутия) по уголовному делу № 1-577/2020 от 27 апреля 2020 г. [Электронный ресурс] / Якутский городской суд Республики Саха (Якутия). Режим доступа: http://jakutsky.jak.sudrf.ru (дата обращения – 16.02.2023).

используя автоматизированные программы продажи, согласно представленному прайс-листу, выбирают вид, объем и стоимость наркотических средств для покупки, получают реквизиты для осуществления расчетов и сведения о месте нахождения тайника с приобретенным наркотиком, при условии оплаты криптовалютой[152].

Таким образом, можно констатировать тот факт, что часть преступлений с использованием криптовалюты совершается организованной группой или преступным сообществом. Типичным примером такого преступного сообщества является так называемый магазин Hydra, существующий в сети Даркнет до настоящего времени[153]. Структурные подразделения Hydra имеются практический на всей территории Российской Федерации и состоят из двух или более лиц, включая руководителя, в рамках и в соответствии с общими целями преступного сообщества (преступной организации) осуществляют преступную деятельность по незаконной реализации наркотических средств и их прекурсоров. Такого рода структурные подразделения, объединенные общими целями и решением общих задач преступного сообщества (преступной организации), могут не только совершать отдельные преступления, но и выполняют иные задачи, направленные на обеспечение функционирования преступного сообщества (преступной организации): осуществляют легализацию полученной в результате преступной деятельности криптовалюты, ее обмен на фиатные деньги и придания им видимости законности, вовлечение в преступную деятельность иных лиц[154]. В свою очередь к организованной группе можно отнести группу лиц, заранее объединившихся для совершения одного или

---

[152] См.: Приговор Якутского городского суда Республики Саха (Якутия) по уголовному делу № 1-577/2020 от 27 апреля 2020 г. [Электронный ресурс] / Якутский городской суд Республики Саха (Якутия). Режим доступа: http://jakutsky.jak.sudrf.ru (дата обращения – 16.02.2023).

[153] См. об этом: Интервью со специалистом в области национальной и международной безопасности, ведущим аналитиком АНО «Ассоциация специалистов по информационным операциям» Константином Стригуновым // Юрист спешит на помощь. 2021. № 3. С. 9–18.

[154] См.: Дворянкин О.А. Даркнет – темная сторона Интернета или неужели так все плохо? // Национальная ассоциация ученых. 2021. № 71–1. С. 19.

нескольких тяжких либо особо тяжких преступлений, в том числе более мелкие, по сравнению с той же Hydra, «интернет-магазины» (торговые площадки), осуществляющие незаконную реализацию наркотиков, действующие в определенном населенном пункте Российской Федерации и не имеющие структурных подразделений в других регионах, в том числе и для выполнения иных задач, направленных на обеспечение функционирования преступной деятельности такой группы.

Вышеизложенное доказывает необходимость включения в УК РФ специальных норм, которые предусматривали бы ответственность за незаконное использование криптовалюты, в том числе посредством создания и обеспечения работы сетевых платформ (торговых площадок) для осуществления преступной деятельности с использованием криптовалюты.

§ 2.3. Основные направления совершенствования законодательства об уголовной ответственности за преступления, совершаемые с использованием криптовалюты

Необходимо отметить, что преступления с использованием криптовалюты можно отнести к преступлениям, совершаемым в условиях неочевидности, что само по себе является фактором, повышающим их латентность.

Изучив принципы функционирования криптовалют, определив основные виды преступлений, совершаемых с использованием криптовалюты, выявив их основные причины и условия, можно сформировать систему мер противодействия таким преступлениям в Российской Федерации, направленных на:

1) выявление и устранение причин, порождающих преступления с использованием криптовалюты;

2) выявление и устранение условий совершения преступлений с использованием криптовалюты.

С использованием криптовалюты совершаются различные преступления, в которых криптовалюта не всегда является самоцелью, вследствие чего речь должна идти о совершенствовании правового механизма оборота криптовалюты, который бы исключал ее криминальное использование или значительно снижал бы привлекательность криптовалют для преступников.

В качестве причин, порождающих использование криптовалюты для совершения преступлений, можно назвать в первую очередь возможность получения незаконного дохода при минимальной возможности привлечения к уголовной ответственности за совершенное преступление.

В свою очередь активное использование криптовалюты в преступных целях – торговля наркотиками, легализация доходов, полученных от преступной деятельности, финансирование терроризма – создают

благоприятные условия для совершения таких преступлений, как вымогательство и взяточничество, что уже является вызовом не только для национальной, но и для глобальной системы противодействия отмыванию денежных средств и финансированию терроризма (ПОД/ФТ), так как обеспечить необходимую прозрачность обращения криптовалют, позволяющую осуществлять контроль за их оборотом, невозможно.

В целях устранения причин и условий совершения преступлений с использованием криптовалюты необходим комплекс системных мер, среди которых мерам уголовно-правового воздействия должна быть отведена решающая роль.

Необходимо отметить, что на сегодняшний день в Российской Федерации превалируют два подхода к решению проблемы устранения причин и условий совершения преступлений с использованием криптовалюты. Так, Минфин России подготовил и в феврале 2022 г. внес в Правительство Российской Федерации разработанный по его поручению на основе утвержденной концепции регулирования механизма организации оборота цифровых валют, законопроект[155] о регулировании криптовалют, предполагающий, что запрет на использование любых видов цифровых валют в качестве средства платежа на территории Российской Федерации будет по-прежнему сохранен. Соответственно, любые цифровые валюты, в том числе и криптовалюта, могут рассматриваться только лишь в качестве определенного финансового инструмента для инвестиций.

Представленным законопроектом определяются необходимые требования к биржам и так называемым обменникам (операторам), осуществляющим деятельность, непосредственно связанную с организацией оборота цифровых валют. Для этого будет необходимо создать специальный реестр операторов, который будет вести учет лиц и организаций, связанных с

[155] Минфин России направил в Правительство России проект федерального закона «О цифровой валюте» [Электронный ресурс] // Официальный сайт Минфина России. Режим доступа: https://minfin.gov.ru. (дата обращения – 01.02.2023).

оборотом цифровой валюты. Требования касаются корпоративного управления, составления отчетности, хранения информации, внутреннего контроля и аудита, системы управления рисками и размера собственных средств. Деятельность таких организаций должна быть лицензирована, и за ней должен будет осуществляться контроль определенным Правительством Российской Федерации органом. Иностранные криптовалютные биржи для получения лицензии должны будут получить регистрацию в Российской Федерации.

При всем этом операции с покупкой либо продажей криптовалюты должны быть возможны только при условии проведения идентификации клиента. Оборот криптовалюты от клиента оператору и наоборот должен осуществляться исключительно через банки с обязательным использованием банковского счета. Соответственно, идентификация клиентов будет проводиться как операторами при приеме клиентов на обслуживание, так и банками при открытии соответствующего банковского счета для последующего проведения финансовых операций с использованием криптовалюты. Операторы, как и банки, будут обязаны осуществлять комплексные системные процедуры, направленные на выявление лиц, уклоняющихся от выполнения вышеуказанных требований, и информировать Росфинмониторинг об обнаруженных подозрительных операциях.

В целях защиты прав и интересов инвесторов биржи будут обязаны информировать граждан о высоких рисках, связанных с приобретением криптовалют. Граждане, в свою очередь, должны будут проходить онлайн-тестирование перед приобретением криптовалюты. Такое тестирование определит уровень знаний о специфике вложений в цифровые валюты и осведомленности о возможных рисках. При успешном прохождении тестирования граждане смогут осуществлять вложение своих средств в криптовалюты с ограничением до 600 000 руб. ежегодно. В тех случаях, когда такое тестирование не будет пройдено, предельный размер вложений будет ограничиваться до суммы не более 50 000 руб. Указанные ограничения

должны быть прежде всего направлены именно на обеспечение безопасности граждан, желающих инвестировать свои сбережения в криптовалюту. При всем этом квалифицированные инвесторы, то есть отдельная категория инвесторов, имеющих соответствующие знания, опыт и располагающие финансовыми возможностями, позволяющими им осознанно инвестировать денежные средства в рисковые активы, а также юридические лица должны получить возможность совершать операции с криптовалютой без всяких ограничений.

Биржи будут обязаны отделять в информационной системе цифровую валюту (криптовалюту), принадлежащую им, от цифровой валюты участников торгов. На криптовалюту граждан и юридических лиц не может быть распространенно взыскание по долгам оператора торговой платформы, что, в свою очередь, будет являться дополнительной защитой для лиц, участвующих в биржевой торговле криптовалютой. Для сохранности денежных средств клиентов необходимым условием деятельности криптобирж должно быть введение режима номинального счета, на котором будут находиться денежные средства участников биржевых торгов. Биржи и операторы будут обязаны вести реестры с указанием адресов – идентификаторов каждого обладателя цифровых валют.

В законе должно быть закреплено определение майнинга как определенного вида деятельности, направленной на получение криптовалюты. Также в законопроекте предусмотрен механизм предоставления налоговым органам информации, необходимой для осуществления возложенных на них контрольных и надзорных функций.

Целью вышеуказанных изменений является формирование легального рынка цифровых валют с установлением правил их оборота и круга участников такого оборота. Оценивая подход Минфина России к совершенствованию законодательства, необходимо отметить следующее:

1. Предлагаемые изменения законодательства связаны с введением ряда запретов, но при этом не представлен механизм принуждения к их исполнению и виды ответственности за несоблюдение указанных запретов.

2. Не представлен механизм контроля за соблюдением указанных законодательных нововведений, то есть фактически предложения не содержат механизма и способа их реализации.

3. Представленные предложения носят обобщенный характер, что фактически делает их реализацию если не невозможной, то трудно осуществимой.

В целом характер предложенных Минфином России законодательных мер носит конструктивный характер, но в силу вышеуказанных причин они труднореализуемы, вследствие чего вряд ли могут достичь целей, направленных на создание легального, контролируемого рынка цифровых валют с установлением единого для всех правил их оборота и круга участников криптовалютного рынка.

Другие предложения по совершенствованию законодательства о регулировании рынка оборота криптовалют и об уголовной ответственности за преступления, совершаемые с использованием криптовалюты, разработаны и представлены Банком России и соотносятся с предложениями автора, также полагающего необходимым введение законодательных ограничений оборота криптовалюты на территории Российской Федерации и установление уголовной ответственности за нарушение либо несоблюдение вводимых запретов.

В качестве обоснования указанных предложений можно сослаться на наличие потенциальных рисков распространения криптовалют, которые по мере их распространения могут привести к системным угрозам, к которым прежде всего относят: угрозу для благосостояния граждан Российской Федерации, угрозу для финансовой стабильности государства, угрозу расширения нелегальной деятельности, связанной с непосредственным использованием криптовалют.

Риски использования криптовалют для частных инвесторов, граждан Российской Федерации связаны прежде всего с возможностью полной потери вложенных в криптовалюты денежных средств, без последующей возможности их возврата, так как криптовалютный рынок, как отмечают специалисты ЦБ России, характеризуется очень высокой волатильностью. При этом наблюдается сильная зависимость цен на криптовалюты от информационного фона. Любые заявления публичных или медийных лиц способствуют резким скачкам стоимостного курса криптовалют в течение короткого периода времени.

По мнению экспертов Банка России[156], высокая волатильность обусловлена в том числе и тем, что криптовалюты сконцентрированы в руках небольшого количества владельцев, что в свою очередь создает возможность для проведения умышленных манипуляций на рынке с резкими скачками стоимостного курса криптовалют. Анонимность участников таких манипуляций способствует резкому изменению цены криптовалюты на криптобиржах, так называемых обменниках и P2P-платформах, где традиционные механизмы противодействия манипулированию рынком не могут быть реализованы, а лица, виновные в манипулировании рынком, не несут уголовную ответственность. Такое положение дел порождает не только чувство безнаказанности, но и приводит к систематическому совершению преступлений, что только увеличивает угрозу для финансовой безопасности добросовестных участников криптовалютного рынка.

Учитывая то обстоятельство, что помимо иностранных криптовалютных бирж, в России также распространена покупка различного вида криптовалют через так называемые «криптообменники», осуществляющие анонимные транзакции, необходимо предусмотреть не только обязательное лицензирование деятельности организаций подобного рода, но и уголовную

---

[156] См.: Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 23.

ответственность за уклонение от такого лицензирования. При лицензировании деятельности криптобирж и так называемых обменников криптовалюты необходимо обеспечить обязательность сбора персональных данных клиентов, осуществляющих транзакции с использованием криптовалюты. В настоящее время отсутствие лицензирования и «простота входа»[157], предоставляющие возможности купить или продать криптовалюту за фиатные деньги посредством P2P-переводов с использованием банковских карт, делают такие операции идеальным средством для легализации денежных средств, полученных в результате совершения преступления. Зачастую такие операции осуществляются с использованием электронных кошельков и лицевых счетов абонентов операторов связи, которые, в свою очередь, оформлены на подставных лиц, что делает фактически невозможным как выявление истинных лиц, стоящих за такими транзакциями, так и истинных целей их (транзакций) осуществления.

При этом, согласно результатам проведенного в 2021 году Банком России исследования, криптовалюта в России по частоте совершаемых с ней сделок (12 %) находится на втором месте после акций (29 %)[158]. В августе 2021 года Россия вышла на 3-е место по объему майнинга криптовалюты биткойн. На долю России приходится 11,23 % вычислительных мощностей, используемых для майнинга криптовалюты биткойн. В начале 2021 года доля России в указанном майнинге составляла 6 %[159]. Все вышеизложенное свидетельствует о вовлеченности в криптовалютную экономическую отрасль большого количества физических лиц, граждан Российской Федерации. Некоторыми учеными отмечается начало перехода от традиционных фиатных денег к цифровой валюте[160]. При всем этом нельзя отрицать и наличие высоких

---

[157] См.: Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М., 2022. С. 19.
[158] Там же. С. 9.
[159] Там же. С. 19.
[160] Михайлишин А.Ю. Предпосылки появления и мировой опыт внедрения цифровых валют центральных банков // Актуальные проблемы экономики и права. 2021. Т. 15, № 2. С. 294–307.

рисков потери денежных средств граждан, желающих стать инвесторами криптовалютного рынка. Подобного рода риски связаны не только с высокой волатильностью криптовалют, но и с криминализацией криптовалютного рынка в России, имеющего при этом высокую степень латентности, в том числе в силу анонимизации его участников[161].

Преодоление анонимизации участников криптовалютного рынка возможно либо путем анализа данных соответствующего блокчейна, что само по себе является достаточно трудоемким и далеко не всегда достоверным, либо путем введения уголовно-правовых запретов на осуществление анонимной деятельности при сделках с криптовалютой.

Анализ транзакций в соответствующей блокчейн-сети[162] представляет собой метод построения связей между криптокошельками, в соответствии с произведенными с их помощью транзакциями, с последующим присвоением криптокошелькам на основании полученной информации меток (например, о том, что кошелек использовался в мошеннических схемах или для оплаты запрещенных товаров либо услуг), что позволяет оценивать совершаемые транзакции по уровню риска причастности к совершению преступлений[163]. Такой метод получил название – метод кластеризации. Однако, если при осуществлении криптовалютных транзакций применялся такой инструмент, как «криптовалютный миксер», использование метода кластеризации становится невозможным и анонимность владельцев криптокошельков сохраняется.

Установить реального владельца кошелька возможно лишь в случае, если такой кошелек использовался в сервисах, которые предоставляют услуги только идентифицированным клиентам. Другим источником информации для

---

[161] См.: Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М. 2022. С. 23.

[162] Под анализом транзакций в соответствующей блокчейн-сети понимается процесс исследования, классификации адресов и транзакций в блокчейне для понимания характера деятельности различных участников такой сети.

[163] См.: Банк России. Доклад для общественных консультаций… С. 21.

аналитического исследования могут быть криптобиржи, которые, в зависимости от законодательства конкретной страны, осуществляют предоставление информации о клиентах и ходе торгов при наличии законных оснований у органа государственной власти для ее получения[164]. Таким образом, для получения информации о транзакциях необходимо взаимодействие с иностранными регуляторами финансового рынка, в чью компетенцию входит надзор за деятельностью криптобирж тех стран, где законодательно регулируется оборот криптоактивов, что существенно осложнено в условиях проводимого западными странами санкционного режима в отношении России. Но даже в иных условиях полученная информация также будет носить обобщающий характер, так как не будет включать сведения о так называемых P2P-продажах криптовалюты. Без наличия соответствующих уголовно-правовых запретов на определенные способы осуществления деятельности на криптовалютных рынках, особенно в странах с формирующимися рынками, невозможно осуществлять эффективное противодействие преступлениям в указанной сфере.

Таким образом, существующие потенциальные риски финансовой стабильности, связанные с оборотами криптовалют различного вида, значительно выше для стран с формирующимися рынками, к которым можно отнести и Российскую Федерацию, в частности, из-за традиционно более высокой склонности к валютизации, то есть аккумулированию своих активов в валютах, не являющихся платежным средством Российской Федерации, и недостаточного уровня финансовой грамотности населения. При этом страны с резервными валютами могут пока позволить себе мягкое отношение к криптовалютам, следуя по пути постепенного расширения охвата регулирования и не прибегая при этом к мерам уголовно-правового регулирования криптовалютного рынка.

---

[164] См.: Банк России. Доклад для общественных консультаций... С. 20.

Расширение использования криптовалют будет создавать значительные риски для национального финансового рынка Российской Федерации. При отсутствии ограничений, определяемых, в том числе, и мерами уголовно-правового воздействия, и дальнейшем росте объемов инвестирования в криптовалюты российскими гражданами и организациями, вовлечении в рынок криптовалют банков и иных финансовых организаций, риски, присущие этой деятельности, будут многократно увеличиваться и нести системные угрозы для благосостояния граждан Российской Федерации, финансовой стабильности государства, а также угрозу расширения сферы деятельности, запрещенной в Российской Федерации.

Кроме прочего, Банк России полагает, что криптовалюты способствуют совершению преступлений, так как анонимность владельцев криптокошельков является фактором, способствующим проведению криптовалютных транзакций в рамках преступной деятельности, в частности такой, как легализация денежных средств, полученных преступным путем, торговля наркотическими, сильнодействующими веществами, ядами, финансирование терроризма, вымогательство, дача и получение взяток, а также нелегальный вывод денежных средств за рубеж. Относительно последнего вида деятельности необходимо учитывать, что с помощью различного вида криптовалют не только происходит неконтролируемое со стороны государства перемещение денежных средств за рубеж, но и отсутствует фактическая возможность понять целевое назначение перемещаемых финансов, что само по себе уже создает серьезную проблему сложившейся системе противодействия отмыванию денег и финансированию терроризма (ПОД/ФТ) и обуславливает необходимость создания механизма ее совершенствования. В то же время совершенствование такого правового механизма контроля за использованием криптовалют невозможно без применения комплексного правового механизма, включающего в себя не только меры, направленные на регламентацию деятельности криптовалютного

рынка, но и меры уголовно-правовой ответственности за их несоблюдение или игнорирование.

Банк России обоснованно полагает, что в странах, в которых отсутствует запрет на осуществление сделок с криптовалютами, регуляторы разрабатывают и вводят законодательные требования к биржам криптовалют, направленные на предотвращение рисков легализации денежных средств, полученных преступным путем, и финансирования терроризма [165] в целях осуществления мониторинга, помогающего определить дальнейшее направление уголовно-правовой политики и минимизировать риски, связанные с неконтролируемым обращением криптовалют. Регуляторы вводят либо ужесточают уже имеющиеся требования в части лицензирования деятельности поставщиков услуг в криптовалютном сегменте экономической деятельности. Такие требования относятся и к лицам, оказывающим посреднически услуги по купле-продаже криптовалюты.

Также необходимо реализовать комплекс мер, направленных на контроль за процессом генерации (майнинга) криптовалюты, так как бесконтрольность такого процесса приводит к необоснованному расходованию электроэнергии, которая зачастую используется незаконно, при так называемых случаях «криптоджекинга»[166].

Стоимость электроэнергии – важный показатель доходности «майнеров», так как высокая стоимость электроэнергии резко увеличивает его затраты, вследствие чего часть из них использует электроэнергию незаконно, прибегая при этом к различным способам ее получения[167].

---

[165] См.: Банк России. Доклад для общественных консультаций… С. 31.

[166] См.: Русскевич Е.А., Малыгин И.И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики.2021. № 3. С. 106–125.

[167] См.: Чащин О.Н., Савченко Н.В. Исследование и математическое моделирование доходности майнинга криптовалюты на примере биткойна // Анализ, моделирование, управление, развитие социально-экономических систем: сборник научных трудов XII Международной школы-симпозиума АМУР-2018 (Симферополь-Судак, 14–27 сентября 2018 г.) / Под общей редакцией А. В. Сигала. Симферополь-Судак, 2018. С. 486–488.

Не отрицая проработанность предложений Минфина России относительно законодательных мер, направленных на регулирование криптовалютного оборота, тем не менее необходимо отметить тот факт, что законодательная регламентация любой деятельности должна предусматривать механизм реализации таких мер. В данном случае реализация возможна только путем применения мер уголовно-правового воздействия в отношении физических лиц, нарушающих установленные законодательные запреты, в целях устранения возникающих угроз нарушения прав добросовестных участников криптовалютного рынка.

Полагаем, что в данном случае необходимо вести речь о комплексе законодательных дополнений, предусматривающих не только введение законодательных ограничений оборота криптовалюты на территории Российской Федерации, но и уголовную ответственность за нарушение или несоблюдение вводимых запретов.

Результаты проведенного автором среди следователей и руководителей следственных подразделений Следственного комитета Российской Федерации социологического исследования свидетельствуют о возникающих сложностях расследования уголовных дел о преступлениях с использованием криптовалюты и необходимости совершенствования законодательства в указанной сфере.

Между тем, совершенствование законодательства, регулирующего криптовалютный оборот, невозможно без введения уголовной ответственности за преступления, совершенные с использованием криптовалюты. Необходимо внести изменения в УК РФ, предусматривающие введение уголовной ответственности за нарушение законодательных запретов на использование криптовалюты в качестве средства платежа за товары, работы, услуги, продаваемые и покупаемые юридическими и физическими лицами – резидентами Российской Федерации, за нарушение запрета на организацию выпуска, обращения, обмена либо непосредственно выпуск, организацию и обмен криптовалюты (в том числе криптобиржами,

криптообменными пунктами, виртуальными P2P-платформами) на территории Российской Федерации, а также за нарушение запрета для финансовых организаций на собственные вложения в криптовалюты и непосредственно связанные с ними финансовые инструменты, использование российских финансовых посредников и инфраструктуры финансового рынка для осуществления любых операций с криптовалютой: приобретение криптовалюты, осуществление платежей и переводов, отчуждение криптовалют и способствование осуществлению подобных операций (в том числе оказание услуг по хранению или содействие принятию рисков через деривативы). Из вышеизложенного можно сделать вывод, что бесконтрольный оборот криптовалют на территории Российской Федерации может привести к фактической конкуренции криптовалют с национальной валютой, имеющей официальное хождение на территории страны, что в свою очередь неизбежно приведет к финансовой дестабилизации государства и, как следствие, резкому падению благосостояния граждан.

В целях недопущения угроз благосостоянию граждан Российской Федерации, финансовой стабильности государства, расширения нелегальной деятельности и снижения количества преступлений, совершаемых с использованием криптовалюты, и, как следствие, стабилизации национальной финансовой системы автором предлагается внесение изменений в уголовное законодательство Российской Федерации, которые позволят прекратить или в значительной степени ограничить использование криптовалют юридическими и физическими лицами – резидентами Российской Федерации в качестве фактического средства платежа как на территории Российской Федерации, так и вне ее юрисдикции. В свете изложенного видится необходимым принятия закона, ограничивающего деятельность по осуществлению майнинга криптовалют и предлагается рассмотреть проект закона о внесении изменений в УК РФ о введении уголовной ответственности за осуществление незаконного майнинга и незаконного использования криптовалют (См. Приложение № 7).

8 июня 2022 года в Государственной Думе прошло заседание рабочей группы по вопросу законодательного регулирования криптовалют под председательством А.В. Гордеева. Членами группы обсуждался проект Федерального закона «О регулировании цифровых валют (криптовалют)». По итогам обсуждения были внесены предложения по новому регулированию порядка обращения цифровых валют. Среди прочего экспертный совет предлагает классифицировать майнинг как предпринимательскую деятельность с установлением коммерческих тарифов на электроэнергию, используемую для его осуществления. Для выделения в отдельную категорию в целях возможности контроля и регулирования так называемого «бытового майнинга», то есть майнинга без использования интегральных схем специального назначения (ASIC), необходимо на законодательном уровне дать определение бытового энергопотребления, которое в настоящее время отсутствует.

Сформированные на заседании рабочей группы предложения переданы в Правительство Российской Федерации, где сейчас рассматривается проект Федерального закона «О регулировании цифровых валют (криптовалют)». Документ, разработанный Министерством финансов, рассматривается с участием Банка России и планируется к внесению в Государственную Думу до конца весенней сессии[168].

Представляется, что предлагаемые изменения позволят в полной мере восполнить пробелы в уголовном законе и будут направлены на эффективное противодействие преступлениям, совершаемым с использованием криптовалюты.

---

[168] В Государственной Думе обсудили регулирование майнинга и криптовалют [Электронный ресурс] / Официальный сайт Государственной Думы. Режим доступа: http://duma.gov.ru/news/54548/ (дата обращения – 05.05.2023).

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволяет сделать вывод о том, что эффективной реализации уголовно-правовой политики противодействия преступлениям с использованием криптовалюты препятствуют отсутствие законодательного обеспечения контроля за осуществлением генерации (майнинга) криптовалюты, ее оборота на территории Российской Федерации и, как следствие, недостатки в технико-юридическом конструировании отдельных статей особенной части Уголовного кодекса Российской Федерации, отсутствие рекомендаций Верховного Суда Российской Федерации по уголовным делам указанной категории, противоречивые подходы к оценке одних и тех же предметов и явлений представителями науки уголовного права.

Необходимо отметить, что в настоящее время на всех уровнях государственной власти цифровизации современной российской экономики, а также государственных управленческих структур придается первостепенное значение. В рамках реализации Указа Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», в том числе с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством Российской Федерации на базе программы «Цифровая экономика Российской Федерации» была сформирована национальная программа «Цифровая экономика Российской Федерации», которая была утверждена «протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7»[169].

Отдельного внимания заслуживают системы распределенного реестра данных, так называемые блокчейн-технологии, являющиеся стратегическим

[169] См.: Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. Режим доступа: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения – 11.05.2023).

инструментом, обозначающим приоритеты и перспективы развития цифровых технологий в России.

Технология систем распределенного реестра представляет собой принципиально новый подход к созданию баз данных любой направленности.

Крайне важным условием развития указанных технологий является устранение существующих барьеров, препятствующих их внедрению в экономику и государственные управленческие структуры, ввиду чего необходимо не только скорректировать существующее законодательство с целью создания благоприятной нормативно-правовой среды, но и определить научные основы, обеспечивающие единообразие квалификации преступлений, совершаемых с использованием таких технологий, одной из разновидностей которых является криптовалюта. Такой комплексный подход будет способствовать обеспечению безопасности цифрового пространства от преступных посягательств, защите имущественных прав граждан Российской Федерации, то есть решению задач, определенных Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

Необходимо отметить растущий интерес российских граждан к криптовалюте, объем сделок с которой постоянно увеличивается. Российские граждане являются активными пользователями различных интернет-платформ, осуществляющих торговлю криптовалютами, Российская Федерация находится в числе лидеров по объему мировых майнинговых мощностей. Все это приводит к внутригосударственному перераспределению финансов и активному развитию криптовалютного сектора экономики, однако долгосрочный потенциал применения криптовалют для расчетов представляется ограниченным и связанным со значительными рисками, в том числе криминального характера.

Стремительный рост рыночной стоимости криптовалют определяется, в первую очередь, спекулятивным спросом в расчете на дальнейший рост

курса, что приводит к формированию так называемого финансового пузыря, то есть появлению на рынке больших объемов ничем не обеспеченных финансовых активов, что в свою очередь не только запускает инфляционные процессы, но и создает причины и условия совершения преступлений с использованием виртуальной среды. Также криптовалютам присущи определенные характеристики финансовой пирамиды, поскольку рост их цены поддерживается в том числе за счет расширения участников криптовалютного рынка, а также публичных заявлений медийных личностей относительно отдельных видов криптовалют. Соответственно, бесконтрольное распространение криптовалют создает существенные угрозы для благосостояния граждан Российской Федерации и стабильности финансовой системы государства в целом.

Криптовалюта не может быть запрещена на законодательном уровне в силу технологических особенностей, позволяющих использовать ее, игнорируя любые законодательные запреты. Как показывает анализ, любой законодательный запрет на использование криптовалюты неизбежно приводит к отсутствию действенного механизма его реализации. Это служит фактором ее дополнительной популяризации, что, в свою очередь, стимулирует повышение котировок отдельных видов криптовалют, приводя к росту волатильности.

Высокая волатильность курса криптовалют создает предпосылки для совершения различных видов мошенничества как непосредственно в торговле криптовалютами, так и при совершении сделок с ее использованием, что также повышает риски утраты гражданами существенной части вложенных в криптовалюту средств. Относительная анонимность при использовании криптовалюты делает ее привлекательным инструментом для противоправной деятельности (отмывание доходов, наркоторговля, финансирование терроризма, вымогательство, взяточничество и т.д.), создавая благоприятные условия для незаконных финансовых операций, в том числе международного

характера, что уже само по себе является вызовом для глобальной системы противодействия отмыванию денег и финансированию терроризма.

В зависимости от способа совершения преступления криптовалюта может выступать как предметом хищения, так и предметом подкупа, взятки, легализации (отмывания), а также средством финансирования незаконной деятельности, средством совершения других преступлений против личности, общественной безопасности и т.д., либо в качестве суррогатного средства платежа.

Необходимо отметить, что легализация посредством криптовалюты денежных средств, полученных в результате совершения преступлений, является фактической основой криптовалютной преступности, так как конечной целью большинства преступлений, предметом которых является криптовалюта, является конвертация криптовалюты в фиатные деньги, которые можно на законном основании хранить в кредитных организациях и использовать по своему усмотрению. Указанного явления можно избежать либо значительно уменьшить его масштабы путем принятия закона, устанавливающего контроль со стороны государственных органов за процессом создания и оборотом криптовалют и введения уголовно-правовых запретов за нарушение указанного закона.

Невозможность законодательного запрета на использование криптовалют не означает невозможность контроля их использования, в том числе и средствами уголовно-правового регулирования, направленными на противодействие преступлениям, совершаемым с использованием криптовалюты. В целях реализации положений закона, обеспечивающего контроль за осуществлением генерации (майнинга) криптовалюты и ее оборотом, необходимо дополнить особенную часть Уголовного кодекса Российской Федерации статьями, предусматривающими ответственность за осуществление генерирования (майнинга) криптовалют без регистрации или без лицензии, за нарушение запрета на использование российских финансовых

посредников и инфраструктуры финансового рынка для осуществления любых операций с криптовалютой.

На основании проведенного исследования сформулированы основные выводы и научно обоснованные рекомендации, определены перспективы дальнейшей разработки темы, указывающие направления развития национального уголовного законодательства, а также совершенствования правоприменительной деятельности в сфере противодействия преступлениям, совершаемым с использованием криптовалюты.

Полученные результаты позволяют наметить следующие перспективы дальнейшей разработки темы исследования:

– изучение способов совершения преступлений с использованием криптовалюты как элемента объективной стороны преступления с целью последующего разграничения смежных составов преступлений;

– исследование особенностей квалифицирующего признака «крупный или особо крупный размер» применительно к хищениям криптовалюты;

– анализ причинной связи совершения преступлений с использованием криптовалюты;

– выработка критериев отграничения преступлений, совершенных с использованием криптовалюты, от других преступлений в сфере высоких технологий.

Рекомендации, которые были сформулированы по итогам исследования, могут быть использованы при внесении законопроектов об изменении и дополнении Уголовного кодекса Российской Федерации, а также использоваться Верховным Судом Российской Федерации при даче рекомендаций в виде постановлений Пленума и Обзоров рассмотрения уголовных дел в сфере оборота криптовалюты.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты, официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г., с изменениями, одобренными в ходе 174 общероссийского голосования 01.07.2020 г.) // Российская газета. — 2020. — 4 июля, № 144. (дата обращения: 11.05.2023).

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149—ФЗ (ред. от 02.12.2019) // Российская газета. 2006. 29 июля. № 165. (дата обращения: 17.05.2023).

3. О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генпрокуратуры России № 35/11, МВД России № 1 от 24.01.2020. Документ опубликован не был. Доступ из Справочно-правовой системы «Консультант плюс». (дата обращения: 16.05.2023).

4. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон Российской Федерации от 31 июля 2020 г. № 259—ФЗ // Российская газета. 2002. 30 июля. (дата обращения: 17.05.2023).

5. О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114—ФЗ (ред. от 01.07.2021) // Российская газета. 2002. 30 июля. № 138—139. (дата обращения: 17.05.2023).

6. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 29.07.2017 № 276—ФЗ // Собрание законодательства РФ. 2017. 31 июля. № 31 (часть I). Ст. 4825. (дата обращения: 16.05.2023).

7. О Стратегии государственной национальной политики Российской Федерации на период до 2025 года: Указ Президента Российской

Федерации Федерации от 19 декабря 2015 г. № 1666 // Собрание законодательства РФ. 2012. 24 декабря. (дата обращения: 17.05.2023).

8. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 // Собрание законодательства РФ. 2016. 4 января. № 1 (ч. II). Ст. 212. (дата обращения: 17.05.2023).

9. О безопасности: Закон от 05.03.1992 № 2446—1 // Российская газета. 1992. 6 мая. (дата обращения: 15.05.2023).

10. Уголовный кодекс Российской Федерации от 13.06.1996 № 63—ФЗ (ред. от 30.12.2020) // Собрание законодательства РФ. — 1996. — № 25. (с последующими изменениями и дополнениями). (дата обращения: 19.05.2023).

11. Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1—ФЗ (с изм. и доп., вступ. в силу с 17.01.2021). — URL: http://www.consultant.ru/document/cons_doc_LAW_12940/ (дата обращения: 18.05.2023).

12. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174—ФЗ (ред. от 08.12.2020) (с изм. и доп., вступ. в силу с 19.12.2020) // Российская газета. — 2001. − № 249. (дата обращения: 18.05.2023).

13. О противодействии терроризму: Федеральный закон от 06.03.2006 № 35—ФЗ (ред. от 26.05.2021) // Российская газета. 2006. 10 марта. № 48. (дата обращения: 17.05.2023).

14. О противодействии коррупции: Федеральный закон от 25.12.2008 № 273—ФЗ (ред. от 30.12.2021) // Российская газета. 2008. 30 декабря. № 266. (дата обращения: 16.05.2023).

15. О безопасности: Федеральный закон от 28.12.2010 № 390—ФЗ (ред. от 09.11.2020) // Собрание законодательства РФ. 2011. 3 января. № 1. Ст. 2. (дата обращения: 15.05.2023).

Монографии, учебники, пособия

16. Бакулина, А. А. Блокчейн как объект оценки / А. А. Бакулина, В. В. Григорьев. — М.: Общество с ограниченной ответственностью «Русайнс», 2021. — 200 с.

17. Волынский, А. Ф. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты) / А. Ф. Волынский, В. А. Прорвич. — М.: Экономика, 2019. — 363 с.

18. Гаухман, Л. Д. Квалификация преступлений: закон, теория, практика / Л. Д. Гаухман. — 4—е изд., перераб. и доп. — М.: Центр ЮрИнфоР, 2010. — 557 с.

19. Гилинский, Я.И. Криминология: теория, история, эмпирическая база, социальный контроль: монография / Я.И. Гилинский. — Спб.: Алеф-Пресс, 2014. — 573 с.

20. Головненков, П.В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия : Strafgesetzbuch (StGB) : научно-практический комментарий и перевод текста закона / П. В. Головненков. — URL: https://publishup.uni—potsdam.de/frontdoor/index/index/docId/47371 (дата обращения: 19.03.2022).

21. Дьяков, С.В. Преступления против основ конституционного строя и безопасности государства. (Теория и практика уголовного права и уголовного процесса) / С.В. Дьяков. — М.: Юридический центр, 2012. — 265 с.

22. Ермолович, Я.Н. Должностные преступления в Российском уголовном праве: монография / Я.Н. Ермолович. — М.: Юрлитинформ, 2020. — 328 с.

23. Жалинский, А.Э. Глава 6. Объект преступления // Уголовное право России : в 2 т. — Т. 1 : Общая часть / отв. ред. А.Н. Игнатов, Ю.А. Красиков. — М., 2000. — 370 с.

24. Изотов, Ю. Г. Теория криптовалют / Ю. Г. Изотов. — М. : Общество с ограниченной ответственностью «Проспект», 2022. — 312 с.

25. Иншаков, С.М. Криминология: учебник / С.М. Иншаков. — М. Юриспруденция, 2000. — 426 с.

26. Избранные труды / О. Е. Кутафин ; сост: В.В. Касьянов, В.Н. Нечипуренко, С.И. Самыгин ; М-во образования и науки Российской Федерации, Московский гос. юридический ун-т им. О. Е. Кутафина (МГЮА). М.: Проспект, 2016. — 367 с.

27. Катков, Д.Б. Конституционное право: Вопросы и ответы: учеб. пособие для вузов / Д.Б. Катков, Е.В. Корчиго. — 2 изд. исп., доп. — М., 2001. — 188 с.

28. Князьков, А.А. Теория и практика квалификации преступлений. Учебное пособие / А.А. Князьков. — Ярославль: Ярославский государственный университет им. П. Г. Демидова, 2018. — 66 с.

29. Красинский, В. В. Терроризм 2.0: монография / В. В. Красинский ; [рец.: А. Д. Керимов, И. В. Холиков]. — Москва : Юрлитинформ, 2023. — 262 с.

30. Криптовалюта как средство платежа: частноправовой и налоговый аспекты : монография / Министерство науки и высшего образования Российской Федерации; Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). — М. : Общество с ограниченной ответственностью «Проспект», 2021. — 352 с.

31. Крылов, Г. О. Проблемы безопасности оборота цифровых финансовых активов в криптоэкономике / Г. О. Крылов, В. М. Селезнев. — М.: Общество с ограниченной ответственностью «Издательство Прометей», 2020. — 348 с.

32. Лазар, М. Г., Лейман, И. И. НТР и нравственные факторы научной деятельности. Ленинград : Наука. Ленингр. отд-ние, 1978. — 160 с.

33. Лопашенко, Н.А. Преступления против собственности. Авторский курс. — Кн. I. Общетеоретическое исследование посягательств на собственность: монография. — М.: Юрлитинформ, 2019. — 294 с.

34. Мертон, Р. Российское уголовное право. Общая часть: курс лекций / Р. Мертон, А.В. Наумов. — М., 1996. — 560 с.

35. Ожегов, С.И., Шведова Н.Ю. Толковый словарь русского языка / Российская академия наук. Институт русского языка им. В. В. Виноградова. 4—е изд. Дополненное. М: Азбуковник, 1977. — 944 с.

36. Ордов, К. В. Криптовалюта: теория и практика создания и функционирования / К. В. Ордов, В. В. Григорьев. — М. : Общество с ограниченной ответственностью «Издательство «КноРус», 2021. — 202 с.

37. Основы российского рынка криптовалют / В. А. Галанов, Д. Г. Перепелица, Н. Ф. Челухина [и др.]. — М. : Компания КноРус, 2019. — 134 с.

38. Перов, В. А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты : учебно-методическое пособие / В. А. Перов. — М. : Издательство «Юрлитинформ», 2017. — 200 с.

39. Перов, В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: учебно-методическое пособие / В.А. Перов. — М.: Юрлитинформ, 2017. — 200 с.

40. Пинкевич, Т. В. Международный опыт противодействия преступной деятельности с использованием криптовалюты / Т. В. Пинкевич, Е. С. Смольянинов. — М. : Академия управления Министерства внутренних дел Российской Федерации, 2021. — 108 с.

41. Простосердов, М. А. Экономические преступления, совершаемые в киберпространстве / М. А. Простосердов. — М. : Издательство «Юрлитинформ», 2017. — 168 с.

42. Противодействие преступлениям, совершаемым в сфере оборота криптовалюты / А. В. Андреев, Д. В. Галиев, В. В. Гончар [и др.]. — М. : Издательский Дом «Инфра-М», 2022. — 211 с.

43. Пшеничников, В. В. Эволюция форм и видов денег: от раковин каури до криптовалют / В. В. Пшеничников ; Воронежский государственный аграрный университет им. Императора Петра I. — Воронеж : Воронежский государственный аграрный университет им. Императора Петра I, 2019. — 175 с.

44. Рарог, А. И. Проблемы квалификации преступлений по субъективным признакам / А. И. Рарог. — М. : Издательство Проспект, 2015. — 232 с.

45. Расследование преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных технологий : Научно-практическое пособие / А. А. Бессонов , Ф. О. Байрамова, И. В. Гарт [и др.] ; Следственный комитет Российской Федерации. — М. : Издательство «Юрлитинформ», 2021. — 176 с.

46. Расследование преступлений, совершенных с использованием криптовалюты : учебное пособие / Д. А. Иванов, М. М. Макаренко, В. В. Пушкарев, Е. А. Русскевич. — М., 2021. — 80 с.

47. Риски цифровизации : виды, характеристика, уголовно-правовая оценка: монография / отв. ред. Ю.В. Грачева. — М. : Проспект, 2022. — 272 с.

48. Русскевич, Е. А. Уголовное право и «цифровая преступность»: проблемы и решения / Е. А. Русскевич. — 2-е издание. — М. : Издательский Дом «Инфра-М», 2022. — 351 с.

49. Уголовное право. Особенная часть. Государственные преступления / Герцензон, А.А., Меньшагин, В.Д., Ошерович, Б.С., Пионтковский, А.А. — М. : Юрид. Изд-во, 1938. — 160 с.

50. Устинов, В. С. Техника конструирования дефиниции в уголовном законодательстве / В.С. Устинов ; под ред. акад. А. М. Баранова. //

Законодательная техника современной России: состояние, проблемы, совершенствование: сб. статей в 2 т. — Н. Новгород, 2001. — Т. 2. — 207 с.

51. Фильченко, А. П. Противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : Монография / А. П. Фильченко, В. Ю. Жандров. — М. : Московский университет МВД России имени В.Я. Кикотя, 2018. — 110 с.

52. Черненко, Т. Г. Квалификация преступлений: вопросы теории и практики: монография / Т.Г. Черненко. — 2 — е изд., перераб.и доп. — Кемерово, 2012. — 188 с.

53. Чурилов, А. Ю. Правовое регулирование применения технологии блокчейн / А. Ю. Чурилов. — М. : Юридический Дом «Юстицинформ», 2021. — 152 с.

54. Шаргородский, М. Д. Избранные работы по уголовному праву / М.Д. Шаргородский. — СПб., 2003. — 434 с.

55. Яковлев, В. И. Объекты гражданских прав / В. И. Яковлев, В. А. Внукова. — Белгород : Автономная некоммерческая организация высшего образования «Белгородский университет кооперации, экономики и права», 2017. — 190 с.

56. Якушин, В.А. Квалификация преступлений. Общие вопросы. Курс лекций / В.А. Якушин. — Тольятти: ВУиТ, 2016. — 188 с.

Диссертации и авторефераты

57. Бадамшин, С.К. Преступления террористической направленности, совершаемые с использованием электронных или информационно-телекоммуникационных сетей: уголовно-правовая и криминологическая характеристика: дис. ... канд. юрид. наук. — М., — 2018. — 275 с.

58. Григорян, Г.Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: автореф. дис. ... канд. юрид. наук. — Самара, 2021. — 23 с.

59. Дурнова, И.А. Правовой механизм защиты основ конституционного строя Российской Федерации: автореферат дис. … канд. юрид. наук. — Саратов, 2013. — 226 с.

60. Дюдикова, Е.И. Перспективы развития электронных денег как элемента национальной платежной системы Российской Федерации: автореф. дис. ... канд. экономич. наук. — Ставрополь, 2017. — 27 с.

61. Купцова, Т.А. Функционирование денежных суррогатов в форме криптовалюты в системе современных экономических отношений: автореф. дис. ... канд. экономич. наук. — Самара, 2022. — 22 с.

62. Летёлкин, Н.В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет»: автореф. дис. ... канд. юрид. наук. — Нижний Новгород, 2018. — 24 с.

63. Луценко, Н.С. Судебный штраф: проблемы теории и правоприменения : дис. … канд. юрид. наук. — Хабаровск, 2019. — 237 с.

64. Мелкумян, К.С. Эффективность деятельности Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) в противодействии финансированию терроризма: дис. … канд. полит. наук. — М., 2019. — 345 с.

65. Миц, Д.С. Конституционно-правовые ценности и механизмы в сфере противодействия противоправным посягательствам на конституционный строй: сравнительное—правовое исследование. автореф. дис. … канд. юрид. наук. — М., 2016. — 32 с.

66. Мочалкина, И.С. Цифровые права и цифровая валюта как предмет преступлений в сфере экономики: дис. ... канд. юрид. наук. — М., 2022. — 240 с.

67. Немова, М.И. Альтернативные средства расчёта как предмет и средство совершения преступлений в сфере экономики: дис. ... канд. юрид. наук. — М., 2020. — 236 с.

68. Русскевич, Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно—

коммуникационных технологий, и проблемы их квалификации: дис. ... докт. юрид. наук. — М., 2020. — 521 с.

69. Соловьева, Е.А. Преступления, совершаемые в платежных системах: автореф. дис. ... канд. юрид. наук. — Саратов, 2019. — 33 с.

70. Токолов, А.В. Правовое регулирование информационных отношений в сфере оборота цифровых финансовых активов: автореф. дис. ... канд. юрид. наук. — М., 2022. — 21 с.; и др.

71. Фролов, М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук. — М., 2019. — 26 с.

72. Хисамова, З.И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: автореф. дис. ... канд. юрид. наук. — Краснодар, 2016. — 32 с.

Научные статьи

73. Аблятипова, Н. А. К вопросу о необходимости законодательного закрепления виртуальной валюты / Н. А. Аблятипова, А. Н. Самохина // — 2018. — Т. 8, № 11А. — С. 61—69.

74. Александров, А. Г. Использование сети Даркнет при подготовке и совершении преступлений / А. Г. Александров, А. А. Сафронов // Вестник Санкт-Петербургского университета МВД России. — 2021. — № 1(89). — С.156—160.

75. Ализаде, В. А. Судебная практика применения ст. 174[1] УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты / В. А. Ализаде, А. Г. Волеводз // Наркоконтроль. — 2017. — № 4. — С. 8—14.

76. Алубин, В. Е. Криптовалюты: проблемы уголовно-правовой квалификации / В. Е. Алубин, В. В. Ерахмилевич // Труды молодых ученых Алтайского государственного университета. — 2018. — № 15. — С. 310—313.

77. Бастрыкин, А. И. Выявление и расследование преступлений, совершенных с использованием информационно—коммуникационных технологий / А. И. Бастрыкин // Вестник Российской правовой академии. — 2022. — № 4. — С. 88—94.

78. Безручко, Е. В. Преступления, совершаемые с использованием информационно-телекоммуникационных средств: философско-правовое конструирование эффективных классификаций / Е.В. Безручко, А.А. Ходусов // Философия права. — 2020. — № 3 (94). — С. 89—95 .

79. Бойченко, О. В. Инновации противодействия атакам программ-вымогателей / О. В. Бойченко // Теория и практика экономики и предпринимательства : труды XVIII Всероссийской с международным участием научно-практической конференции, Симферополь—Гурзуф, 27—29 апреля 2021 года. — Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2021. — С.13—14.

80. Борщ, Л. М. Современные аспекты сдвигов инновационной парадигмы от цифровой экономики к цифровой трансформации / Л. М. Борщ, С. В. Герасимова // Инновационная парадигма экономических механизмов хозяйствования : сборник научных трудов VII Всероссийской научно-практической конференции с международным участием, Симферополь, 16 мая 2022 года. — Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2022. — С.73—77.

81. Вепрев, С.Б., Перов, В.А. Вопросы информационной безопасности при использовании криптовалют // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. — 2017. — № 2. — С. 66—68.

82. Галкин, Р. Е. О методах тестирования блокчейн-приложений / Р. Е. Галкин, С. М. Старолетов // Высокопроизводительные вычислительные системы и технологии. — 2021. — Т. 5, № 1. — С. 98—106.

83. Дворянкин, О. А. Даркнет — темная сторона Интернета или неужели так все плохо? / О. А. Дворянкин. — 2021. — № 71-1. — С.14 — 20.

84. Детков, А. А. Бесконтактный сбыт наркотических средств посредством сети Интернет: криминогенная обстановка в Алтайском крае / А. А. Детков, М. А. Стародубцева // Уголовно-исполнительное право. — 2021. — Т. 16, № 4. — С. 512—521.

85. Долгиева, М. М. Квалификация вымогательства криптовалюты / М. М. Долгиева // Вестник Воронежского института МВД России. — 2022. — № 3. — С. 219—224 .

86. Долгиева, М. М. Квалификация деяний, совершаемых в сфере оборота криптовалюты / М. М. Долгиева // Вестник Восточно-Сибирского института Министерства внутренних дел России. — 2019. — № 1(88). — С. 1 — 12.

87. Долгиева, М. М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты / М. М. Долгиева // Современное право. — 2018. — № 11. — С. 103—108.

88. Долгиева, М.М. Особенности объекта и предмета преступлений, совершаемых в сфере оборота криптовалюты. // Уголовная юстиция. — № 12. — 2018. — С. 19 —22 .

89. Дробязко, С.Г. Принципы в праве / С.Г. Дробязко // Проблемы развития юр. науки и совершенствование правопр. практики : сб. науч. тр. — Минск: БГУ, 2005. — С. 27—33.

90. Егорова, М. А. Понятие криптовалют в контексте совершенствования российского законодательства / М. А. Егорова, Л. Г. Ефимова // Lex Russica (Русский закон). — 2019. — № 7(152). — С.130—140.

91. Жигас, М. Г. Природа и сущность криптовалюты / М. Г. Жигас, С. Н. Кузьмина // Известия Байкальского государственного университета. — 2018. — Т. 28, № 2. — С. 201—207.

92. Ивличев, П. С. Незаконные методы снижения издержек в процессе криптовалютного майнинга / П. С. Ивличев // Математические методы и информационно-технические средства : Материалы XVI Всероссийской

научно-практической конференции, Краснодар, 19 июня 2020 года. — Краснодар: Краснодарский университет МВД России, 2020. — С. 57—60 .

93. Исаев, А. С. Китай в мировом киберпространстве / А. С. Исаев // Проблемы Дальнего Востока. — 2020. — № 4. — С. 6—23.

94. Качалов, В. В. Получение взятки криптовалютой: вопросы квалификации / В. В. Качалов // Союз криминалистов и криминологов. — 2020. — № 2. — С. 9—25.

95. Кобец, П. Н. О проблеме испытательного срока в механизме условного осуждения / П. Н. Кобец // Российская юстиция. — 2009. — № 9. — С. 13 — 16.

96. Кобец, П. Н. Общая характеристика объективной стороны преступления по действующему уголовному законодательству Российской Федерации / П. Н. Кобец // Символ науки: международный научный журнал. — 2017. — Т. 2, № 2. — С. 187—189.

97. Коренная, А.А. Квалификация преступлений, совершаемых с использованием криптовалюты // Проблемы экономики и юридической практики. — 2018. — № 3. — С. 220 — 223.

98. Костюкова, Е.Н. Криптовалюта и риски ее функционирования / Е.Н. Костюкова // Экономика. Управление. Инновации. — 2019. — №1(5). — С. 42—46.

99. Кочергин, Д. А. Криптоактивы: экономическая природа, классификация и регулирование оборота / Д. А. Кочергин // Вестник международных организаций: образование, наука, новая экономика. — 2022. — Т. 17, № 3. — С. 75—130.

100. Краюшкин, А. А. Понятие финансовой операции как вида деятельности, образующей легализацию преступных доходов / А. А. Краюшкин // Вестник Московского университета МВД России. — 2009. — № 10. — С. 113—115.

101. Криштаносов, В. Б. Концептуально-аналитические подходы к возникновению потенциальных угроз в цифровой экономике /

В. Б. Криштаносов, Н. А. Бровко // AlterEconomics. — 2023. — Т. 20, № 1. — С. 216—245.

102. Кустова, Н. К. Прикосновенность к преступлению и ее соотношение с соучастием в преступлении и иными формами совместной преступной деятельности / Н. К. Кустова // Социально-экономические и гуманитарные науки : сборник избранных статей по материалам Международной научной конференции, Санкт-Петербург, 28 октября 2021 года. — Санкт-Петербург: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2021. — С. 90—92.

103. Лазар, М. Г. НТР и нравственные факторы научной деятельности : Очерки этики науки / М. Г. Лазар, И. И. Лейман. — Ленинград: Санкт-Петербургская издательско-книготорговая фирма «Наука», 1977. — С. 7 —8.

104. Ловцов, Д. А. Информационная безопасность автоматизированных блокчейн систем: угрозы и способы повышения / Д. А. Ловцов // Трансформация национальной социально—экономической системы России : Материалы II Международной научно-практической конференции, Москва, 22 ноября 2019 года. — М.: Российский государственный университет правосудия, 2020. — С.464—473.

105. Лошкарев, А. В. Возмещение ущерба причиненного преступлением с использованием криптовалют / А. В. Лошкарев, А. Е. Крылова // Международный журнал гуманитарных и естественных наук. — 2020. — № 10—3(49). — С.127—130.

106. Лыков, А. А. Хищение криптовалюты: проблемы уголовно-правовой квалификации / А. А. Лыков // Современное уголовно-процессуальное право — уроки истории и проблемы дальнейшего реформирования. — 2019. — Т. 2. — № 1(1). — С.13—18.

107. Мамонтов, С. С. История появления термина «луковая маршрутизация» / С. С. Мамонтов // Язык науки и техники в современном

мире : материалы V международной научно-практической конференции, Омск, 14 апреля 2016 года / Министерство образования и науки РФ; Омский государственный технический университет. — Омск: Омский государственный технический университет, 2016. — С.132—135.

108. Митряев, И. С. Тенденции применения кибератак программ-вымогателей / И. С. Митряев // Инновации. Наука. Образование. — 2021. — № 47. — С. 985—991.

109. Нуркаева, М. К. «Темная сеть» Интернета как инструмент для совершения преступлений и обеспечения преступной деятельности / М. К. Нуркаева // Вестник Дальневосточного юридического института МВД России. — 2021. — № 4(57). — С.120—130 .

110. Нысанбаева, С. Е. Создание инструмента для выявления сетевых вирусов-майнеров на основе криптовалюты monero / С. Е. Нысанбаева, А. Т. Нюсупов, Ж. Б. Манас // Проблемы оптимизации сложных систем : материалы XIV Международной Азиатской школы—семинара, Алматы, 20—31 июля 2018 года. — Алматы: Институт информационных и вычислительных технологий МОН РК, 2018. — С.113—119.

111. Перов, В. А. Криптовалюта как объект гражданского права / В. А. Перов // Гражданское право. — 2017. — № 5. — С.7—9.

112. Перов, В. А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют / В. А. Перов // Безопасность бизнеса. — 2018. — № 2. — С.25—29.

113. Перов, В.А. Проблемные уголовно-правовые аспекты, возникающие при расследовании преступлений, совершенных с использованием криптовалюты. Уголовное право как средство управления обществом. Материалы всероссийской научно—практической конференции. (Москва. 17 марта 2022 года. Часть 2). — С. 149—160.

114. Пикуров, Н. И. Проблемы определения юридической природы криптовалюты для квалификации преступлений против собственности / Н. И.

Пикуров // Вестник Университета прокуратуры Российской Федерации. — 2021. — № 4(84). — С. 59—69 .

115. Пинкевич, Т. В. Предупреждение преступлений, совершаемых в сфере оборота цифровой валюты (криптовалюты) / Т. В. Пинкевич // Правовое государство: теория и практика. — 2021. — № 4(66). — С. 82—96.

116. Поздышев, Р. С. Криптовалюта как угроза финансово-правовому механизму надзора в сфере противодействия легализации преступных доходов и финансированию терроризма / Р. С. Поздышев //. — 2019. — № 8(24). — С.125—128.

117. Полпудников, С. В. Атака 51% в системе биткоин / С. В. Полпудников, А. С. Степанова // European Scientific Conference : сборник статей VIII Международной научно-практической конференции : в 3 ч., Пенза, 07 января 2018 года. Том Часть 1. — Пенза: Наука и Просвещени, 2018. — С. 139—141.

118. Попандопуло, И. Д. «Атака 51%» в криптовалютных системах: сущность, прецеденты, затратность / И. Д. Попандопуло, А. В. Аникин // Научно—методический электронный журнал «Концепт». — 2019. — № 1. — С.205—211.

119. Прудникова, Т. А. К вопросу о квалификации преступлений, совершенных с использованием криптовалюты / Т. А. Прудникова // Вестник Полоцкого государственного университета. — Серия D. Экономические и юридические науки. — 2019. — № 6. — С.165—169 .

120. Пузиков, Е. В. Вредоносный майнинг (криптоджекинг) — новая угроза информационной безопасности / Е. В. Пузиков, А. П. Лапсарь // Информационные системы, экономика и управление : Ученые записки. Том Выпуск 24. — Ростов-на-Дону : Ростовский государственный экономический университет «РИНХ», 2022. — С.70—77.

121. Раднаева, Э. Л. Незаконный оборот наркотических средств и их аналогов с использованием компьютерных технологий (сети интернет) / Э. Л. Раднаева, Р. Н. Салихов // Банзаровские чтения : Материалы международной

научной конференции, посвященной 200-летию со дня рождения Д. Банзарова и 90-летию БГПИ—БГУ. В 2-х частях, Улан-Удэ, 30—31 марта 2022 года / Научный редактор В.В. Номогоева, отв. редактор О.Н. Полянская. Том Часть 2. — Улан-Удэ: Бурятский государственный университет имени Доржи Банзарова, 2022. — С. 73—76.

122. Родыгин, Р. А. К вопросу об особенностях совершения преступлений в сфере незаконного оборота наркотиков с использованием сети Интернет / Р.А. Родыгин // Право: ретроспектива и перспектива. — 2022. — № 4(12). — С. 65—72 .

123. Русскевич Е. А. Уголовное право и информатизация / Е.А. Русскевич // Журнал российского права. — № 8 — 2017. —76 с.

124. Русскевич, Е. А. Преступления, связанные с обращением криптовалют: особенности квалификации / Е.А. Русскевич, И.И. Малыгин // Право. Журнал Высшей школы экономики. — 2021. — № 3. — С. 106—125 .

125. Савенков, А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. — 2017. — № 10. — С. 5—18.

126. Савицкий, А. А. Судебная финансово-экономическая экспертиза операций с криптовалютой манейро // Вестник криминалистики. — 2020. — № 2(74). — С.75—80.

127. Самолысов, П. В. Правовое регулирование майнинга криптовалют // Право и цифровая экономика. — 2020. — № 3(09). — С.13—20 .

128. Санташов, А. Л. Проблемы противодействия хищению денежных средств с банковских счетов, а равно в отношении электронных денежных средств // Пенитенциарная система России в современных условиях развития общества: от парадигмы наказания к исправлению и ресоциализации : Сборник материалов международной научно-практической конференции. В 3-х частях, Вологда, 09—11 декабря 2021 года / Под общей редакцией В.Н. Некрасова. Часть 2. — Вологда: Вологодский институт права и экономики Федеральной службы исполнения наказаний, 2022. — С.111—115.

129. Семибратов, И. В. Оценка вероятности успешной атаки нарушителя в блокчейн-сети / И. В. Семибратов, В. М. Фомичев // Прикладная дискретная математика. Приложение. — 2019. — № 12. — С.169—172 .

130. Сидоренко, Э. Л. Криминологические риски оборота криптовалюты / Э.Л. Сидоренко // Экономика. Налоги. Право. — 2017. — № 6. — С.147—154 .

131. Сидоренко, Э. Л. Криптовалюта как предмет хищения: проблемы квалификации / // Мировой судья. — 2018. — № 6. — С. 18—24.

132. Сидоренко, Э. Л. Хищение криптовалюты: парадоксы квалификации / Э. Л. Сидоренко // Гуманитарные, социально-экономические и общественные науки. — 2018. — № 6. — С.166—171.

133. Сидоренко, Э.Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. — 2018. — № 2 — С.129—137.

134. Состояние преступности в России (2020—2022 гг.): сборник. — М.: Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации, 2020. — С. 1—7.

135. Стригунов, К. Константин Стригунов: «Современные наркокартели — это целые квазигосударства, структуры, сочетающие в себе наемников, повстанцев, террористов и криминальных элементов». Интервью со специалистом в области национальной и международной безопасности, ведущим аналитиком АНО «Ассоциация специалистов по информационным операциям» Константином Стригуновым / К. Стригунов // Юрист спешит на помощь. — 2021. — № 3. — С.9—18 .

136. Сукманов, А. О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений / А. О. Сукманов // Вестник Калининградского юридического института МВД России. — 2010. — № 4(22). — С.104—107 .

137. Тороев, А. С. Классификация и анализ атак на блокчейн-системы / А. С. Тороев, А. В. Колованов // Информационная безопасность — актуальная проблема современности. Совершенствование образовательных технологий

подготовки специалистов в области информационной безопасности. — 2019. — № 1(10). — С.189—196 .

138. Тьюринг, А. М. Может ли машина мыслить? / А. М. Тьюринг // Точки над Ё. — 2014. — № 4(13). — С.90—138 .

139. Усачева, Е. А. Криптовалюта как предмет взятки и коммерческого подкупа: проблемы регулирования / Е. А. Усачева, А. Д. Филимонов // Искусство правоведения. — 2023. — № 1(5). — С.80—90 .

140. Фильченко, А. П. Использование режима санкций и системы комплаенс в снижении рисков незаконных операций с виртуальными активами: зарубежный и российский опыт / А. П. Фильченко, В. Ю. Жандров // Правовое государство: теория и практика. — 2022. — № 3(69). — С. 171—183.

141. Хорошилова, О. С. Классификация составов преступлений по моменту окончания преступления / О. С. Хорошилова // Вестник Кемеровского государственного университета. — 2015. — № 2—2(62). — С.223—226.

142. Чащин, О. Н. Исследование и математическое моделирование доходности майнинга криптовалюты на примере биткойна / О. Н. Чащин, Н. В. Савченко // Анализ, моделирование, управление, развитие социально-экономических систем : сборник научных трудов XII Международной школы—симпозиума АМУР—2018, Симферополь—Судак, 14—27 сентября 2018 года / Под общей редакцией А. В. Сигала. — Симферополь—Судак: ИП Корниенко А.А., 2018. — С.486—488.

143. Черепнев, М. А. Децентрализованная схема защищенного создания и хранения баз данных / М. А. Черепнев // International Journal of Open Information Technologies. — 2020. — Т. 8, № 7. — С.109—115.

144. Черниговский, А. В. Проблема майнинга в корпоративной среде / А. В. Черниговский, М. В. Кривов // Вестник Ангарского государственного технического университета. — 2021. — № 15. — С.123.

145. Шепель, Н. В. Некоторые особенности доказывания при расследовании преступлений, связанных с использованием криптовалют и других виртуальных активов / Н. В. Шепель // Право: ретроспектива и перспектива. — 2022. — № 3(11). — С.93—97 .

146. Ярыгин, П. К. Анализ эффективности применения комбинированной атаки на сети Bitcoin / П. К. Ярыгин // Информатизация и связь. — 2023. — № 1. — С. 98—104 .

147. Яшин, А. В. Проблемы противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемым посредством сети интернет / А. В. Яшин, В. Р. Шикшеев // Вестник Пензенского государственного университета. — 2020. — № 3(31). — С.108.

Иные источники

148. «Концепция законодательного регламентирования механизмов организации оборота цифровых валют». СПС Консультант—плюс (дата обращения: 14.04.2023).

149. Bitcointalk.URL:https://bitcointalk.org/index.php?topic=879455.msg9705944#msg9705944 (дата обращения: 16.05.2022).

150. Chainalysis: отчет по крипто преступлениям 2021. https://vc.ru/finance/251237—chainalysis—otchet—po—kripto—prestupleniyam—2021 (дата обращения: 22.04.2022).

151. Chainalysis: отчет по крипто преступлениям 2021. URL: https://vc.ru/finance/251237—chainalysis—otchet—po—kripto—prestupleniyam—2021 (дата обращения: 22.04.2022).

152. Chainalysis: отчет по крипто преступлениям 2021. URL: https://vc.ru/finance/251237—chainalysis—otchet—po—kripto—prestupleniyam—2021. (дата обращения: 15.05.2023).

153. Cryptocurrency Anti—Money Laundering Report (Report—AML—20180703) / CipherTrace, 2018.— URL:

https://cdn2.hubspot.net/hubfs/4345106/crypto_aml_report_2018q2.pdf (дата обращения: 02.05.2022)

154. Состояние преступности в РФ за январь—декабрь 2021 г. — Текст : электронный // Министерство внутренних дел Российской Федерации : официальный сайт. — 2022. — URL: https://media.mvd.ru/files/application/2315310 (дата обращения: 18.02.2022).

155. Состояние преступности. — Текст : электронный // Министерство внутренних дел Российской Федерации : официальный сайт. — 2022. — URL: https://мвд.рф/reports (дата обращения: 02.01.2022).

156. Group—IB нашла вирус—шифровальщик, который научился майнить криптовалюту // РИА Новости. 24.06.2019. URL: https://ria.ru/20190624/1555846747.html (дата обращения: 08.05.2022).

157. L. Grustniy. Скрытые майнеры в Google Play. — Kaspersky Daily 04.04.2018 URL: https://www.kaspersky.ru/blog/google—play—hidden—miners/20111/ (дата обращения: 21.10.2022).

158. Merriam—webster. URL: https://www.merriam—webster.com/dictionary/extremism. (дата обращения: 22.01.2021).

159. Nakamoto: Bitcoin: A Peer—to—Peer Electronic Cash System. URL: https://nakamotoinstitute.org/bitcoin/.(дата обращения: 15.05.2023).

160. Oxford Learner’s Dictionaries. URL: https://www.oxfordlearnersdictionaries.com/us/definition/english/extremism?q=extremism. (дата обращения: 18.01.2021).

161. URL:http://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf. (дата обращения: 12.03.2022).

162. URL:https://www.faz.net/aktuell/finanzen/devisen—rohstoffe/digitale—waehrung—deutschland—erkennt—bitcoins—als—privates—geld—an—12535059.html (дата обращения: 10.01.2021).

163. Van Wirdum, A. IS BITCOIN ANONYMOUS? A COMPLETE BEGINNER’S GUIDE // Bitcoin Magazine. Nov. 18, 2015. Цит. по: Анонимность в сети Биткоин. Мифы и реальность. [Электронный ресурс]. Режим доступа:

https://cryptor.net/bitkoin—dlya—chaynikov/anonimnost—v—seti—bitkoin—mify—i—realnost (дата обращения — 15.05.2022).

164. Абрамов Е. Взгляд венчурного инвестора на Блокчейн | 09: Атака эгоистичного майнера. URL: https://vc.ru/crypto/330905—vzglyad—venchurnogo—investora—na—blokcheyn—09—ataka—egoistichnogo—maynera (дата обращения: 21.10.2022).

165. Анонимность в сети Биткоин. Мифы и реальность. URL: https://cryptor.net/bitkoin—dlya—chaynikov/anonimnost—v—seti—bitkoin—mify—i—realnost. (дата обращения: 15.05.2022).

166. Атаки в мире криптовалют. URL: https://cryptor.net/bezopasnost/ataki—v—mire—kriptovalyut (дата обращения: 10.04.2022).

167. Банк России. Доклад для общественных консультаций. Криптовалюты: тренды, риски, меры. М. 2022. — 36 с.

168. Безмалый, В. Что такое программа—вымогатель как услуга (RaaS)? — Bis Journal. — 16.06.2021. URL: https://ib—bank.ru/bisjournal/news/15767 (дата обращения: 19.10.2022).

169. Большой юридический словарь // В.Н. Додонов, В.Д. Ермаков, М. М. Крылова. — М.: Издательство «Инфра-М», 2001. — 790 с.

170. Вирусы наступают: как крадут деньги из криптовалютных кошельков. 01.05.2019. Igorka [электронный ресурс]. URL: https://igorka.ru/crypto/virusyi—nastupayut—kak—kradut—dengi—iz—kriptovalyutnyix—koshelkov (дата обращения: 28.10.2022).

171. Генпрокуратура предложит включить в УК криптовалюту как имущество. Текст : электронный // Интерфакс : официальный сайт. — 2021. — URL: https://www.interfax.ru/russia/803274 (дата обращения: 10.12.2021).

172. Германия признала биткоин законным платежным средством. URL:https://forklog.com/germaniya—priznala—bitkoin—zakonnym—platezhnym—sredstvom/ (дата обращения: 10.04.2022).

173. Доля пользователей интернета в России среди молодежи приблизилась к 100%. — Текст : электронный // РосБизнесКонсалт : официальный сайт. — 2021. — URL: https://www.rbc.ru/technology_and_media/12/01/2021/5ffde01e9a79478eb5230426 (дата обращения: 21.08.2021).

174. Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими. — Текст : электронный // Федеральная служба безопасности Российской Федерации : официальный сайт. — 2021. — URL: http://www.fsb.ru/fsb/npd/terror.htm (дата обращения: 24.10.2021).

175. Заседание коллегии ФСБ от 20 февраля 2020 года. — Текст : электронный // Президент Российской Федерации : официальный сайт. — 2020. — URL: http://www.kremlin.ru/events/president/news/62834 (дата обращения: 20.02.2020).

176. Заседание Пленума Верховного Суда РФ 28 октября 2021 года посредством веб—конференции. URL: https://www.youtube.com/watch?v=4IwoQxqBoZQ (дата обращения: 08.11.2021).

177. Интервью Председателя Следственного комитета Российской Федерации Бастрыкина А.И. Текст : электронный // РИА Новости : официальный сайт. — 2020. — URL: https://ria.ru/20201209/korruptsiya—1588207057.html (дата обращения: 27.02.2021).

178. Информационное сообщение Федеральной службы по финансовому мониторингу (Росфинмониторинга) «Об использовании криптовалют» от 06 февраля 2014 г. Текст : электронный // Росфинмониторинга : официальный сайт. — 2020. — URL: http://www.fedsfm.ru/news/957 (дата обращения: 27.02.2021).

179. Исследование: Атака 51% на Биткойн нереалистична. URL:https://bitnovosti.com/2018/11/27/issledovanie—ataka—51—na—bitkojn—nerealistichna/ (дата обращения: 22.04.2022).

180. Как была устроена Hydra. URL: https://rusrepublic.com/2022/04/09/kak—byla—ystroena—hydra—2 (дата обращения: 11.04.2022).

181. Как операторы и программы вымогатели атаковали российский бизнес в 2021 году // Group—IB. URL:https://www.group—ib.ru/whitepapers/ransomware—in—russia— (дата обращения: 09.05.2022).

182. Как русскоязычная даркнет—площадка Hydra за год заработала $1,4 млрд. URL: https://www.securitylab.ru/news/520568.php (дата обращения: 10.04.2022).

183. Карьера в Блокчейне: Колесо возможностей. Какая из них подходит для Вас? URL:https://101blockchains.com/ru/ (дата обращения: 02.05.2022).

184. Краткая характеристика состояния преступности в Российской Федерации за период 2016—2021 гг. [Электронный ресурс]. Министерство внутренних дел Российской Федерации : официальный сайт. — 2021. — URL: https://мвд.рф/reports (дата обращения: 02.01.2022).

185. Крипто—преступность 2021 // Chainalysis. URL: https://is—systems.org/blog_article/11617368536 (дата обращения: 09.05.2022).

186. Куликова, К. Россия намайнила серебро. Она вышла на второе место в мире по производству криптовалют / Коммерсант. 07.04.2023. URL: https://www.kommersant.ru/doc/5915688 (дата обращения 10.04.2023).

187. Ларина Е., Овчинский В. Криптопреступность, новый элемент транснациональной организованной преступности. — Завтра. — 9 марта 2021. URL: https://zavtra.ru/blogs/kriptoprestupnost (дата обращения: 29.04.2022).

188. Манеев, М. Los Angeles Times взломан.Prometheus.[электронный ресурс]. URL: https://prometheus.ru/haker—sumel—ne—tol—ko—vnedrit—

strochki—koda—po—no—i—ostavit—druzheskoe—poslanie / (дата обращения: 25.10.2022).

189. Манеев, М. В рекламных баннерах на YouTube обнаружили майнер Monero Prometheus.[электронный ресурс]. URL: https://prometheus.ru/skript—byl—raskryt—pol—zovatelem—s—pomosch—yu—antivirusa—avast / (дата обращения: 25.10.2022).

190. Механизм комиссий в Биткоине и зачем дружить с майнерами. URL: https://habr.com/ru/company/distributedlab/blog/417775/ (дата обращения: 08.07.2022).

191. Накамото, С. Биткойн: система цифровой пиринговой наличности. URL:https://opartnerke.ru/wp—content/uploads/2017/12/belaya_kniga_bitcoina_satoshi_nakamoto.pdf

192. Нефедова М. Более 200 000 маршрутизаторов MikroTik заражены майнинговой малварью.[электронный ресурс]. URL: https://xakep.ru/2018/08/03/mikrotik—under—attack / (дата обращения: 26.10.2022).

193. Отчет ФАТФ: Финансирование терроризма на этнической или расовой почве. — Текст : электронный // Росфинмониторинг : официальный сайт. — 2021. — URL: https://www.fedsfm.ru/content/files/documents/2021/ethnically—or—racially—motivated—terrorism—financing%20(ru)%20(1)%20(1).doc (дата обращения: 31.10.2021).

194. Отчёт Центробанка по криптовалютам — выжимка с основными тезисами. URL: https://habr.com/ru/post/646955/ (дата обращения: 01.05.2022).

195. Официальный сайт Главного управления МВД России по Волгоградской области. URL:https://34.xn——b1aew.xn——p1ai/ (дата обращения: 11.05.2022).

196. Официальный сайт Лаборатории Касперского. Что такое криптоджекинг — определение и описание. URL:

https://www.kaspersky.ru/resource—center/definitions/what—is—cryptojacking/ (дата обращения: 05.05.2022).

197. Официальный сайт МВД РФ https://xn——b1aew.xn——p1ai/reports/item/23163626 (дата обращения: 04.03.2021).

198. Официальный сайт Министерства внутренних дел по Удмуртской Республики. URL: https://18.xn——b1aew.xn——p1ai/mvdur/ (дата обращения: 22.04.2022).

199. Официальный сайт прокуратуры Республики Коми. URL: https://epp.genproc.gov.ru/web/proc_11/sections?section=25924455 (дата обращения: 12.04.2022).

200. Официальный сайт прокуратуры Республики Коми. URL: https://epp.genproc.gov.ru/web/proc_11/sections?section=25924455.

201. Официальный сайт Следственного комитета Российской Федерации: https://sledcom.ru/activities/statistic (дата обращения: 15.04.2022)

202. Официальный сайт Следственного комитета Российской Федерации: В Чувашии перед судом предстанет местный житель, обвиняемый в покушении на мошенничество в особо крупном размере с криптовалютой. URL: http://sledcom.ru/news/item/1197736/.

203. Парфенов В. В бюджетных смартфонах из Китая найдены «штатные» вирусы. — Techinsider. — 25.08.2020 .URL:https://www.techinsider.ru/gadgets/news—612503—v—byudzhetnyh—smartfonah—iz—kitaya—naydeny—shtatnye—virusy/ (дата обращения: 21.10.2022).

204. Петров, С. Уничтожаем криптомифы. Можно ли защитить монету от атаки 51 процента? URL: https://2bitcoins.ru/mozhno—li—zashhititsya—ot—ataki—51/ (дата обращения: 29.04.2022).

205. Попандопуло, И. Д., Аникин, А. В. Атака 51% в криптовалютных системах: сущность, прецеденты, затратность. — Научно—методический электронный журнал «Концепт». — 2019. — № 1 (январь). —С.5.

URL:file:///C:/Users/User/Downloads/ataka—51—v—kriptovalyutnyh—sistemah—suschnost—pretsedenty—zatratnost.pdf (дата обращения: 29.04.2022).

206. Пулы для майнинга — что это? URL: https://zen.yandex.ru/media/id/5ddc12d2f30b6a4cdd4557af/puly—dlia—maininga—chto—eto—5de514ded4f07a00ac1be392 (дата обращения: 05.05.2022).

207. Роскомнадзор приступил к формированию реестра социальных сетей. — Текст : электронный // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации : официальный сайт. — 2021. — URL: https://rkn.gov.ru/news/rsoc/news73860.htm (дата обращения: 24.09.2021).

208. Росфинмониторинг встревожен финансированием терроризма через криптовалюты. — Агенство «Интерфакс». —27.06.2022. URL:https://www.interfax.ru/business/849049. (дата обращения: 22.10.2022).

209. Росфинмониторинг пресек финансовую деятельность более 15 000 террористов. — Текст : электронный // Ведомости : URL: https://www.vedomosti.ru/society/news/2021/10/29/893737—rosfinmonitoring—presek—deyatelnost—terroristov (дата обращения: 31.10.2021).

210. Сводные статистические сведения о деятельности федеральных судов общей юрисдикции и мировых судей за 2020 год. — Текст : электронный // Судебный департамент при Верховном Суде Российской Федерации : официальный сайт. — 2020. — URL: http://cdep.ru/index.php?id=79&item=5671 (дата обращения: 07.07.2021).

211. Сводные статистические сведения о состоянии судимости в России за 2020 год. — Текст : электронный // Судебный департамент при Верховном Суде Российской Федерации : официальный сайт. — 2020. — URL: http://www.cdep.ru/userimages/sudebnaya_statistika/2021/k4—svod_vse_sudy—2020.xls (дата обращения: 06.10.2021).

212. Сводные статистические сведения о состоянии судимости в России за I полугодие 2020 года. — Текст : электронный // Судебный

департамент при Верховном Суде Российской Федерации : официальный сайт. — 2021. — URL: http://www.cdep.ru/index.php?id=79&item=5895 (дата обращения: 20.10.2021).

213. Сводные статистические сведения о состоянии судимости в России за I полугодие 2020 года. — Текст : электронный // Судебный департамент при Верховном Суде Российской Федерации : официальный сайт. — 2020. — URL: http://cdep.ru/index.php?id=79&item=5460 (дата обращения: 07.07.2021).

214. Справка обобщения судебной практики по делам о преступлениях, предусмотренных статьями 280, 282, 282.1, 282.2 УК РФ . — Текст : электронный // Верховный Суд Удмуртской Республики : официальный сайт. — 2011. — URL: http://vs.udm.sudrf.ru/modules.php?id=499&name=docum_sud (дата обращения: 22.02.2020).

215. Суд вынес приговор сотруднику ядерного центра в Сарове за майнинг // РБК. URL:https://www.rbc.ru/society/27/09/2019/5d8e3c489a79479544347d35 (дата обращения: 25.04.2022).

216. Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/CQABiQ3tU55V/ (дата обращения: 07.07.2022).

217. США ввели санкционные меры в отношении Hydra и Garantex. URL:https://rus—republic.com/2022/04/07/ssha—vveli—sankcionnye—mery—v—otnoshenii—hydra—i—garantex (дата обращения: 01.07.2022).

218. Токарев Д. Обзор действующих блокчейн—приложений. URL:https://bitcryptonews.ru/blogs/blokchejn/obzor—dejstvuyushhix—blokchejn—prilozhenij (дата обращения: 26.04.2022).

219. Угрозы шифровальщиков 2021 // Palo Alto Networks. URL: https://is—systems.org/blog_article/31624268053 (дата обращения: 09.05.2022).

220. ФСБ арестовала двух сотрудников Российского ядерного центра за майнинг биткоинов на суперкомпьютере. URL:https://www.cnews.ru/news/top/2018—02—

09_dva_rossijskih_inzhenera_majnili_bitkoiny_na_superkompyutere (дата обращения: 10.04.2022).

221. Число пользователей интернета в России достигло 124 млн. — Текст :электронный // ТАСС : официальный сайт. — 2021. — URL: https://tass.ru/obschestvo/12698757 (дата обращения: 06.02.2022).

222. Что Делает Блокчейн Таким Безопасным? // Binanc academy. URL: https://academy.binance.com/ru/articles/what—makes—a—blockchain—secure (дата обращения: 10.04.2022).

223. Что такое Double Spending (двойная трата): типы атак. — 10.07.2020. URL: https://bit.news/member/chto—takoe—double—spending—dvojnaya—trata—tipy—atak (дата обращения: 21.10.2022).

224. Что такое криптоджекинг — определение и описание. Лаборатория Касперского. URL: https://www.kaspersky.ru/resource—center/definitions/what—is—cryptojacking (дата обращения: 06.05.2022).

225. Что такое системные ресурсы компьютера. URL: https://doma35.ru/computers/chto—takoe—sistemnye—resursy—kompyutera/ (дата обращения: 06.05.2022).

226. Что угрожает блокчейн—сетям: рассматриваем атаки и способы защиты. URL: https://habr.com/ru/company/bitfury/blog/346656/ (дата обращения: 29.04.2022).

227. Шпунт, Я. Крипта все чаще в криминальных сводках // Новости цифровой трансформации, телекоммуникации, вещания и ИТ Comnews.15.06.2022 URL: https://www.comnews.ru/content/220715/2022—06—15/2022—w24/kripta—vse—chasche—kriminalnykh—svodkakh (дата обращения: 18.10.2022.

Акты судебных органов

228. Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации

(отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». СПС «Консультант плюс» (дата обращения: 29.03.2023).

229. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате». СПС «Консультант плюс» (дата обращения: 07.04.2023).

230. Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 15.12.2022) «О судебной практике по делам о краже, грабеже и разбое». СПС «Консультант плюс» (дата обращения: 15.04.2023).

231. Постановление Пленума Верховного Суда РФ от 09.07.2013 № 24 (ред. от 24.12.2019) «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» (дата обращения: 28.04.2023).

232. Постановление Пленума Верховного Суда РФ от 24.12.2019 № 59 «О внесении изменений в постановления Пленума Верховного Суда Российской Федерации от 9 июля 2013 года № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» и от 16 октября 2009 года № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» (дата обращения: 12.05.2023).

233. Приговор Железнодорожного районного суда г. Симферополя (Республика Крым) по уголовному делу по делу № 1—200/2020 от 29 июля 2020 г. [Электронный ресурс] Железнодорожны районный суд г.Симферополя(РеспубликаКрым)URL:http://zheleznodorozhniy.krm.sudrf.ru/modules.php?name=press_dep&op=12&arc_list=2019—07 (дата обращения: 25.04.2023).

234. Приговор Октябрьского районного суда г. Кирова по уголовному делу № 1—44/2020 от 13 февраля 2020 г. [Электронный ресурс] / Октябрьский

районный суд г. Кирова. URL: https://oktyabrsky——kir.sudrf.ru (дата обращения: 26.02.2023).

235. Приговор Октябрьского районного суда г. Кирова по уголовному делу № 1—44/2020 от 13 февраля 2020 г. [Электронный ресурс] / Октябрьский районный суд г. Кирова. URL: https://oktyabrsky——kir.sudrf.ru (дата обращения: 26.02.2023).

236. Приговор Петроградского районного суда г. Санкт-Петербурга по уголовному делу № 1—95/2020 от 30 июня 2020 г. [Электронный ресурс] / Петроградский районный суд г. Санкт—Петербурга. URL: http://pgr.spb.sudrf.ru (дата обращения: 16.02.2023).

237. Приговор Собиского городского суда по уголовному делу № 1—1—276/2017 от 14 декабря 2017 г. [Электронный ресурс] / Собинский городской суд Владимирской области. URL: https://sobinsky——wld.sudrf.ru (дата обращения: 16.02.2023).

238. Приговор Сургутского городского суда Ханты-Мансийского автономного округа — Югры по уголовному делу № 1—762/2017 от 3 ноября 2017 г. [Электронный ресурс] / Сургутский городской суд Ханты-Мансийского автономного округа - Югры. URL: http://surggor.hmao.sudrf.ru/ (дата обращения: 26.02.2023).

239. Приговор Якутского городского суда Республики Саха (Якутия) по уголовному делу № 1—577/2020 от 27 апреля 2020 г. [Электронный ресурс] / Якутский городской суд Республики Саха (Якутия). URL: http://jakutsky.jak.sudrf.ru (дата обращения: 16.02.2023).

240. Решение Волгодонского районного суда по гражданскому делу № 2—4140/2018 от 18 марта 2019 г. [Электронный ресурс] / Волгодонский районный суд Ростовской области. URL: http://volgodonskoy.ros.sudrf.ru/ (дата обращения: 21.11.2022).

ПРИЛОЖЕНИЕ

Приложение 1

Интернет-сайты-обозреватели

В телекоммуникационной сети Интернет существуют так называемые сайты-обозреватели, с помощью которых можно отслеживать различные криптовалютные транзакции в блокчейне.

К примеру:

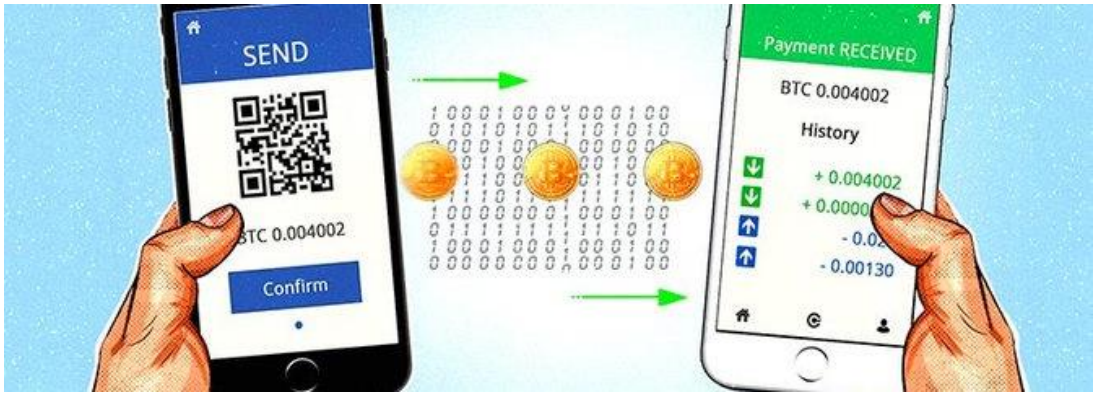
Blockchain.com (криптовалюты ETH, BCH, BTC);

Bitcoin.com (криптовалюты BCH, BTC);

BlockExplorer (криптовалюты ZEC, BCH, BTC);

BlockCypher (криптовалюты DASH, Doge, LTC, Grin, BTC).

Такого рода сайты существуют для необходимости проверки факта отправки криптоперевода, то есть перечисления криптомонет с одного криптокошелька на другой, как схематично представлено на рисунке.



Криптовалютная транзакция

Такого рода проверка может быть непосредственно осуществлена любым желающим с помощью сайтов-обозревателей, в том числе вышеуказанных. При этом необходимо знать либо хеш транзакции либо адрес, с которого был осуществлен перевод, либо идентификатор транзакции (TXID).

TXID представляет из себя криптографически защищенный 64-символьный код, который состоит из определенной последовательности букв и цифр. Такой код генерируется индивидуально для каждой криптовалютной транзакции после ее формирования и содержит информацию о ней.

Передача TXID третьим лицам вполне безопасна, так как вся персональная информация криптографически зашифрована, без возможности восстановления исходных данных.

Таким образом, для отслеживания криптовалютной транзакции следователю необходимо получить сведения о хеш транзакции или электронном адресе, с которого был осуществлен перевод, либо TXID. Такого рода сведения могут быть получены в результате допроса потерпевшего, либо свидетеля.

Для того чтобы отследить криптовалютную блокчейн-транзакцию необходимо:

1. Зайти на сайт обозревателя транзакций.

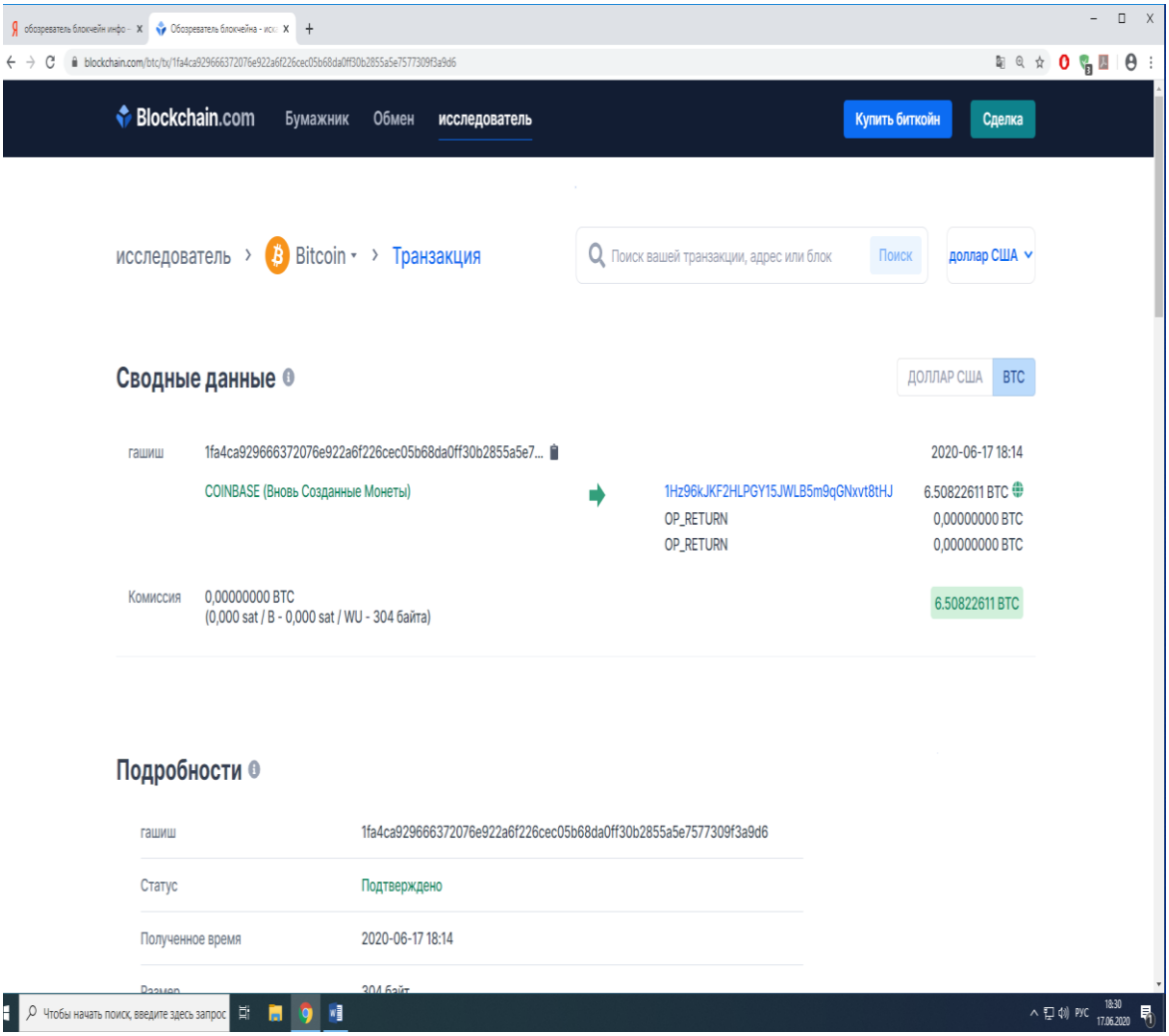
2. В верхней части интерфейса, в поле поиска, вводим хеш транзакции либо адрес, с которого был осуществлен перевод, либо идентификатор транзакции (TXID).

3. Выбираем необходимый блокчейн.

4. Нажимаем «Поиск» и отслеживаем транзакцию в блокчейне.

Таким образом, при помощи вышеуказанных сервисов, можно узнать, на каком этапе находится отправленная блокчейн транзакция, и получить полные данные по данной транзакции.

Так, например, транзакции с определенными видами криптовалют отражаются в обозревателе https://blockchain.info/search, что видно на представленном ниже скриншоте.



Эксплорер Blockchain.com

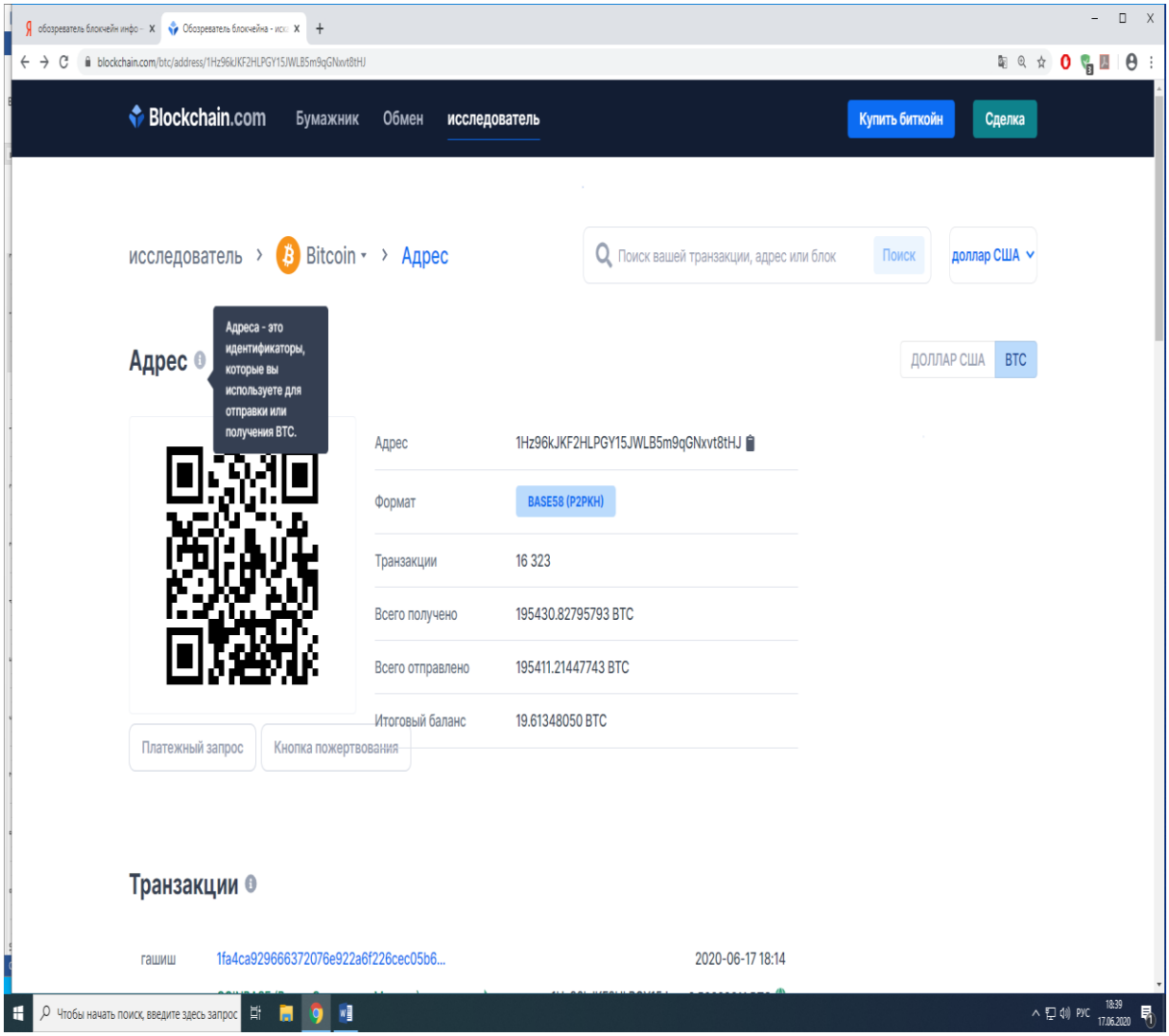
Любая криптовалютная транзакция состоит из трех элементов: вход, выход и сумма.

Вход транзакции — представляет собой электронный адрес, с которого осуществляется отправка данных (криптомонет).

Выход транзакции — это электронный адрес, на который такие данные (криптомонеты) поступают.

И, наконец, сумма, то есть количество отправленных криптомонет.

Таким образом можно идентифицировать определенную криптовалютную транзакцию, увидеть электронный адрес отправителя (на скриншоте ниже) и далее по IP-адресу устройства определить его местонахождение, а по данным провайдера определить владельца.



Эксплорер Blockchain.com

Так как сеть биткоина является публичной, любой желающий может просматривать хранящиеся в ней транзакции. Для просмотра или проверки транзакции в биткойн блокчейне может использоваться практически любой универсальный обозреватель блоков. В настоящие время практически все обозреватели являются универсальными, то есть работают с несколькими видами криптовалют. Один из первых сервисов подобного рода — Blockchain.com (изначально Blockchain.info), о котором было сказано выше.

Имеются также и другие экспловеры, среди которых наиболее популярными являются BlockCypher, BTC.com, Blockchair и SoChain.

На примере SoChain, который позиционируется как один из самых быстрых экспловеров, можно рассмотреть процесс проверки транзакции в

блокчейне биткоина. Скорость обновления данных по транзакциям и блокам, представлены на главной странице эксплорера.

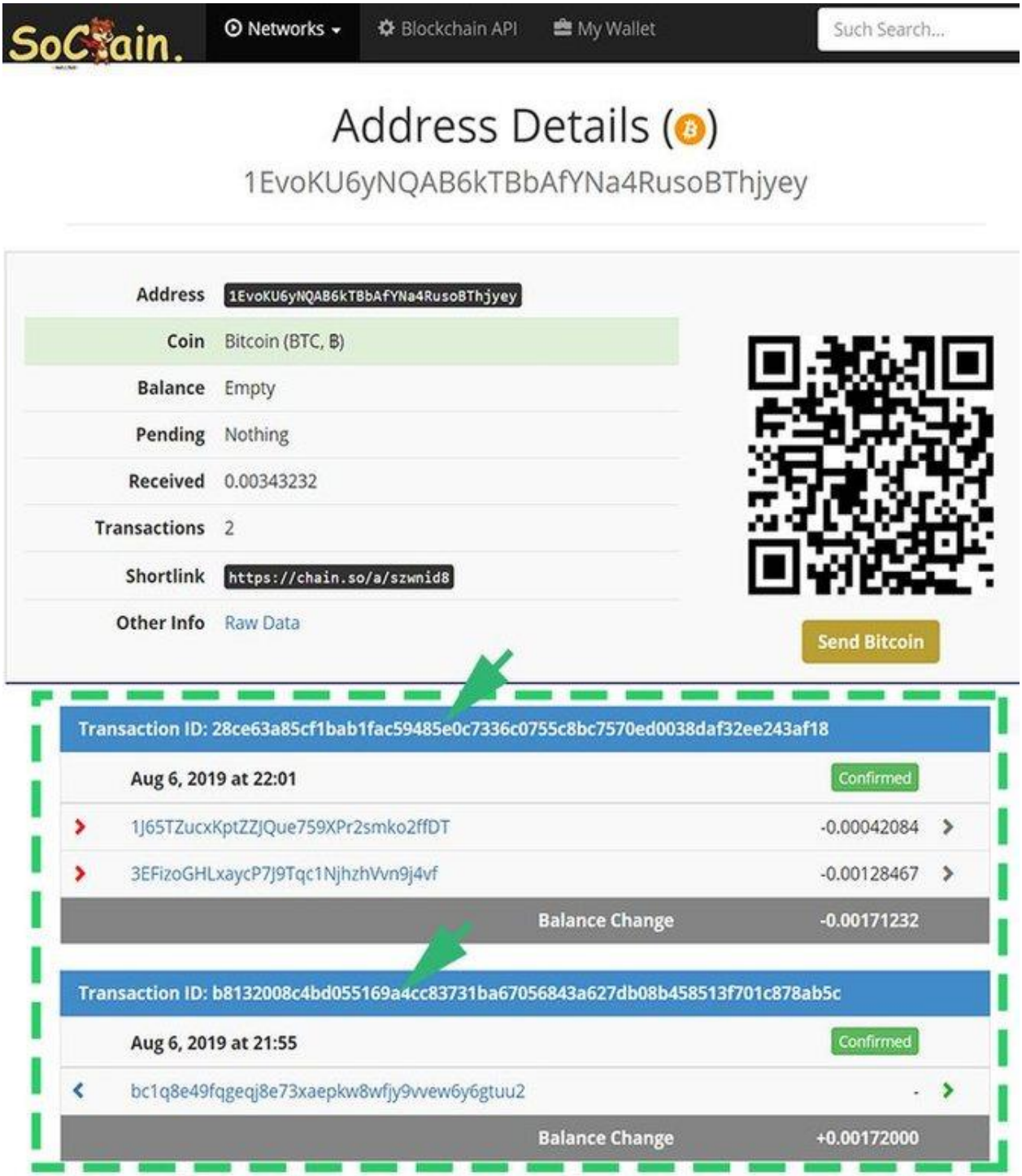
Для просмотра деталей отдельной сделки нужно ввести ее хеш (tx id) в соответствующее поле и нажать кнопку поиска.

Latest TX	Size	Sent (B)
...e3ce7265	0.20 kb	0.022174
...e566d479	0.22 kb	0.043618
...bfb480a7	0.52 kb	5.174001
...9df218d6	0.22 kb	0.000876
...d9b64243	0.14 kb	0.267139
...989306da	0.20 kb	0.138800
...4153b97c	0.81 kb	0.001041
...e4c127f2	0.81 kb	0.043059
...7cfb0274	0.22 kb	18.041768
...984be6b9	1.32 kb	1.995961

Block #	Age	Miner	Transactions	Size
589,000	4 minutes	bc1qjl8u...	2,612	1,058.70 kb
588,999	14 minutes	ViaBTC	3,038	1,186.73 kb
588,998	29 minutes	1Hi8WYJ9...	2,025	797.05 kb
588,997	37 minutes	F2pool (Discus Fish)	2,214	860.49 kb
588,996	about an hour	1Cb4X74M...	1,513	1,237.49 kb
588,995	about an hour	ViaBTC	3,010	1,225.79 kb
588,994	about an hour	1C81BGyi...	1,340	449.09 kb
588,993	about an hour	ViaBTC	2,017	725.06 kb
588,992	about an hour	1MvYASoH...	516	205.38 kb
588,991	about an hour	F2pool (Discus Fish)	1,778	609.70 kb

Главная страница эксплорера SoChain.

В случае когда идентификатор перевода неизвестен, можно вместо него указать биткоин-адрес отправителя (если речь идет о биткоине) либо получателя и в его списке истории транзакций указать нужную, определив ее по переводимой сумме, кликнув на нее стрелкой мышки.



Поиск транзакции в BTC-аккаунте через эксплорер SoChain

В открывшемся окне будут представлены все хранящиеся в сети детали транзакции, обновляющиеся в реальном времени:

Хеш;

Номер блока включения;

Время и дата обработки транзакции;

Статус (подтвержденная/неподтвержденная);

Количество подтверждений, входов и выходов;

Пересылаемая сумма в BTC;

Комиссия за проведение сделки;

Вес транзакции в байтах;

Адреса отправителя и получателя;

Скрипты с подписью инициатора операции и прочими данными.

Независимо от выбора эксплорера для проверки транзакций в блокчейне, в каждой из них будут содержаться данные, аналогичные вышеперечисленным. Разница может быть только в порядке и визуальном отображении параметров.

Далее с участием владельцем устройства должны быть проведены необходимые следственные мероприятия, направленные на выяснение обстоятельств, совершенного преступления. К таким следственным действиям можно отнести допрос владельца компьютерного оборудования, с которого был осуществлен вход в сеть блокчейн.

Приложение 2

Автоматизированные информационные системы (АИС)

Необходимую помощь в выявлении лиц, совершивших преступления с использованием блокчейн-технологий могут оказать автоматизированные информационные системы (АИС).

Можно дать типичное определение, раскрывающие понятие информационной системы как взаимосвязанной совокупности средств и методов, которые используются для хранения, обработки и выдачи информации в интересах разрешения поставленной задачи.

Соответственно автоматизированная информационная система (АИС) предполагает возможность работы с полученными данными в автоматическом режиме.

Использование АИС ориентирована на определенную предметную область человеческой деятельности, то есть применяется для решения проблем имеющую определенную специфику.

В данном случае речь идет о криминалистике. То есть использовании АИС для построения логических информационных связей между определенным событием произошедшем в виртуальном пространстве с лицами, которые могут быть причастны к его совершению.

При этом доказательства, полученные при использовании таких АИС, могут использоваться при осуществлении квалификации соответствующих преступлений.

В данном случае автоматизированная информационная система (АИС) должна представлять из себя комплекс, который включает компьютерное и коммуникационное оборудование, программное обеспечение, лингвистические средства, информационные ресурсы, а также системный персонал, обеспечивающий поддержку динамической информационной

модели некоторой части реального мира для удовлетворения информационных потребностей пользователей и для принятия решений.

Такие системы призваны, аккумулировать и обрабатывать разнообразную криминалистическую и оперативно-розыскную информацию.

Следует отметить неоспоримое преимущество автоматизированных информационно-поисковых систем при анализе связей между различными сегментами информации.

Получение необходимой информации из различных источников, ее систематизация и анализ требуют больших временных затрат. Эта задача становится еще более сложной, если речь идет о различных источниках информации внешне друг с другом не связанных.

К такой информации относиться нахождение определенного лица в мире виртуальном, то есть совершение им действий в виртуальном пространстве к которой естественно относиться и блокчейн, и его нахождение в мире реальном, то есть нахождение в определенной географической точке. Именно для совмещения этих сегментов информации и используются АИС.

С использованием информационно-поисковых систем задача быстрого подбора необходимой информации и дальнейшее построение логических связей значительно упрощается.

Такие автоматизированные информационно-логические системы (АИЛС) предназначены для решения на основе систематизированной информации различного вида логических задач. В результате работы таких систем происходит не только поиск необходимой при решении задач информации (как в информационно-поисковых), но и с помощью определенных логических процедур синтез новых сведений, не содержащихся явно в отобранной информации, то есть построение логических связей между, казалось бы, разнородными массивами информации, то есть решать задачи анализа информации.

Так в данном случае можно говорить о том, что АИЛС может в автоматическом режиме собирать данные соответствующего эксплорера,

биллинга, то есть информации об использовании телекоммуникационных услуг определенным абонентом, данные об IP-адресе компьютерного оборудования используемого пользователем блокчейн-сети и анализировать данную информацию на предмет их взаимосвязи.

Кроме того системы, в которой реализованы определенные логические алгоритмы, можно назвать автоматизированной системой информационного обеспечения (АСИО).

Такие системы выдают методические описания и рекомендации по расследованию преступлений.

Так лицо совершающие указанные преступления выбирает один из следующих вариантов поведения:

1. Совершает преступления с использованием блокчейн-технологий, в которых предметом преступного посягательства является криптовалюта. Такие преступления в свою очередь можно разделить на две группы:

Это преступления, совершаемые с использованием технических средств.

К другой по механизму совершения преступления группе можно отнести преступления так называемой «общеуголовной направленности».

К таковым можно отнести преступления против жизни и здоровья потерпевшего, целью которых является завладение криптовалютой.

Так, например, по сообщению таиландского информационного издания Phuket Gazette от 18.01.2018, со ссылкой на национальную полицию, в Таиланде двое россиян стала жертвами группы преступников, которые, угрожая применением насилия путем насильственного введения им наркотического средства с последующей передачей для привлечения к уголовной ответственности полиции Тайланда, получили от потерпевших пароль от их криптокошелька, завладев принадлежавшей потерпевшим криптовалютой «Биткоин» на сумму эквивалентную 100 000 Евро, путем перечисления криптомонет на кошелек преступников. Аналогичные преступления совершаются и на территории Российской Федерации.

Также по механизму совершения преступлений можно выделить группу преступлений, в которых криптовалюта является фактическим средством оплаты.

При этом необходимо констатировать, что на сегодняшний день большинство товаров, реализуемых за криптовалюту, запрещены или ограничены в гражданском обороте. Это наркотические или сильнодействующие вещества, оружие, поддельные документы или деньги.

Так, например, если, с помощью популярного сегодня «TOR»-браузера зайти в онион (onion) зону, то можно обнаружить большое количество такого рода интернет-магазинов (интернет-площадок), торгующих товарами подобного рода или принимающих заказы на сомнительные услуги, типа: «продаем удостоверения МВД, ФСБ, СК России, Прокуратуры Российской Федерации, Росгвардии, судьи, адвоката». И это не самое криминальное, но, пожалуй, наиболее часто встречаемое объявление.

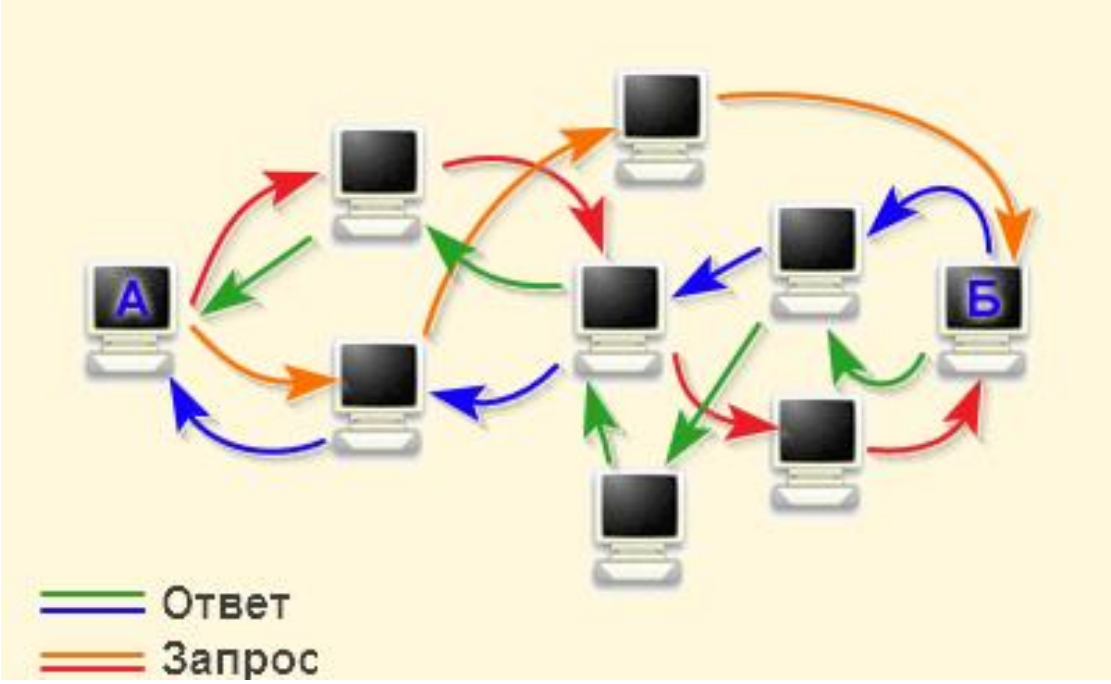
У подобного рода интернет-магазинов существует свой рейтинг и свои интернет-форумы, где покупатели в сети Даркнет обмениваются друг с другом информацией о надежности того или иного продавца и качестве приобретенного ими товара или оказанной услуги.

При этом местоположение и IP-адрес onion-сервиса скрыты, вследствие чего гораздо труднее его блокировать или идентифицировать владельца.

Весь осуществляемый между пользователями «Tor» и onion-сервисами трафик защищен сквозным шифрованием, а адреса onion-сервиса генерируется автоматически.

Соответственно, оплата приобретаемого товара в интернет-магазинах подобного рода осуществляется путем криптовалютных перечислений с крипто-кошелька покупателя на крипто-кошелек продавца. В свою очередь доставка покупателю оплаченного подобным образом товара осуществляется либо путем «закладок», то есть оставления приобретенного товара в определенном месте, предварительно согласованного с покупателем, либо путем почтовых отправлений на абонентский ящик покупателя.

При этом если доступ к сети «Тор» будет заблокирован интернет-провайдером, то «Тор»-браузером предусмотрены определенные инструменты (подключаемые транспорты) для обхода таких блокировок, которые свободно можно найти на сайте Tor Browser.



Общая схема функционирования сетей «Даркнет».

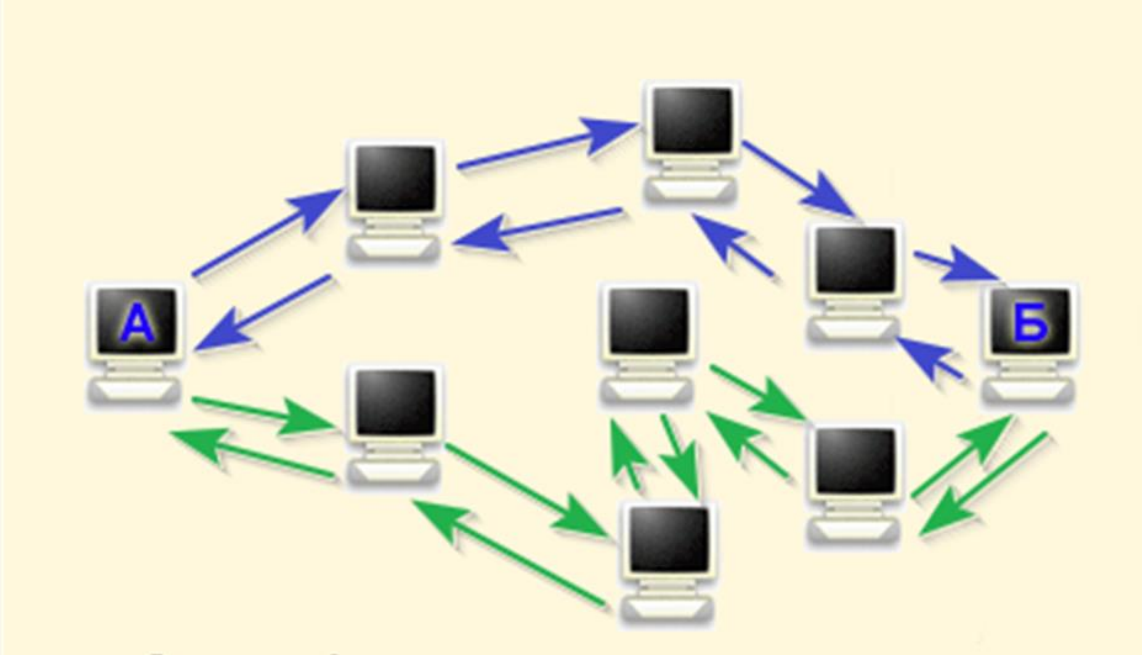


Схема передачи данных в сети «Tor».

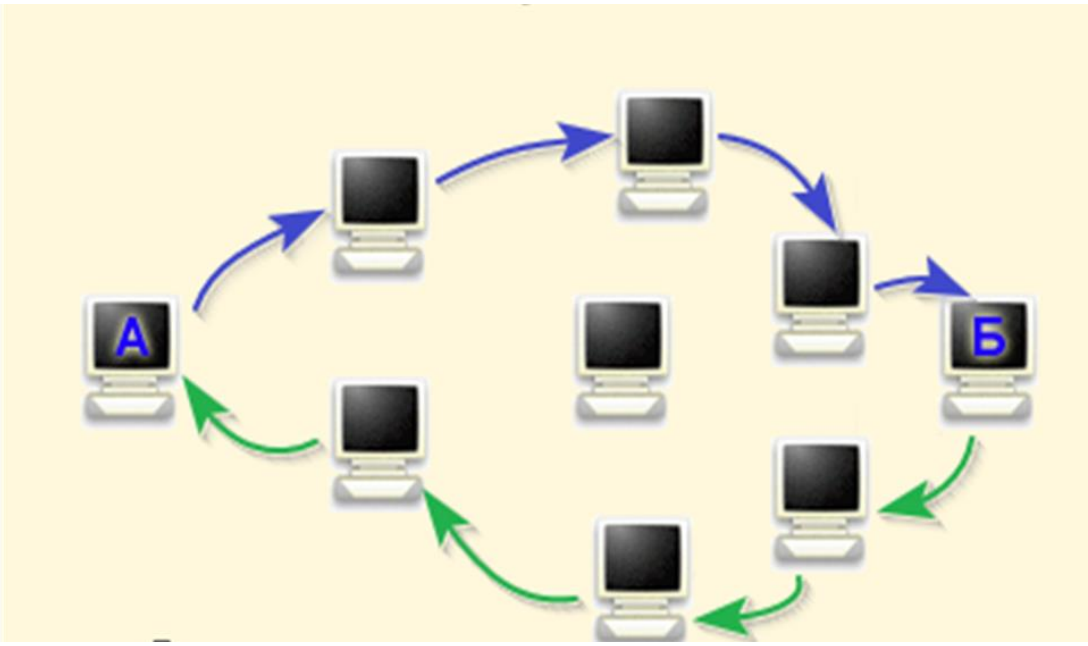


Схема передачи данных в сети «I2P».

Также нередки случаи хищения криптомонет из криптокошельков, совершаемые как путем банального фишинга (разновидности интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей, то есть определенным логинам и паролям, с помощью которых можно получить доступ к чужому счету и произвести перечисление денежных средств, применительно к данному случаю криптовалюты), так и путем автоматического подбора соответствующего ключа, осуществляемого ботом (роботом). При этом в каждом конкретном случае от метода, которым было совершено то или иное преступление, зависит его юридическая квалификация.

К сожалению, в настоящий момент можно говорить о том, что выявляются, пресекаются и расследуются преступления, в которых криптовалюта фактически является средством платежа, но не преступления, в которых криптовалюта выступает в качестве предмета преступного посягательства.

Как правило, такие преступления выявляются и пресекаются на стадии, когда покупатель уже получил доставленное ему почтой специальное отправление (посылку, бандероль) или попытался в заранее оговоренном

месте взять оставленную для него «закладку». При этом незаконное приобретение товара фиксируется, а покупатель незаконно приобретший указанный товар как правило задерживается и в отношении него возбуждается уголовное дело. Также имеют место случаи задержания и привлечения к уголовной ответственности так называемых «закладчиков», то есть лиц, непосредственно осуществляющих в специально оговоренном с покупателем месте закладку ограниченного или запрещенного в гражданском обороте товара.

При всем этом к ответственности чаще всего привлекаются лишь исполнители преступления, а организаторы продолжают руководство преступным сообществом, осуществляющим незаконный сбыт товаров, запрещенных или ограниченных в гражданском обороте, в том числе наркотических средств и сильнодействующих средств, оружия, боеприпасов, поддельных документов

Такое положение дел существует по двум причинам.

Во-первых, до конца все-таки не определен правовой статус криптовалюты на территории Российской Федерации, о чем может косвенно свидетельствовать внесение Министерством финансов Российской Федерации 18.03.2022 в Правительство Российской Федерации законопроекта о регулировании криптовалют. Данный проект был разработан по поручению Правительства Российской Федерации на основе утвержденной концепции регулирования механизма организации оборота цифровых валют, что в свою очередь свидетельствует о необходимости конкретизации ее правового статуса в национальной правовой системе и упорядочения контроля за ее оборотом.

Во-вторых, отсутствие единообразного понимания квалификации данных преступлений, что имеет прямую связь с первой причиной.

Таким образом, на сегодняшний день складывается достаточно парадоксальная ситуация, при которой преступления с использованием криптовалюты продолжают совершаться, но какого-либо доступного и

эффективного способа их выявления и квалификации не существует. Уже само по себе отсутствие адекватного противодействия совершаемым преступлениям приводит к увеличению количества таких преступлений, и порождает иллюзию безнаказанности и вседозволенности у лиц их совершающих.

Объявления о сделках с криптовалютой возле станции метро «Шоссе Энтузиастов» г. Москвы.

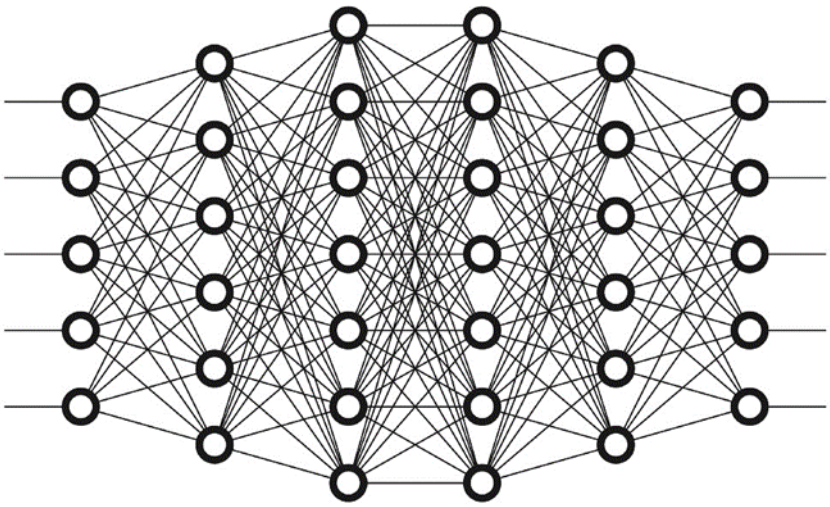
Также к преступлениям подобного рода можно отнести и часть преступлений, предусмотренных главой 30 Уголовного кодекса Российской Федерации «Преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления», то есть так называемые «должностные преступления», ответственность за совершение которых предусмотрена статьями 290 (получение взятки), 291 (дача взятки), 291^1 (посредничество во взяточничестве) Уголовного кодекса Российской Федерации, если предметом взятки является та или иная криптовалюта, которая впоследствии легко может быть обменена на фиатные деньги.

На сегодняшний день не существует единого мнения относительно наиболее эффективных способов выявления преступлений, совершаемых с использованием криптовалюты, последующей их квалификации и расследования такого рода уголовных дел.

Таким образом, принимая во внимание определенный уровень анонимности использования криптовалют, необходимо определить те границы, где указанная анонимность заканчивается и начинаются так называемые «точки доступа» к персональным данным определенного лица, совершающего криптовалютные операции, нарушающие требования национального законодательства.

Учитывая, что криптокошельки как правило являются анонимными, одной из таких «точек доступа» может являться операция по обмену (купле-продаже) той или иной криптовалюты на фиатные деньги. Именно при совершении данной операции, осуществляемой путем зачисления фиатных денежных средств на банковский счет (списания со счета) лица, продавшего (приобретшего) криптомонеты, появляется возможность установить участника такой сделки или по крайней мере лицо, действующее в его интересах или с ним связанное определенными отношениями.

Второй «точкой доступа», хотя и не всегда позволяющей точно персонифицировать лицо, совершающее противозаконные сделки с криптовалютой, но при этом все же позволяющей сделать относительно определенные предположения относительно такого лица, является комплексный анализ информации о связях анонимного лица с уже ранее реально установленными лицами, а также анализ информации анонимных и реальных лиц, в том числе в телекоммуникационной сети Интернет.



Образец блок-схемы транзакций блокчейн.

Для этой цели могут быть успешно использованы как компьютерные программы для построения диаграммы связей, так и схемы, построенные экспертом-аналитиком. Конечно, наиболее эффективным будет являться комплексный подход с использованием аналитических знаний человека и возможностей вычислительной машины.

Комплексное использование двух указанных способов на сегодняшний день является наиболее эффективным средством выявления преступлений, совершаемых с использованием криптовалюты, как элемента блокчейн-технологий и источником доказательств, необходимым для квалификации таких преступлений и расследования соответствующих уголовных дел. Такая методика основывается на практике выявления лиц, совершаемых преступления с использованием криптовалюты, апробированной ФБР США, и системы криминалистических учетов, используемых в СССР. Именно такая автоматизированная информационная учетная программная система (АИС) должна быть использована для упорядочения по определенным признакам сведений, иметь общие принципы описания, хранения и манипулирования такими данными.

Другой вид АИС представляет собой системы, осуществляющие поиск определенной информации (об определенном лице) в телекоммуникационной сети Интернет и установления его возможных связей.

Приложение 3

Криптокошельки

Локальные криптокошельки хранятся в виде программы на персональном компьютере пользователя. Пользователь лично устанавливает характеристики безопасности для такого кошелька и хранит соответствующий файл с ключами также на своем персональном компьютере. Соответственно, такой кошелек может быть использован только на определенном персональном компьютере и занимает на нем достаточно много пространства из-за того, что хранит все цепочки блоков транзакций, однако за счет этого обладает достаточно высокой безопасностью.

Мобильные криптокошельки, в отличие от кошельков локальных, не требуют скачивания всех блоков, подкачивая их по мере необходимости с других, сторонних серверов, что позволяет занимать значительно меньше места и использовать их на портативных, переносных устройствах, таких как планшетные компьютеры, смартфоны. Данное обстоятельство предоставляет их владельцу возможность мобильного использования такого кошелька.

Но, выигрывая в мобильности, такие кошельки менее безопасны, так как при использовании дополнительных серверов появляется возможность передачи информации другим лицам.

Онлайновые криптокошельки схожи с мобильными тем, что также частично подгружают блоки с иных серверов и при этом файл с ключами такого кошелька хранится на определенном сервере, что также предоставляет определенную мобильность использования, но за счет снижения безопасности, так как доступ к такому кошельку можно получить с любого устройства к нему подключенного.

Как уже было указано выше к отдельной группе относятся так называемые аппаратные крипто-кошельки представляющий из себя отдельное устройство, например, обычную флеш-карту или иную микросхему, которая через USB-вход соединяется с персональным компьютером и хранит в себе

необходимые секретные ключи. Таким образом, указанный криптокошелек сочетает в себе безопасность и мобильность использования, но при отсутствии резервной копии делает невозможным использование криптокошелька при утрате данного устройства, то есть его механической составляющей.

Учитывая, что оборот криптовалюты происходит в виртуальном пространстве безопасность использования любого криптокошелька, ее хранящего является насущной необходимостью.

Считается, что существует три способа защиты файла с ключами криптокошелька. Это шифрование данных при помощи пароля, резервное сохранение данных и выведение криптокошелька в оффлайн, так называемое «холодное хранение данных».

Любое шифрование данных обеспечивает дополнительную безопасность. Но, к сожалению, шифрование предполагает возможность дешифровки, вследствие чего безопасность будет зависеть именно от сложности такого шифрования.

Резервное копирование данных поможет их восстановлению после их возможного повреждения или уничтожения, равно как и их оффлайн хранение.

При использовании аппаратных кошельков необходимость резервного копирования данных обусловлено также невозможностью использовать кошелек при потере его механической части при отсутствии соответствующей копии данных на ней хранившихся.

При регистрации программного криптокошелька необходимо соблюдать определенные правила, позволяющие повысить уровень его безопасного использования. Необходимо указывать свой личный адрес электронной почты для получения письма с подтверждением регистрации. Доступ к такому почтовому ящику иных лиц должен быть полностью исключен.

Следует использовать пароль, содержащий не менее десяти символов, содержащий как прописные, так и заглавные буквы, цифры и специальные символы. Такого рода комбинация значительно повышает надежность

придуманного пользователем пароля. Записанный на бумажный или электронный носитель пароль следует хранить в недоступном для иных лиц месте, исключающем его утрату или возможность копирования другими лицами.

Также для повышения безопасности пользования криптокошельком можно использовать так называемую двухфакторную аутентификацию (2FA), например, ввод пароля и телефонный звонок или смс-подтверждение входа.

Для установки программного криптокошелька необходимо использовать сайты, предоставляющие возможность с использованием специальной фразы восстановить доступ к криптокошельку в случае утраты пароля, иначе все крипто-монеты, хранящиеся в таком кошельке, будут для пользователя утрачены безвозвратно.

На сегодняшний день наиболее защищенными следует считать все же аппаратные криптокошельки, исходя из вышеуказанного принципа их работы. В сети Интернет на сайтах, посвященных криптовалюте биткойн, таких, например, как http://bebitcoin.com, http://bitcoin-s.info и многих других, можно найти информацию о наиболее популярных на сегодня аппаратных кошельках.

Наиболее популярные марки и краткое описание:

«Trezor» – назван одним из самых популярных аппаратных кошельков для криптовалюты биткойн и является первым, который начал поставляться покупателям – еще в 2013 году. Известность он также получил благодаря тому, что его разработку возглавлял известный под ником «slus» чешский программист Марек Палатинус (Marek Palatinus) – разработчик концепции группового майнинга. Данный криптокошелек снискал хорошую репутацию и имеет оптимальное сочетание функциональности и безопасности транзакций.

Размер кошелька немного превышает размер кредитной карты. «Trezor» подключается по порту USB, имеет OLED-дисплей для управления и дополнительного подтверждения платежа. Поставляется в пластиковом или алюминиевом корпусе. Закрытые ключи защищены шифрованием и паролем.

Есть функция резервного копирования и удаленного стирания информации при утере кошелька.

Защита PIN-кодом реализована достаточно оригинально – при вводе неправильного пароля время ожидания запуска устройства увеличивается в два раза. Доступных вариантов PIN-кода более 6000, что делает его прямой подбор практически невозможным.

Компания постоянно работает над улучшением системы безопасности, надежность «Trezor» подтверждена независимыми тестами и опытом пользователей по всему миру.

Крипто-кошелек «Trezor».

«Bwallet» разработан на открытом программном обеспечении кошелька «Trezor» и фактически является копией оригинала. Новые версии программного обеспечения и настройки подойдут с сайта оригинала - MyTrezor.com. Каких-либо отличий, кроме внешнего вида и цены, от оригинальной версии нет.

Криптокошелек «Bwallet».

«BTChip HW-1» представляет собой смарт карту с USB-подключением и может использоваться для любой криптовалюты.

Для совершения транзакции карта вставляется в USB-порт и не требует установки дополнительных драйверов, все необходимое программное обеспечение содержится внутри устройства. Из браузеров наиболее совместим с Google Chrome, поддерживаются кошельки Green Address и Electrum.

Для подтверждения транзакции используется двухфакторная парольная защита, закрытые ключи всегда остаются на устройстве. При трех попыток ввода неправильного пароля может активироваться автоматическое стирание информации. При первой транзакции автоматически создается резервная копия информации со своим уникальным паролем.

Тем не менее рекомендуется использовать данный криптокошелек для хранения небольших сумм криптомонет из-за использования только парольной защиты, что не может считаться достаточно надежным. Кошелек подтверждает любую транзакцию после его подключения к компьютеру, то есть он должен быть сконфигурирован как доверенный, а это еще больше снижает безопасность платежей.

Крипто-кошелек «BTChip HW-1».

«Ledger Wallet», по утверждениям его разработчиков, является самым защищенным аппаратным кошельком для криптовалюты биткойн. Среди разработчиков такие компании, как BTChip, производитель описанного выше кошелька HW-1, и платежная криптосистема Chronocoin.

Устройство защищено по стандарту EAL5+, который используется в банковской сфере для защиты пластиковых и смарт-карт. Дополнительно разработаны оригинальные алгоритмы подтверждения транзакций и восстановления доступа к кошельку. «Ledger Wallet» может содержать несколько биткойн криптокошельков.

После подключения к USB-порту кошелек попросит пользователя придумать уникальный PIN-код и ввести специальную кодовую фразу, которая идет в комплекте с устройством и в сочетании с PIN-кодом позволяет восстановить кошелек и создавать неограниченное число публичных адресов и приватных ключей. Затем кошелек устанавливает специальный плагин для браузера Chrome, и пользователь получает доступ к функциям Ledger. Пользователь может хранить биткойны на предоставляемом компанией специальном депозитном счете.

Крипто-кошелек «Ledger Wallet».

В комплект «Ledger Wallet» входя две пластиковые карты, которые используются для подтверждения платежных транзакций. Платеж будет проведен, только в случае если пользователем введен пароль с одной из карт, что будет дополнительной мерой безопасности при использовании онлайн-кошельков или при удаленном контроле хакерами персонального компьютера.

Все пароли и ключи обрабатываются в защищенной операционной системе Ledger OS только внутри аппаратного кошелька.

Программное обеспечение разработано для операционных систем Windows, Linux, OS X, iOS и Android.

Комплект крипто-кошелька «Ledger Wallet».

«Pi Wallet» криптокошелек создан на основе популярного микрокомпьютера Raspberry Pi. В качестве устройства хранения используются сменные SD-карты. Это одна из немногих полностью автономных реализаций криптовалютного кошелька. Устройство подключается к сети через сеть интернет или опциональный Wi-Fi и работает на программном обеспечении Armory. Транзакции проводятся без передачи закрытых ключей.

В комплект криптокошелька «Pi Wallet» входят две SD-карты, одна из которых содержит резервную копию информации. Кроме Armory устройство может комплектоваться ОС Raspbian, что позволяет разработчикам создавать свои программные решения и конфигурации безопасности.

Крипто-кошелек «Pi Wallet».

Следует сказать, что существует множество иных марок аппаратных кошельков, находящихся либо в разработке, либо только поступающих на рынок и еще никоим образом себя не зарекомендовавших.

Для того, чтобы понять принцип работы и получить соответствующие навыки работы с криптокошельком рассмотрим работу с появившимся в 2015 году и активно продвигаемым на рынке, разработанным американской компанией KeepKey LLC аппаратным крипто-кошельком «Keepkey».

Криптовалютный кошелек «Keepkey».

Криптокошелек «Keepkey» поддерживает четыре криптовалюты - Bitcoin, Litecoin, Dogecoin и в последней своей версии Ethereum.

В комплект поставки входят: непосредственно крипто-кошелек «Keepkey», кабель USB длиной 1 метр с нейлоновой оплеткой, небольшая картонная карточка для записи секретной фразы, кожаный чехол для ее хранения, и краткое руководство по его использованию.

Кошелек и его аксессуары черного цвета, других оттенков пока не предусмотрено. Сам кошелек, черно-глянцевый с одной стороны и матово-серый с другой, имеет размеры 93x38x12 мм, разъем micro-USB на одном углу и одну круглую кнопку на противоположном. Дисплей в выключенном состоянии не виден. Корпус кошелька достаточно прочный, выполнен из анодированного алюминия, а передняя панель, прикрывающая дисплей – из поликарбоната.

Как указано на сайте производителя, криптокошелек работает на процессоре ARM Cortex M3 и использует аппаратный генератор случайных чисел TRNG. Разрешение экрана составляет 256x64 пикселя. Установки драйверов не требуется, кошелек распознается как USB HID, то есть интерфейсное устройство.

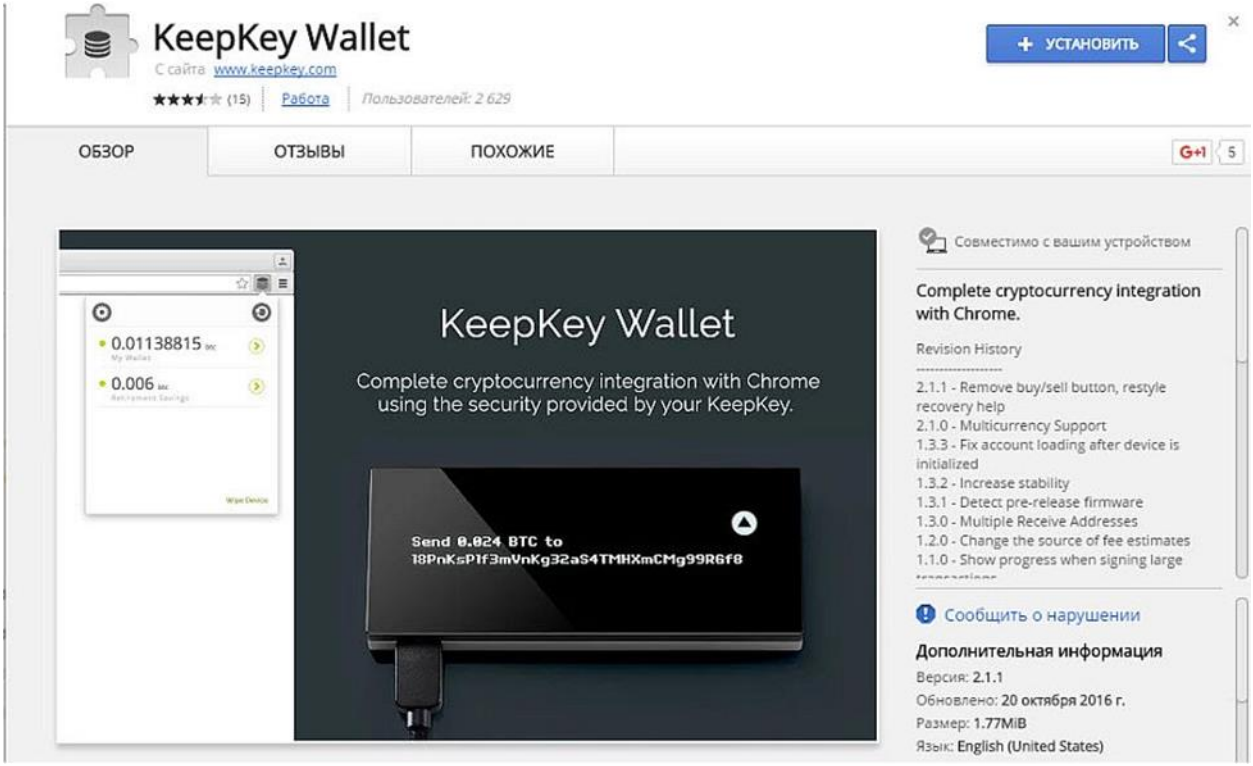
Программное обеспечение крипто-кошелька для Keepkey предназначено для работы с браузером Chrome через устанавливаемое расширение. Одно из расширений для Chrome – KeepKey Wallet – представляет собой так называемый «легкий» криптокошелек, позволяющий отправлять и получать крипто-монеты с использованием аппаратного кошелька в качестве хранилища закрытых и открытых ключей. С аппаратным кошельком можно осуществлять транзакции на любом устройстве. Второе – KeepKey Proxy – предназначено для работы с кошельков из браузера. На сегодняшний день поддерживается только Chrome.

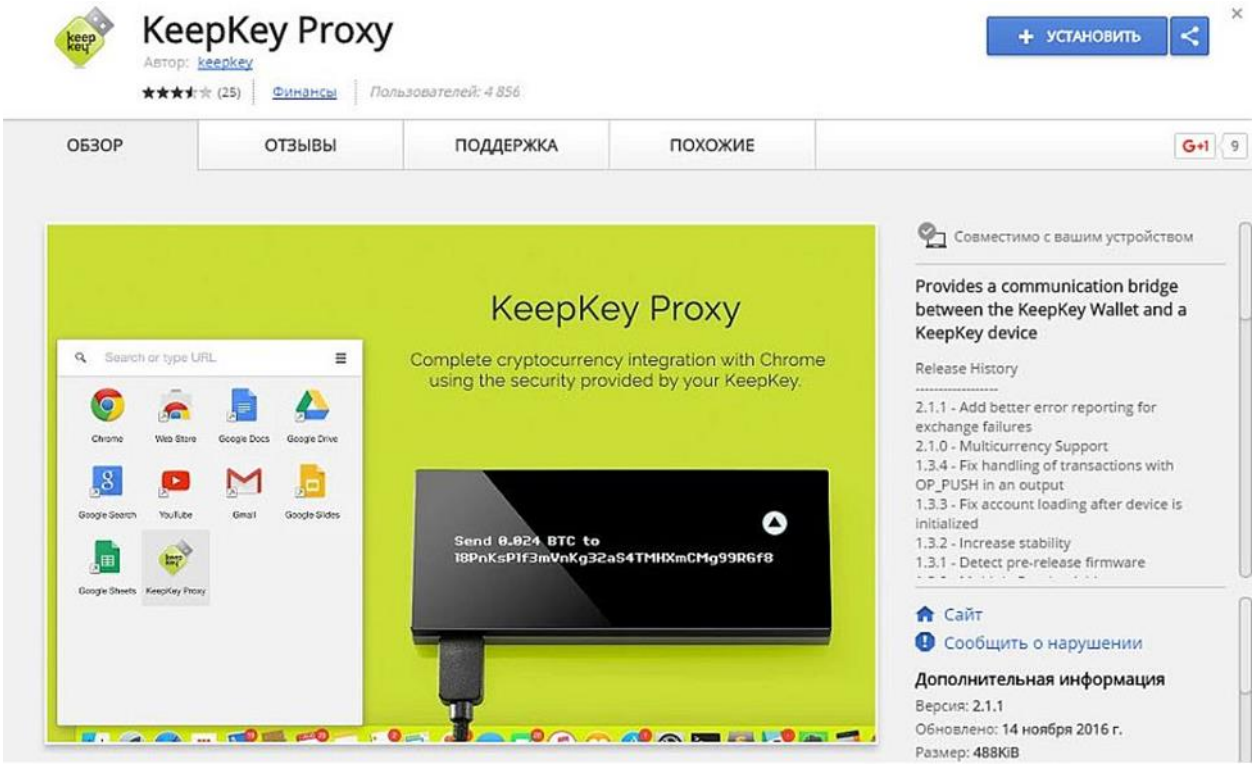
Использовать криптокошелек Keepkey возможно с помощью приложений от производителя в браузере Chrome, а также совместимых легких кошельков Electrum и Multibit, основанных на BIP32. С помощью

секретной фразы можно сгенерировать ключи также на любом другом устройстве, что является актуальным при потере или краже кошелька.

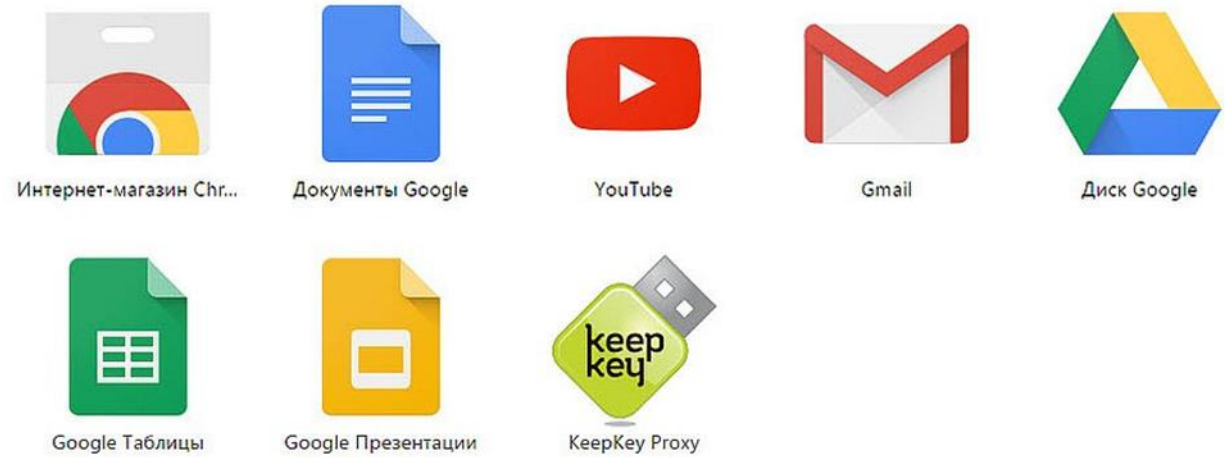
При включении аппаратного кошелька в разъем USB компьютера на экране кошелька, занимающего почти всю его длинну, появляется светящийся логотип KeepKey, который через некоторое время начинает медленно перемещаться по горизонтали слева направо.

После этого следует приступить к установке расширений в Chrome. Сразу же после установки KeepKey Wallet по клику по символе приложения в правом верхнем углу окна браузера, предлагается установить KeepKey Proxy. Поскольку они оба необходимы для работы без сторонних кошельков, можно было бы объединить установку в один пакет.

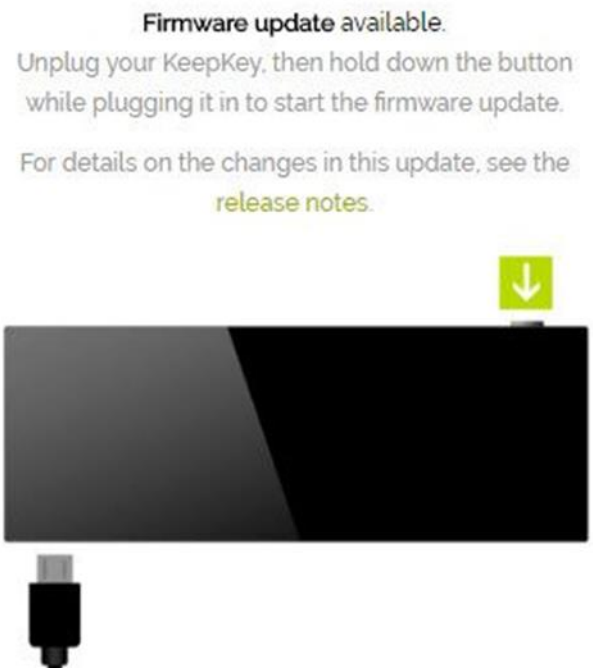




Установив приложения, в списке стандартных приложений Chrome, мы увидим и KeepKey Proxy. Нужно только кликнуть по нему, чтобы наконец оживить кошелек.



При первом подключении может быть предложено обновить прошивку (firmware) кошелька. Для этого необходимо отключить кошелек, и удерживая кнопку, подключить снова. После этого будет предложено запустить обновление, которое проходит в течение приблизительно минуты.



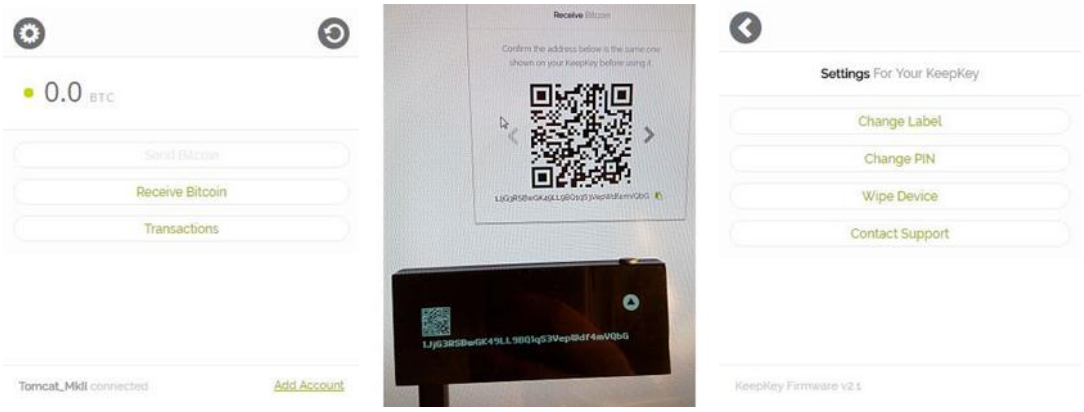
После обновления прошивки (если это произошло) следует приступить к инициализации кошелька, во время которой нельзя переключаться на другие приложения, совершать какие-либо иные действия, например, кликать мышью по экрану, иначе, придется начинать все сначала.

Сначала необходимо ввести метку криптокошелька, которая нужна только для удобства его распознавания, а также придумать ПИН-код из пяти цифр и два раза ввести его в веб-интерфейсе, причем расположение цифровых клавиш высвечивается на экране кошелька и каждый раз меняется для повышения безопасности. После ввода ПИН-кода кошелек выведет на экран двенадцать английских слов – это и есть кодовая фраза, привычная для всех пользователей легких и мобильных HD-кошельков. Эти двенадцать слов, не нарушая последовательности, необходимо списать на прилагаемую карточку или иной желательно бумажный носитель, который хранить в месте недоступном для иных лиц.

После записи секретной фразы необходимо удерживать кнопку крипто-кошелька до тех пор, пока не запустится процесс создания аккаунта и закрытых ключей. Если при этом переключится на иное приложение – окошко

исчезнет и весь процесс придется повторять. Приложение считывает данные с кошелька при каждом действии, и пока кошелек не инициализирован на нем ничего не сохраняется.

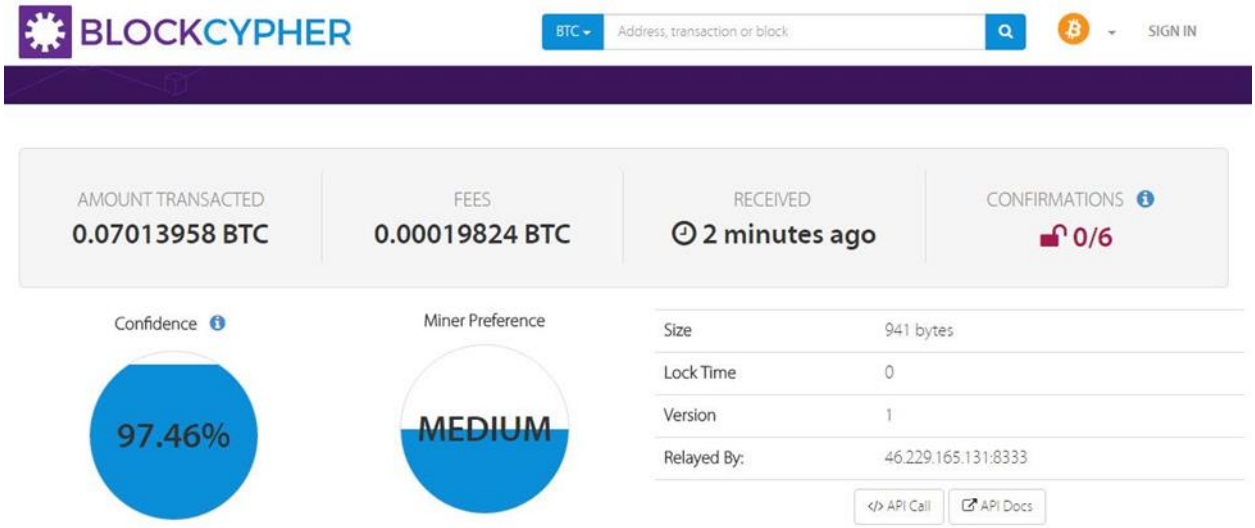
После инициализации появится простое меню приложения, через которое можно отправлять и получать крипто-монеты, а также изменить настройки. В настройках можно изменять метку, ПИН-код. Также можно полностью удалить все данные с кошелька. Добавить новый криптовалютный счет можно нажав на ссылку Add Account в нижней части первого экрана.



Для получения на кошелек именно биткойнов необходимо нажать кнопку «Receive Bitcoin», и будет получен адрес в виде текстовой строки и QR-кода. Стрелкой вправо можно прокрутить несколько адресов. При этом, на экране кошелька также высвечивается выбранный адрес – если злоумышленники взломают расширение Chrome и подменят адрес, то до кошелька они вряд ли доберутся.

Для отправки биткоинов с кошелька следует нажать «Send Bitcoin», ввести адрес получателя и отправляемую сумму. Берется рекомендованная динамическая комиссия за проведенную транзакцию.

После отправки транзакции на выбранный пользователем адрес она вскоре появляется в списке транзакций веб-интерфейса. Подробности транзакции показываются через сервис blockcypher.com.



Так как криптокошелек Keepkey во многом напоминает криптокошелек Trezor, так как оба этих кошелька базируются на одних и тех же стандартах – BIP32 и BIP44 освоившим работу с Keepkey смогут также работать с Trezor.

Стоит отметить, что аппаратные криптокошельки являются достаточно молодым сегментом рынка, вследствие чего большинство таких устройств находятся в стадии разработки или экспериментального применения и опыт их практической эксплуатации пока еще не велик. Их удобно носить с собой, то есть они предоставляют своему владельцу определенную мобильность в их использования и осуществления платежей практически из любой точки мира, в которой они находятся, конечно при условии наличия сети интернет и компьютера или переносного мобильного устройства к ней подключенных.

При этом учитывая небольшие размеры аппаратных кошельков и возможность их мобильного использования они легко могут быть утеряны, а восстановить их без резервной копии невозможно. Поэтому обязательную резервную копию необходимо хранить на устройстве без доступа в сеть, например, на флеш-карте, которая в свою очередь должна храниться в месте

исключающей ее утрату и обеспечивающим невозможность доступа к ней посторонних лиц.

Приложение 4

Принципы работы блокчейн

Обратимся к статье Сатоши (Сатоси) Накамото, в которой он описывает принцип работы сети и которая заслуживает того, чтобы каждый, кто интересуется проблематикой, связанной с криптовалютой, прочитал её полностью. Но мы отметим и некоторые непонятные и спорные вопросы, на которые С. Накамото ответа пока не дает.

Так, например, С. Накамото пишет: «Для компенсации возрастающей вычислительной мощи процессоров и колебания числа работающих узлов в сети, сложность хэширования должна изменяться, чтобы обеспечивать равномерную скорость генерации блоков. Если они появляются слишком часто – сложность возрастает, и наоборот». Здесь сразу возникает ряд вопросов: кто (что) определяет уровень сложности хэширования и по какому критерию он изменяется, тем более что процесс майнинга, в общем, случайный?

«Система работает по следующим правилам: Новые транзакции рассылаются всем узлам. Каждый узел объединяет пришедшие транзакции в блок. Каждый узел пытается подобрать хэш блока, удовлетворяющий текущей сложности. Как только такой хэш найден, этот блок отправляется в сеть. Узлы принимают этот блок, только если все транзакции в нем корректны и не используют уже потраченные средства. Здесь тоже возникает вопрос о том, как сеть осуществляет выбор решения, где конкретно, на каком сервере (а сеть всемирная) принимается окончательное решение?

Свое согласие с новыми данными узлы выражают, начиная работу над следующим блоком и используя хэш предыдущего в качестве новых исходных данных. Здесь тоже возникает вопрос, каким образом идет

синхронизированное распределение данных по сети от центра, принявшего решение?

Участники всегда считают истинной самую длинную версию цепочки и работают над ее удлинением. Если два узла одновременно опубликуют разные версии очередного блока, то кто-то из остальных пиров получит раньше одну версию, а кто-то – другую. В таком случае каждый начнет работать над своей версией цепочки, сохранив другую на случай, если она будет продолжена раньше. Двойственность исчезнет, как только будет получен новый блок, который продолжит любую из ветвей, и те узлы, что работали над конкурирующей версией, переключатся на нее. Но что делать, если в каждую ветвь придет новый блок от разных узлов? Блокчейн раздвоится? Или кто-то волевым решением рано или поздно отменить «слабую» ветвь? Тогда кто? Крайне важно, чтобы правила, применяемые для подтверждения транзакций нодами пользователей, не противоречили правилам, применяемым большинством майнеров. Если кто-то из майнеров включает в блок транзакции, отвергаемые другими нодами, то весь блок будет считаться данной нодой ошибочным. Если эта нода является майнером, это может привести к двойным тратам и раздвоению блокчейна.

Новые транзакции не обязательно должны достигать всех узлов (то есть предыдущий случай возможен?). Если о них будет знать достаточно много узлов (сколько конкретно в количестве или процентах?), вскоре они попадут в один из блоков. Правила рассылки блоков тоже не являются строгими в отношении потерянных сообщений. Как только узел, пропустивший один из блоков, получит уже следующий за ним, он запросит недостающую информацию, чтобы заполнить очевидный пропуск»[170].

Таковы основные правила и возможности функционирования сети блокчейн.

---

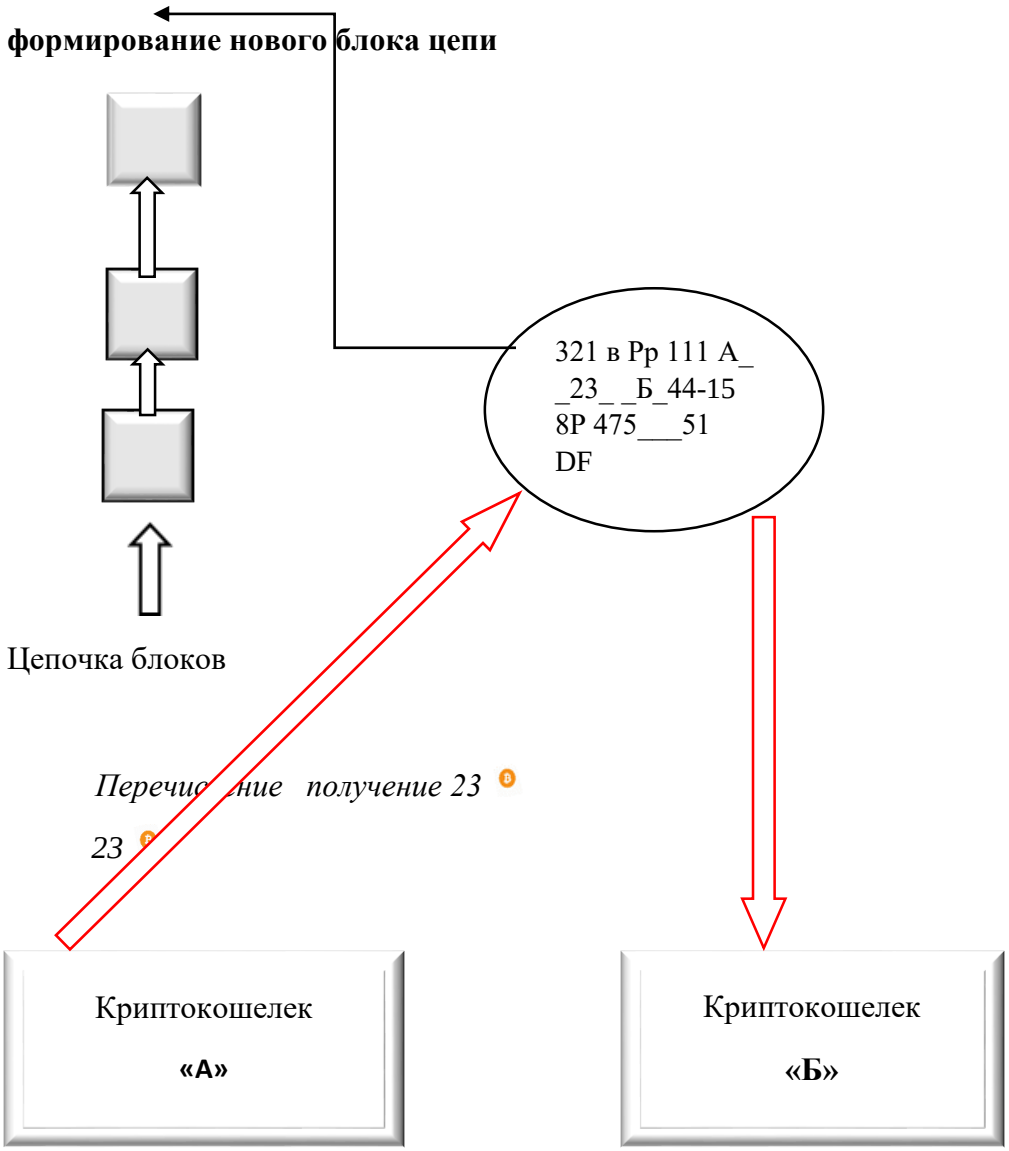
[170] Накамото С. Биткойн: система цифровой пиринговой наличности. Режим доступа: https://opartnerke.ru/wp-content/uploads/2017/12/belaya_kniga_bitcoina_satoshi_nakamoto.pdf (дата обращения - 02.02.2021).

Теперь остановимся еще на одном важном вопросе функционирования блокчейн, каковым является алгоритм отбора транзакций для их дальнейшей обработки.

Необходимо отметить, что время получения клиентом транзакции от пользователя не является однозначным критерием в последовательности передачи им транзакции на дальнейшую обработку. Итак, если транзакция включена в блок и этот блок присоединен к блокчейну, эта транзакция считаются выполненной. Пока транзакция не попала в сформированный майнером блок цепи блокчейн, она считается неподтвержденной. Таким образом если, например, владелец криптокошелька «А» переводит владельцу криптокошелька «Б» некое количество криптомонет, то должен пройти определенный период времени (как правило от десяти минут до нескольких часов в зависимости от размера транзакции, количества перечисляемых криптомонет и мощностей сети в определенный период времени. Периодически в интернет-сети можно встретить информацию о том, что та или иная транзакция обрабатывалась на протяжении нескольких дней), пока данная транзакция не будет подтверждена и включена в очередной сформированный блок сети. Считается, что семь – это максимальное количество транзакций, с которыми сеть блокчейн справляется за одну секунду.

Соответственно, если количество транзакций увеличивается, то увеличивается время их обработки и наоборот.

Схематично это можно изобразить следующим образом:



Схематичное изображение формирования блоков в блокчейне

Приложение 5

Рисунки и диаграммы

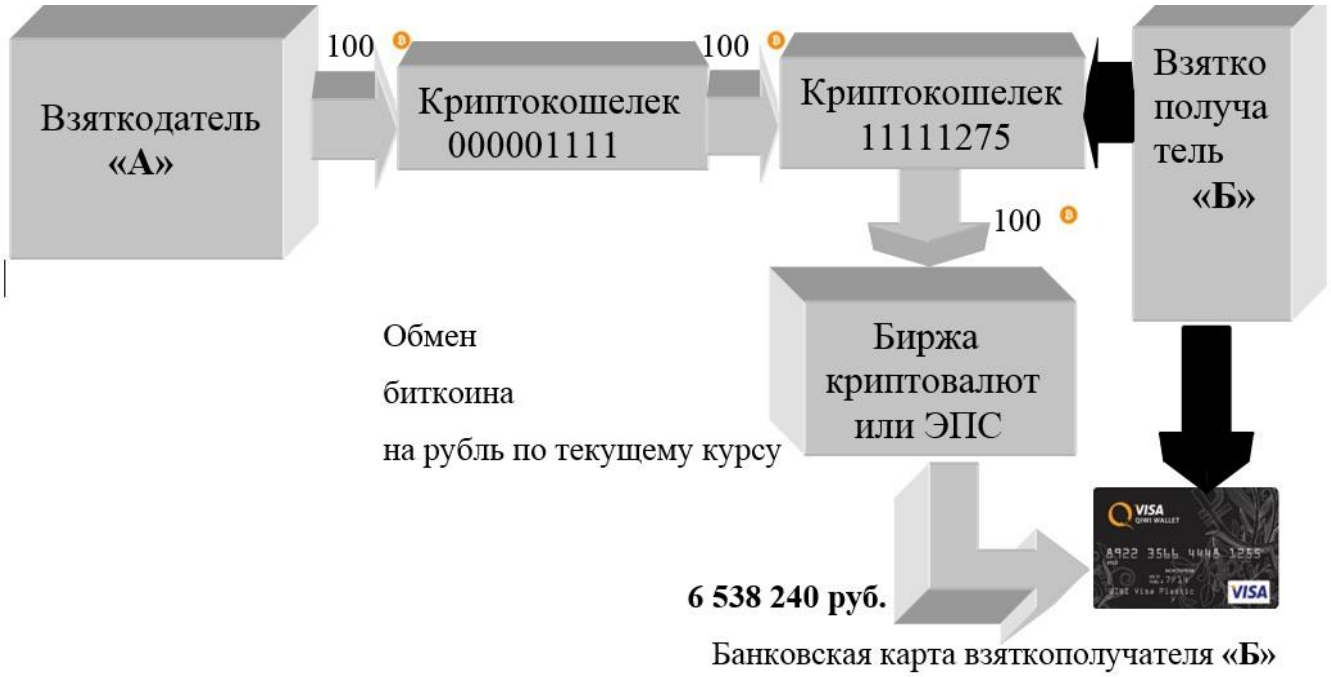


Рис. 1. Схематичное изображение процесса передачи взятки с использованием двух анонимных криптокошельков.

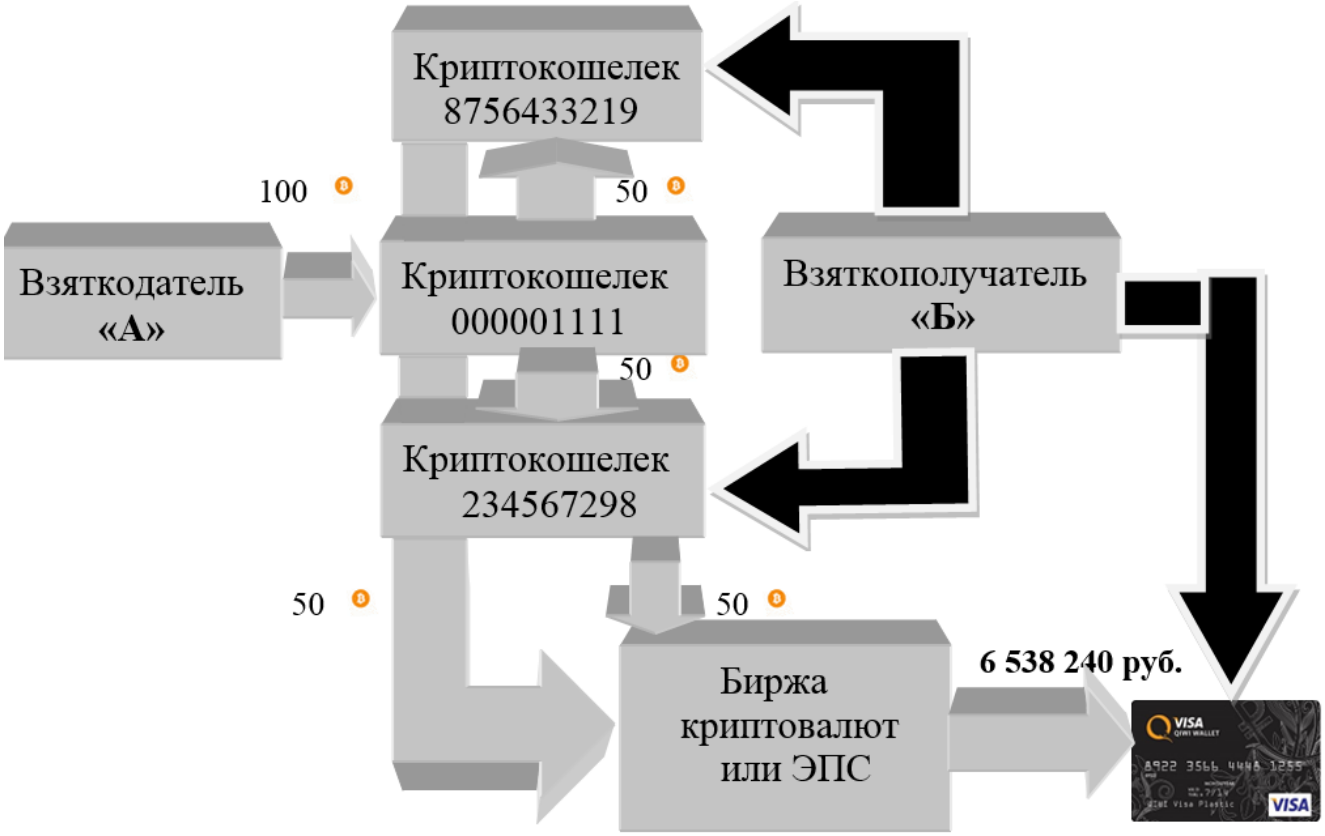


Рис. 2. Схематичное изображение процесса передачи взятки с использованием нескольких анонимных криптокошельков.

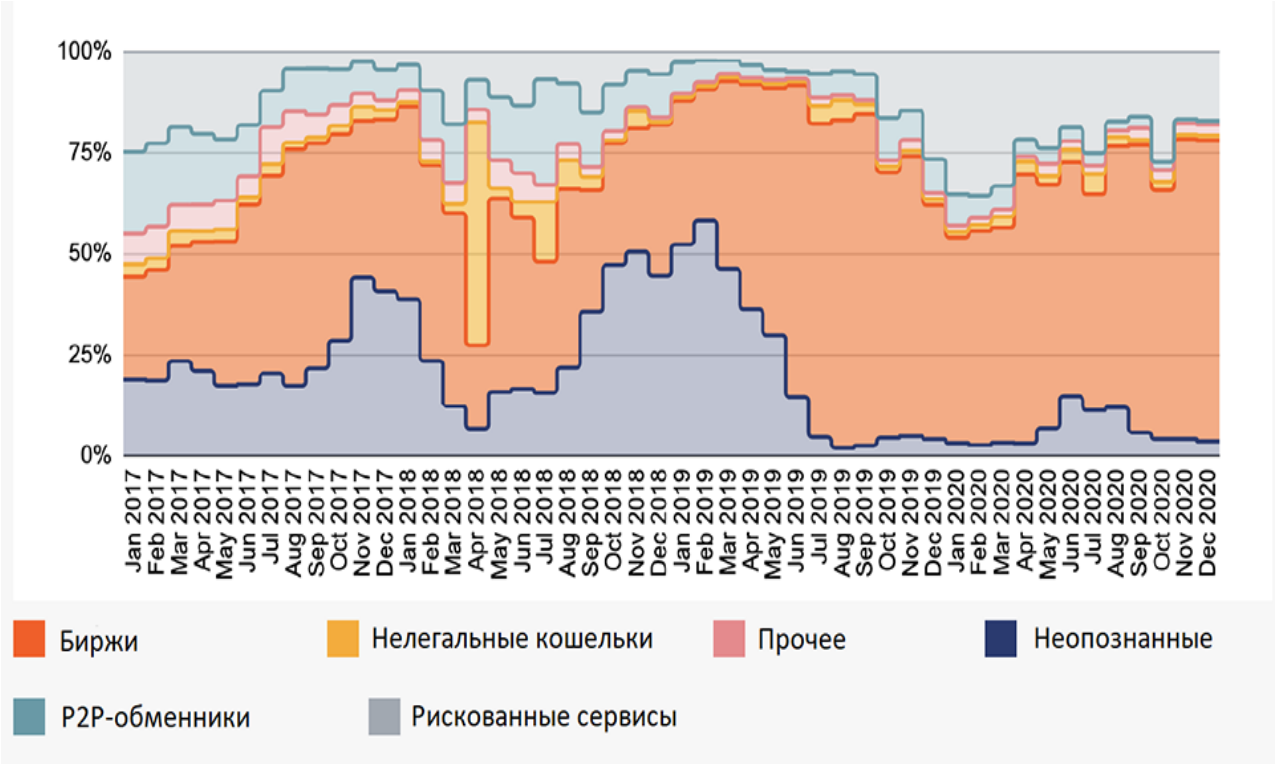


Рис. 3. Получатели переводов с нелегальных кошельков 2017-2020. Валюты: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT.

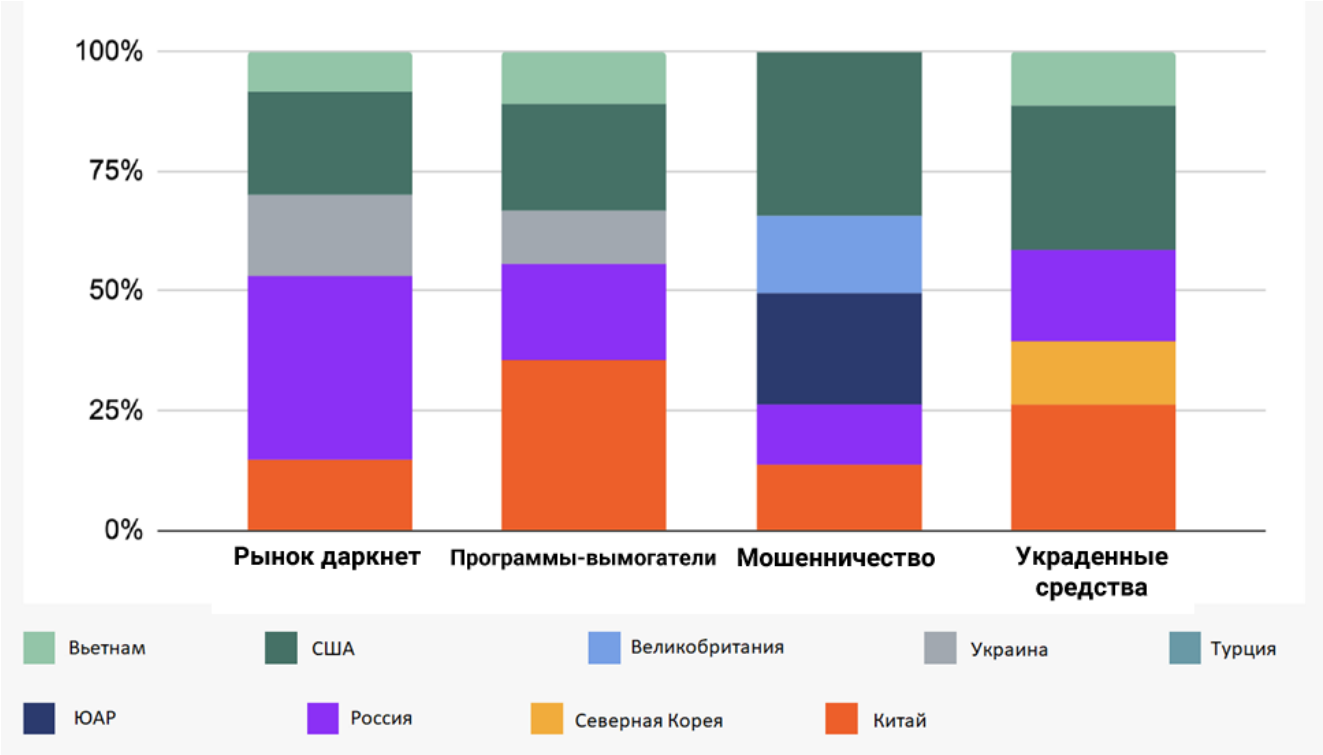


Рис. 4. Страны-получателей криптовалюты с учетом типа криминальной деятельности, за счет которой криптовалюта была получена. Объем подсчитан на основе web-трафика сервисов-получателей нелегальных средств.

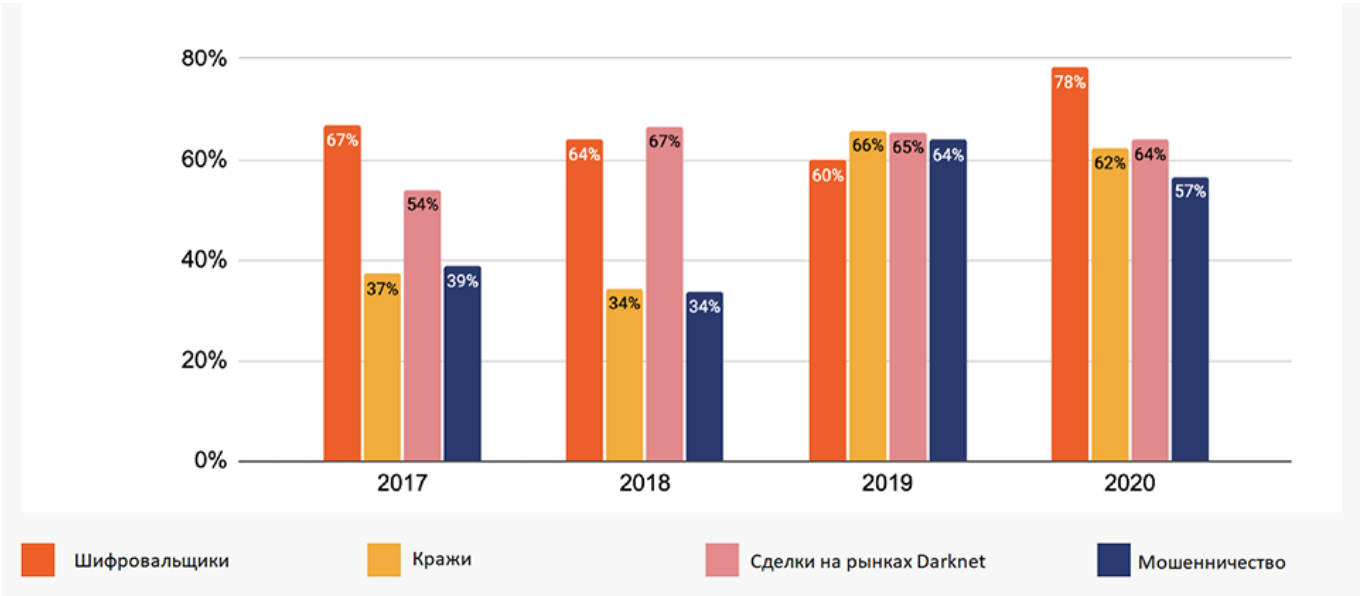


Рисунок 5. Процент нелегальных средств, направляемых на топ-5 сервисов 2017-2020 в разрезе видов криминальной деятельности. Валюты: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT.

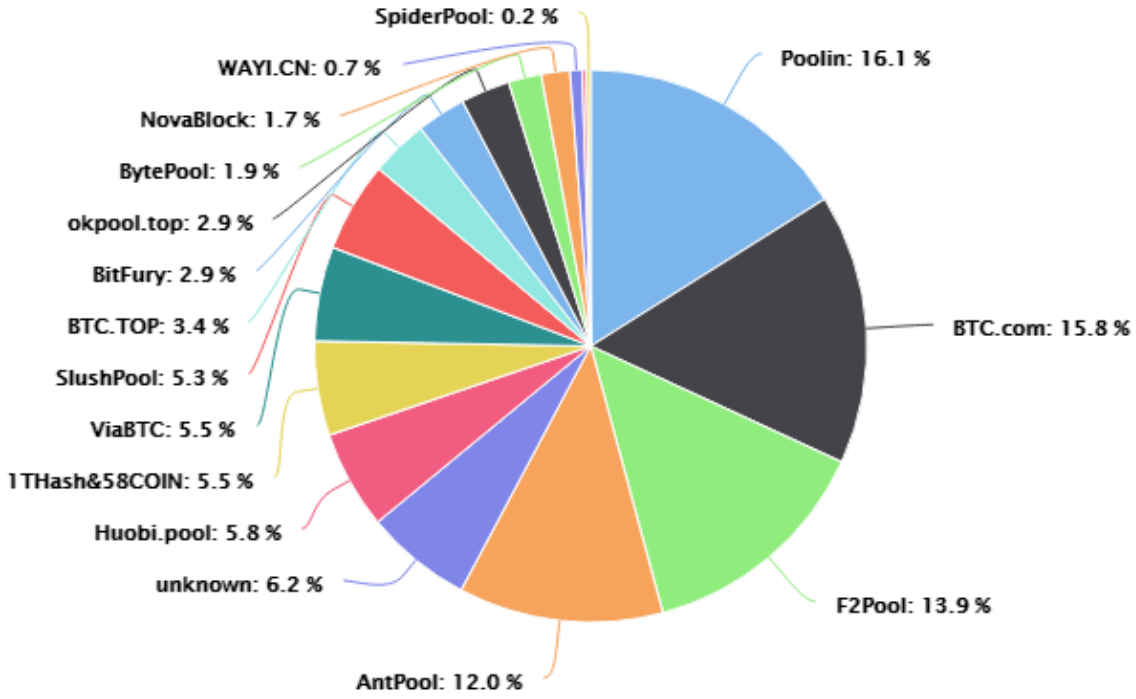


Рис.6. Диаграмма распределение пулов в сети биткоин.

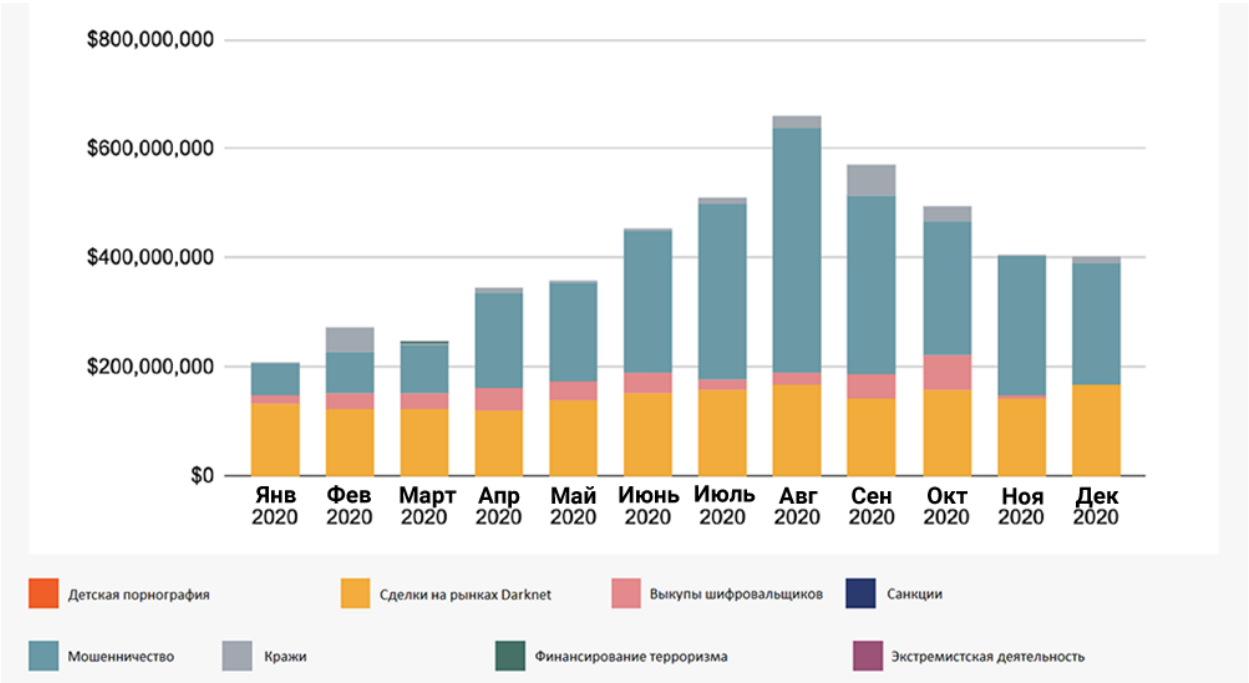


Рисунок 7. Объем криминальных крипто-валютных операций в 2020 году по месяцам.

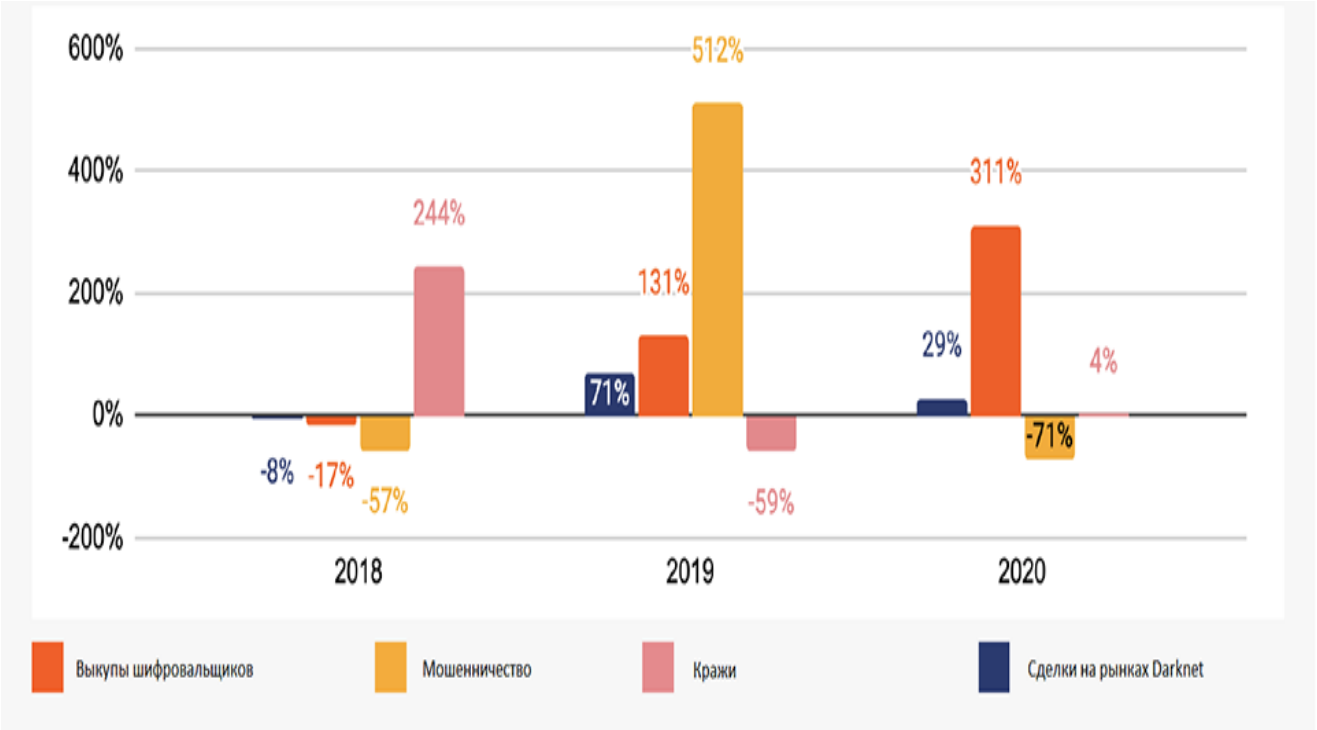


Рис. 8. Рост объема переводов криптовалют в разрезе различных видов преступлений

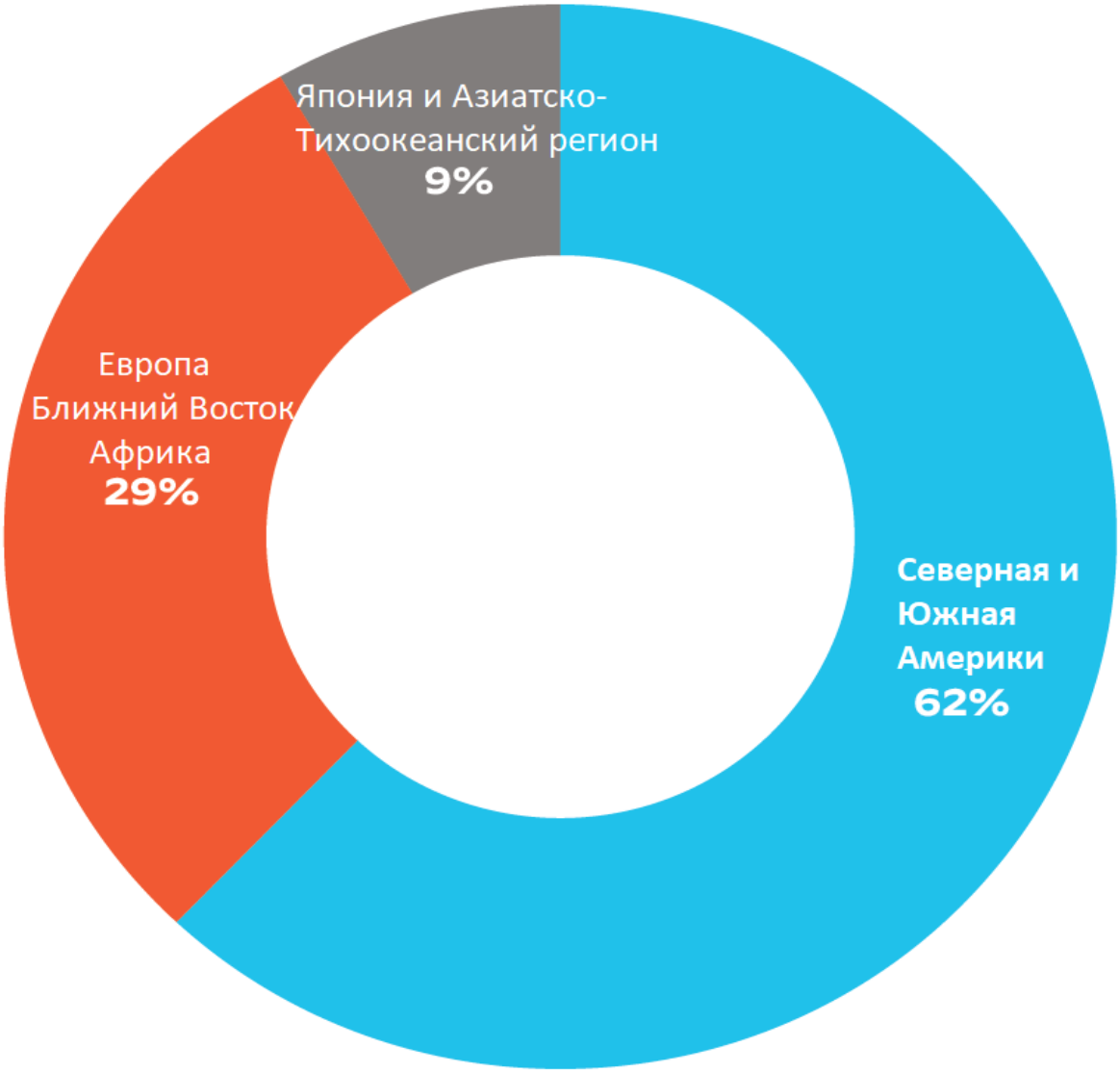


Рис. 9. Регионы мира, чьи организации и отдельные пользователи компьютерных устройства являлись потерпевшими при совершении вымогательств криптовалюты с использованием вируса-шифровальщика.

США	151	Бельгия	4	Чили	1	Пакистан
Канада	39	Швеция	4	Колумбия	1	Перу
Германия	26	ЮАР	3	Хорватия	1	Польша
Великобритания	17	Испания	3	Греция	1	Португалия
Франция	16	Япония	2	Гонконг	1	Саудовская Аравия
Индия	11	Мексика	2	Ямайка	1	Сингапур
Австралия	7	Новая Зеландия	2	Кения	1	Шри-Ланка
Бразилия	5	Южная Корея	2	Люксембург	1	Тайвань
Израель	5	Швейцария	2	Малайзия	1	Тайланд
Италия	5	Австрия	1	Норвегия	1	ОАЭ

Рис. 10. Страны, чьи организации и отдельные пользователи компьютерных устройства являлись потерпевшими при совершении вымогательств криптовалюты с использованием вируса-шифровальщика.

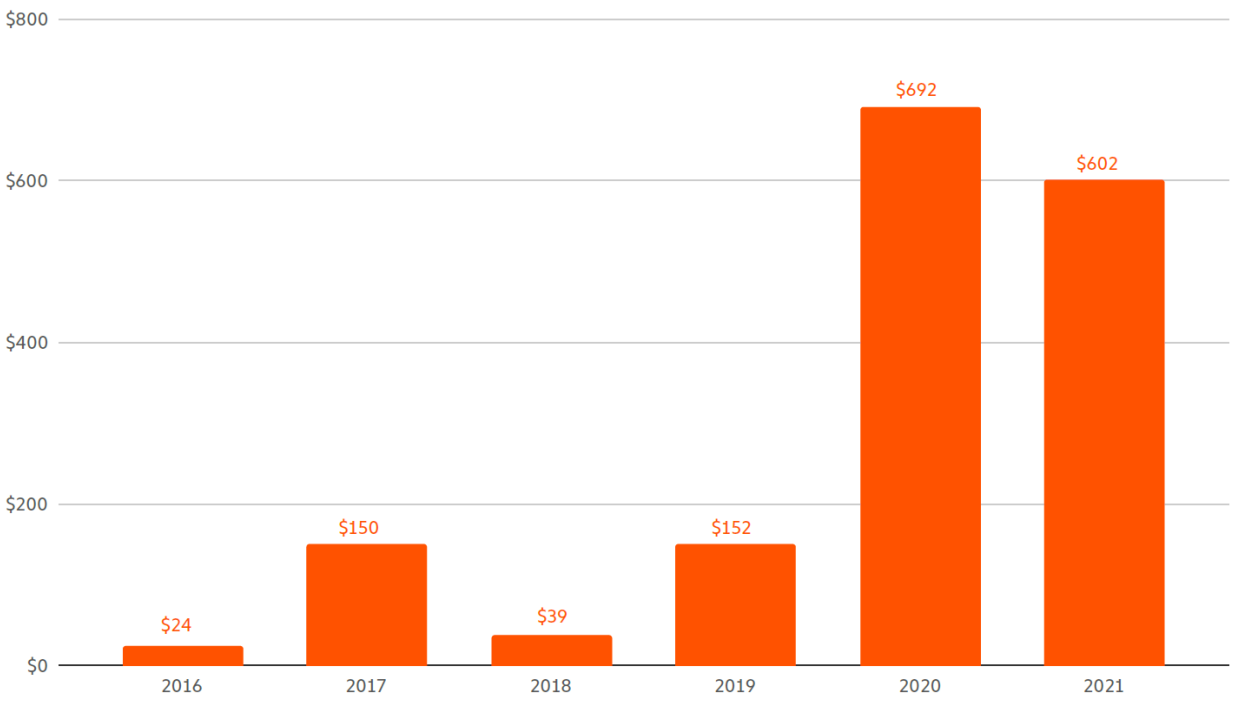


Рис. 11. Общий объем криптовалют, полученный преступниками в результате использования вируса-шифровальщика в мире за период 2016-2022.

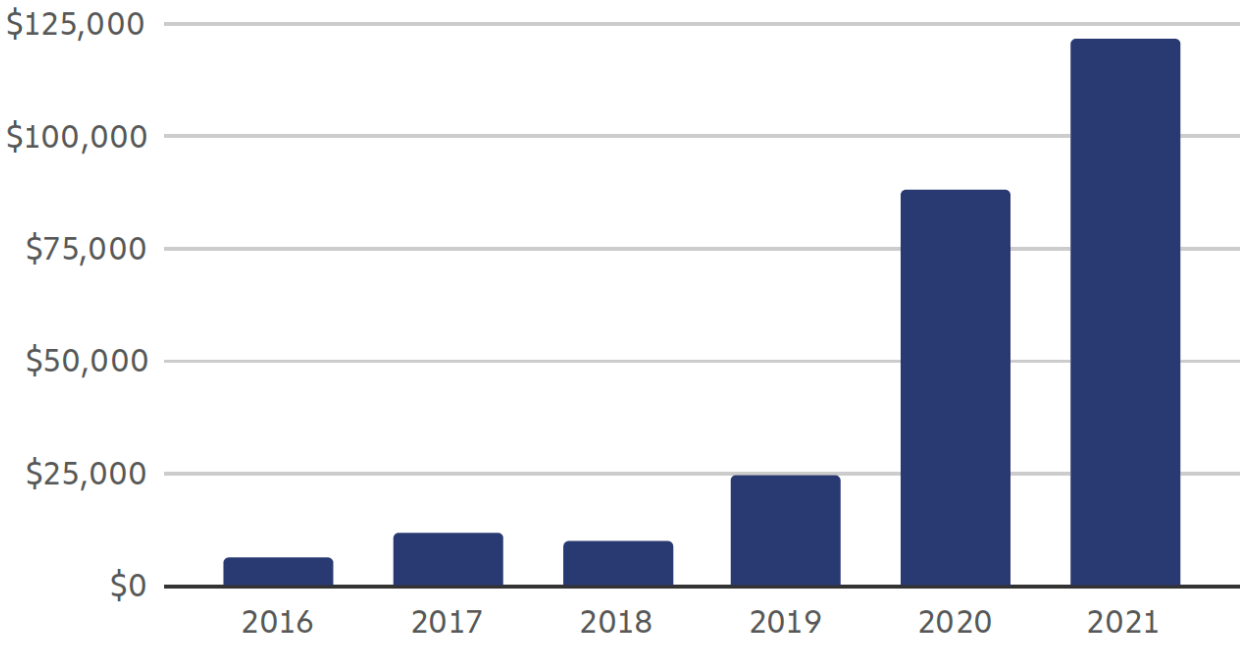


Рис. 12.Средний размер выкупа 2016-2021 требуемый преступниками за разблокировку компьютеров пользователей используемых ими вирусов-шифровальщиков.

Приложение 6

Материалы к заседанию коллегии Следственного комитета Российской Федерации «Об итогах работы следственных органов Следственного комитета Российской Федерации за 2022 г. и задачах на 2023 г».

Расследование киберпреступлений и деяний, совершенных с использованием информационно-телекоммуникационных технологий.

Следственным комитетом принимаются активные меры по противодействию киберпреступности, которая в условиях современных глобальных процессов представляет серьезную опасность. Все большее количество экономических и общеуголовных преступлений совершается с использованием информационно-телекоммуникационных технологий.

В 2022 году в следственные органы Следственного комитета поступило 18 886 сообщений о преступлениях, совершенных с использованием

информационно-коммуникационных технологий или в сфере компьютерной информации, что на треть больше, чем в 2021 году (14 698). Большинство сообщений поступило из органов МВД России (11 428, или 60,5%). По инициативе следователей Следственного комитета зарегистрировано 4 052 сообщения, или 21,5%.

В 2022 году в производстве следователей находилось 16 745 уголовных дел данной категории, или 8% от общего числа находившихся в производстве дел, из них окончено 7 636 уголовных дел, или 45,6%.

Расследовано 15 611 преступлений, совершенных с использованием информационно-коммуникационных технологий или в сфере компьютерной информации, что на 28,9% больше, чем в 2021 году (12 112).

Криминологический анализ расследованных преступлений показал, что более половины преступных деяний (10 790, или 69,1%) совершено с использованием информационно-коммуникационной сети Интернет, в том числе 105 - в ее теневом сегменте «Даркнет». Почти треть всех преступлений совершена с использованием компьютерной техники - 4 511 преступлений (28,9%). Четвертая часть (3 509, или 22,5%) совершена с использованием расчетных (пластиковых) карт. Кроме того, каждое шестое преступление совершено посредством социальных сетей (2 741, или 17,6%). С применением средств мобильной связи совершено 2 455 преступлений (15,7%), программных средств – 1 689 (10,8%), мессенджеров - 1 538 (9,9%).

Каждое пятое преступление в сфере информационных технологий (3 166) совершено лицами, не достигшими 18-летнего возраста, и их доля растет (в 2021 году отмечалось только 2 192 таких преступления).

Одновременно в 2 519 случаях (16,1%) преступления с применением информационно-коммуникационных технологий совершены в отношении детей, что на 13% превышает показатель 2021 года (2 232).

Кроме того, почти на треть увеличилось число преступлений, совершенных в отношении лиц пенсионного возраста (с 543 до 733).

В суд направлено 7 182 уголовных дела (+26,5%, в 2021 г. - 5 677).

Среди направленных в суд преобладают:

материалы по фактам кражи чужого имущества (2 471, или 34,4%);

849 дел, или 11,8%, - о преступлениях, связанных с незаконным оборотом наркотических средств;

622, или 8,7%, - о преступлениях против половой неприкосновенности и половой свободы личности;

447, или 6,2%, - об организации незаконной игорной деятельности;

428, или 6%, - о нарушении неприкосновенности частной жизни;

364, или 5,1%, - о распространении детской порнографии;

208, или 2,9%, - о незаконном использовании документов для образования (создания, реорганизации) юридического лица;

155, или 2,2%, - о преступлениях террористической и экстремистской направленности;

125, или 1,7%, - в сфере компьютерной информации.

Наибольшее число уголовных дел, направленных в суд, отмечается в следственных подразделениях Кемеровской области - Кузбасса (307), Санкт-Петербурга (247), Свердловской (234), Нижегородской (202), Челябинской (200) областей.

Прекращено производство по 419 уголовным делам, или 6% от числа оконченных, из них в связи с отсутствием события или состава преступления прекращено 253 уголовных дела, или 60,4%.

Количество уголовных дел, следствие по которым приостановлено, увеличилось на 33,7% (с 309 до 413), в том числе увеличилось на 32,9% число уголовных дел, приостановленных в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого (с 213 до 283).

По результатам проверки законности принятых решений отменено 4 постановления о возбуждении уголовного дела (в 2021 г. - 1), 156 постановлений об отказе в возбуждении уголовного дела, или 3,9% (+113,7%, в 2021 г. - 73), 29 решений о приостановлении предварительного следствия,

или 5,2% (+107%, в 2021 г. - 14), 26 постановлений о прекращении уголовных дел, или 6,2% (+18,2%, в 2021 г. - 22).

В срок свыше двух месяцев расследовано 2 542 уголовных дела или 34,1%, что на 31% больше, чем в 2021 году (1 942, или 32,3%).

Прокурором возвращено для производства дополнительного расследования 81 уголовное дело, что на 14,1% больше, чем в 2021 году (71). Их удельный вес составил 1,2% (в 2021 г. - 1,3%). Наибольшее число уголовных дел, возвращенных в порядке, предусмотренном ст. 221 УПК РФ, отмечается в следственных управлениях по Республике Калмыкия и Пермскому краю (по 6), Свердловской области - 5.

Для пересоставления обвинительного заключения прокурором возращено 5 дел, что на 58,3% меньше показателя 2021 года (12). По одному такому факту отмечено в Восточном межрегиональном следственном управлении на транспорте, следственных управлениях по Санкт-Петербургу, Красноярскому краю и Республике Хакасия, Республике Коми и Курганской области.

Судом в порядке, предусмотренном ст. 237 УПК РФ, возвращено 42 уголовных дела, что на 50% больше, чем в 2021 году (28). Удельный вес от числа направленных в суд дел составил 0,6% (в 2021 г. - 0,5%). Нарушения, повлекшие возвращение уголовных дел на доработку, допущены Восточным межрегиональным следственным управлением на транспорте (6 дел), следственными управлениями по Республике Татарстан (4), Свердловской и Воронежской областям (по 3).

На стадии следствия в 2022 году прекращено по реабилитирующим основаниям преследование в отношении одного лица (в 2021 г. - 4).

Судом вынесены оправдательные приговоры в отношении 7 лиц (в 2021 г. - 5). Такие факты отмечены в Калужской области (3 лица), Московской области, Республике Калмыкия, Ханты-Мансийском автономном округе - Югре - по 1 лицу.

В 2022 году по 6 909 уголовным делам следователями внесены представления о принятии мер по устранению обстоятельств,

способствовавших совершению преступлений (+24,5%, в 2021 г. - 5 551). Их удельный вес составил 91,4% (в 2021 г. - 91,1%). По внесенным представлениям поступило 6 184 уведомления о принятых мерах (в 2021 г. - 5 188). Привлечено к дисциплинарной ответственности 2 654 должностных лица (в 2021 г. - 1 964).

В результате преступлений в рассматриваемой сфере причинен материальный ущерб на сумму 2 млрд. 570 млн. 160 тыс. рублей (+2,5%, в 2021 г. - 2 млрд. 507 млн. 560 тыс. руб.).

Возмещено в ходе следствия обвиняемыми 1 млрд. 107 млн. 631 тыс. рублей, или 43,1% (-35,3%, в 2021 г. - 1 млрд. 711 млн. 147 тыс. руб., или 68,2%).

По ходатайству следователей наложен арест на имущество обвиняемых на сумму

2 млрд. 473 млн. 426 тыс. рублей (в 2021 г. - 968 млн. 906 тыс. руб.).

Расследование не только сложных киберпреступлений, но и иных преступных деяний, совершенных организованными группами, преступными сообществами, спланированных и скоординированных с использованием сети Интернет, невозможно без применения современных цифровых технологий.

При этом необходимо отметить, что, несмотря на ежегодную тенденцию к увеличению доли преступлений, раскрытых с использованием информационно-коммуникационных технологий, их удельный вес составляет всего 15%, или 2 631 преступление.

Приложение 7

ПРОЕКТ
ФЕДЕРАЛЬНОГО ЗАКОНА

О ВНЕСЕНИИ ИЗМЕНЕНИЙ В УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Внести в Уголовный кодекс Российской Федерации (Собрание законодательства Российской Федерации, 1996, № 25, ст. 2954; 1998, № 22, ст. 2332; № 26, ст. 3012; 1999, № 7, ст. 871, 873; № 11, ст. 1255; № 12, ст. 1407; № 28, ст. 3489, 3490, 3491; 2001, № 11, ст. 1002; № 13, ст. 1140; № 26, ст. 2587; № 33, ст. 3424; № 47, ст. 4404, 4405; № 53, ст. 5028; 2002, № 10, ст. 966; № 11, ст. 1021; № 19, ст. 1793, 1795; № 26, ст. 2518; № 30, ст. 3020, 3029; № 44, ст. 4298; 2003, № 11, ст. 954; № 15, ст. 1304; № 27, ст. 2708, 2712; № 28, ст. 2880) следующие изменения, дополнив статьями:

171.6 Незаконное генерирование (майнинг) криптовалют

1. Осуществление генерирования (майнинга) криптовалют без регистрации или без лицензии либо без аккредитации в национальной системе аккредитации в случаях, когда такие лицензия, аккредитация в национальной системе аккредитации обязательны, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо

обязательными работами на срок до четырехсот восьмидесяти часов, либо арестом на срок до шести месяцев.

2. То же деяние:

а) совершенное группой лиц по предварительному сговору, либо организованной группой;

б) сопряженное с использованием не принадлежащего лицу компьютерного оборудования, -

наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового.

187.1 Неправомерный оборот криптовалюты

1. Организация выпуска, обращения, обмена либо непосредственно выпуск, организация и обмен криптовалюты (в том числе криптобиржами, криптообменными пунктами, виртуальными платформами) на территории Российской Федерации вопреки установленному запрету, -

наказываются принудительными работами на срок до трех лет либо лишением свободы на срок до трех лет со штрафом в размере от двухсот тысяч до четырехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.

2. Те же деяния, совершенные группой лиц, организованной группой, -

наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до пяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет или без такового.

187.2 Нарушение порядка осуществления сделок с использованием криптовалюты

1. Нарушение запрета для финансовых организаций на собственные вложения в криптовалюты и непосредственно связанные с ними финансовые инструменты, а также нарушение запрета на использование российских финансовых посредников и инфраструктуры финансового рынка для осуществления любых операций с криптовалютой: приобретение криптовалюты, осуществление платежей и переводов, отчуждение криптовалют и способствование осуществлению подобных операций (в том числе оказание услуг по хранению или содействие принятию рисков через деривативы), -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на срок до четырех лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового.

2. То же деяние:

а) совершенное организованной группой;

б) сопряженное с извлечением дохода в особо крупном размере, -

наказывается принудительными работами на срок до пяти лет либо лишением свободы на срок до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет или без такового.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ПРОЕКТУ ФЕДЕРАЛЬНОГО ЗАКОНА «О ВНЕСЕНИИ ИЗМЕНЕНИЙ В УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ»

Проект федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» (далее- законопроект) разработан в целях совершенствования норм уголовного законодательства, регламентирующих меры юридической ответственности, применяемые к лицам, совершающим преступления с использованием криптовалюты.

Разработка законопроекта обусловлена наличием бесконтрольного оборота криптовалют на территории Российской Федерации, что может привести к фактической конкуренции криптовалют с национальной валютой, имеющей официальное хождение на территории страны, что в свою очередь неизбежно приведет к дестабилизации финансовой стабильности государства и как следствие резкому падению благосостояния граждан.

В целях недопущения угроз благосостояния граждан Российской Федерации, финансовой стабильности государства, расширения нелегальной деятельности и снижения количества преступлений, совершаемых с использованием криптовалюты, и, как следствие, стабилизации национальной финансовой системы автором предлагается внесение изменений в уголовное законодательство Российской Федерации, которые позволят прекратить или в значительной степени ограничить использование криптовалют юридическими и физическими лицами – резидентами Российской Федерации в качестве фактического средства платежа как на территории Российской Федерации, так и вне ее юрисдикции. В свете изложенного видится необходимым принятия закона, ограничивающего деятельность по осуществлению майнинга криптовалют и предлагается рассмотреть проект закона о внесении изменений

в УК РФ о введении уголовной ответственности за осуществление незаконного майнинга и незаконного использования криптовалют.

ФИНАНСОВО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ К ПРОЕКТУ ФЕДЕРАЛЬНОГО ЗАКОНА «О ВНЕСЕНИИ ИЗМЕНЕНИЙ В УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ»

Реализация проекта федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» не потребует дополнительных расходов из средств федерального бюджета.

Кроме того следует учитывать, что введение уголовной ответственности является превентивной мерой, направленной на предупреждение совершения преступлений в сфере оборота криптовалют.

ПЕРЕЧЕНЬ АКТОВ ФЕДЕРАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА, ПОДЛЕЖАЩИХ ПРИЗНАНИЮ УТРАТИВШИМИ СИЛУ, ПРИОСТАНОВЛЕНИЮ, ИЗМЕНЕНИЮ ИЛИ ПРИНЯТИЮ В СВЯЗИ С ПРИНЯТИЕМ ФЕДЕРАЛЬНОГО ЗАКОНА «О ВНЕСЕНИИ ИЗМЕНЕНИЙ В УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ»

Принятие федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» не потребует признания утратившими силу, приостановления, изменения или принятия иных федеральных законов.