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

Кафедра криминалистики

Специальность 40.05.02 Правоохранительная деятельность
специализация № 1 «Оперативно-розыскная деятельность»,
узкая специализация «Деятельность подразделений по контролю за
оборотом наркотических средств и психотропных веществ органов
внутренних дел»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по теме:

Особенности доказывания по уголовным делам о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием криптовалют

Выполнил:
Слушатель группы П 1702
младший лейтенант полиции
Гайдуцкий Денис Валерьевич

Решение о допуске к защите:
к защите допускается
Заместитель начальника института
по учебной работе
полковник полиции
_____ А.Г. Калугин
«12» мая 2022 г.

Руководитель
Начальник кафедры
уголовного процесса
к.ю.н., доцент
полковник полиции
Судницын Алексей Борисович

Дата защиты:
«22» июня 2022 г.

Оценка: хорошо

Председатель ГЭК
полковник полиции _____ А.С. Самохвалов
(специальное звание) (подпись) (инициалы, фамилия)

Красноярск 2022

СОДЕРЖАНИЕ:

Введение

Актуальность и новизна исследования. Согласно проекту Стратегии государственной антинаркотической политики Российской Федерации до 2030 года[1], разработанной МВД России, ежегодно на территории нашей страны выявляется около 200 тыс. преступлений, связанных с незаконным оборотом наркотиков. Несмотря на то, что в 2021 г. было зарегистрировано снижение количество совершенных наркопреступлений – 190,2 тыс. (-5,0%), 2018 г. – 200,3 тыс. (-4,0%), в 2017 г. – 208,7 тыс. (+3,7%), в 2016 г. – 201,2 тыс. (-15,1%), в 2015 г. – 236,9 тыс.[2], показатель влияния наркоситуации на криминогенную обстановку в целом характеризуется как «тяжелый»[3]. Показатель «Удельный вес наркопреступлений в общем количестве зарегистрированных преступных деяний» составляет порядка 10(2021 г. – 10,1%, 2020 г. – 10,1%, 2019 г. – 10,2)[4]. Опасными тенденциями являются: рост количества лиц с зависимостью от новых психоактивных веществ и полинаркоманией более чем в два раза с 2010 года (2020 г. – 63,4 тыс. чел.; 2015 г. – 48,9 тыс. чел., 2010 г. – 26,4 тыс. чел.);рост зависимости от психостимуляторов более чем в три раза с 2010 года (2020 г.– 24,8 тыс. чел.; 2015 г. – 16,6 тыс. чел., 2010 г. – 7,8 тыс. чел.)[5].

---

[1] МВД России обнародовало проект антинаркотической стратегии до 2030 года [Электронный ресурс] URL: http://политикапрезидента.рф/mvd-obnarodovalo-proekt-antinarkoticheskoy-strategii-do-2030-goda (дата обращения: 22.03.2022).

[2] Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2021 года [Электронный ресурс] https://xn--b1aew.xn--p1ai/reports/item/19897618/ (дата обращения: 22.03.2022).

[3] Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2021 года [Электронный ресурс] https://xn--b1aew.xn--p1ai/reports/item/19897618/ (дата обращения: 22.03.2022).

[4] Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2021 года [Электронный ресурс] https://xn--b1aew.xn--p1ai/reports/item/19897618/ (дата обращения: 22.03.2022).

[5]Бульбачева А.А., Котяжов А.В. — Коллизии и противоречия правового регулирования в сфере противодействия незаконному обороту наркотических средств, психотропных веществ и их прекурсоров:пути совершенствования антинаркотического законодательства// Полицейская деятельность. 2020. № 3. С. 32.

Указанное состояние наркопреступности вызвано множеством факторов, но с развитием информационных технологий способы совершения наркопреступленийподвергаются изменению. Так, «криптовалюта», основанная на технологии «блокчейна», привнесли в современный мир достаточно большое количество возможностей – в экономику, организацию государственных и частных корпораций, бизнес и т.д. Одновременно с этимкритовалюта, принимаемая как средство оплаты, является достаточно привлекательной для преступного мира.Использование криптовалюты при операциях с наркотиками обеспечивает повышенный уровень оперативности осуществления финансовых операций, а также их конспирацию.

В указанных условиях изучение сущности криптовалют, их правового регулирования, особенностей выявления и документирования преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, совершенных с использованием криптовалют, а также возможности использования данных и сведений об операциях с ними при доказывании по уголовному делу представляются особенно важным, как с теоретических, так и прикладных аспектов.

Изложенное обуславливает высокую избранной актуальность темы.

Целью исследования является выработка предложений по усовершенствованию уголовно-процессуального законодательства и правоприменительной деятельности в части доказывания по уголовным делам о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием криптовалют.

Поставленная цель предполагает решения следующих задач:

- установлениепонятия и сущности криптовалют;

- характеристика особенностей использования криптовалют при совершении преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ;

- выявление особенностей криптовалюты как средстваконспирации преступных действий;

- анализ особенностей выявления и документирования преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, совершенных с использованием криптовалют;

- изучение особенностей использования сведений об операциях с криптовалютами в доказывании по уголовным делам в сфере в сфере незаконного оборота наркотических средств и психотропных веществ.

Объектом исследованияявляются общественные отношения, складывающиеся ввиду противоправной деятельности лиц, совершивших преступления, связанные с незаконным оборотом наркотических средств, с использованием криптовалюты, а также деятельности правоохранительных органов по предупреждению, раскрытию и расследованию данного вида преступлений.

Предметом исследованияявляется группа объективных закономерностей, определяющих механизм подготовки, совершения и сокрытия преступлений, связанных с незаконным оборотом наркотических средств, с использованием криптовалюты, механизм образования следов как источников розыскной и доказательственной информации, а также закономерности собирания, исследования, оценки и использования доказательств основанных на операциях с крипотовалютойв процессе раскрытия и расследования данного вида преступлений.

Методология и методика исследования базируется на общенаучном диалектическом методе познания, определяющем важнейшие сущностные аспекты структуры и содержания научных теорий в различных отраслях научного знания, а также позволяющем выработать критерии достоверности результатов научных исследований.

В рамках отдельных этапов исследования применялись методы системного анализа, сопоставления, систематизации и обобщения теоретического и эмпирического материала; методы сравнительно-правового и структурно-криминалистического анализа. В процессе исследования

реализованы также общелогические методы: анализа, синтеза, индукции, дедукции, аналогии, абстрагирования, обобщения.

Теоретической основой исследования выступают труды выдающихся ученых в области теории криминалистики и уголовного процесса – П.В. Галушина, О.А. Суровой, С.И. Земцовой, Л.Е. Чистовой, Ю.В. Трунцевский, А.Н. Сухаренко, Л.М. Изольдина, М.М. Долгиева, Л.В. Ефимова, А.К. Жарова, А.А. Максуров, И.И. Кучеров и других.

Структура работы обусловлена поставленной целью и соответствующими ей задачами. Выпускная квалификационная работа состоит из введения, двух глав, включающих в себя пять параграфов, заключения и списка использованной литературы.

Глава 1. Общая характеристика использования криптовалют при совершении преступлений.

1.1 Понятие и сущность криптовалют.

Рассматривая вопрос о понятии и сущности криптовалюты предлагаем остановиться на следующих аспектах:

- история становления и развития криптовалюты;
- понятие, сущность, виды криптовалюты:
- правовой статус криптовалюты и перспективы его изменения.

В последние годы в российской правовой и экономической действительности можно наблюдать ряд трансформаций, в том числе и трансформацию цифрового характера. Данное направление обозначено в качестве приоритета экономики в России как на федеральном, так и на иных государственных уровнях. При всем при этом в настоящий момент не приняты первоочередные необходимые меры по созданию нормативно-правовой базы для цифровой экономики, необходимой для реализации государственной единой стратегии цифровой трансформации. К таким мерам следует относить разработку фундаментального категориального аппарата и правовых институтов, которые обеспечивали бы оборот инновационных технологий, а также единых подход к их правовому пониманию и регулированию[6].

В Указе Президента Российской Федерации от 7 мая 2018 г. «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» обозначена необходимость реализации адаптивного, гибкого подхода к разработке нормативной базы для наиболее качественного внедрения цифровых технологий в разные части российской

[6]Трибушный И.Ю., Трибушная М.И., Трибушная В.Х. Ключевые аспекты российской цифровой экономики и ее нормативного регулирования // Инновационная экономика: перспективы развития и совершенствования, № 8 (34), 2020. С. 43.

экономики[7].

Впервые идея децентрализованной анонимной системы платежей была озвучена М. Фридманом еще в 1999 г.[8] Со временем данная идея развивалась, но в наиболее проработанном виде она была воплощена в 2009 г., когда СатошиНакамото[9] представил миру биткоин как одноранговую платежную систему[10]. История ее появления имеет загадочные обстоятельства. Ее создателем считается человек или группа людей под псевдонимом «СатосиНакамото». На официальном сайте данной криптовалюты была опубликована информация о том, что создатель - гражданин Японии, но спустя несколько лет, стало известно, что данное лицо или группа, работали с северных районов США. По словам СатосиНакамото, разработка одноранговой системы началась в середине 2007 года. В это же время был обнародован файл с описанием принципа и протокола работы платёжной системы.[11]

3 января 2009 года были впервые сгенерированы первые 50 Биткойнов, а через 9 дней был осуществлен первый перевод в размере 10 Биткойнов в адрес ХэлуФинни. В сентябре 2009 года – состоялся первый в мире обмен Биткойнов на денежную сумму. Марти Малми отправил некому NewLibertyStandard 5050 Биткойнов, за которые Марти получил 5,02 доллара. Именно данная цифровая валюта создала такой ажиотаж и притянула

---

[7] Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Доступ из справ.-прав. системы «КонсультантПлюс».

[8] Прим. Милтон Фридман (англ. MiltonFriedman; 31 июля 1912, Бруклин, Нью-Йорк, США 16 ноября 2006, Сан-Франциско, США) — американский экономист, обладатель премии по экономике памяти Альфреда Нобеля 1976 года за исследования в области потребления, монетарной истории и теории, а также сложности стабилизационной политики.

[9] Сато́сиНакамо́то (англ. SatoshiNakamoto) — псевдоним человека или группы людей, разработавших протокол криптовалютыБиткойн и создавших первую версию программного обеспечения, в котором этот протокол был реализован. Было предпринято несколько попыток раскрыть реальную личность или группу, стоящую за этим именем, но ни одна из них не привела к успеху.

[10] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронныйресурс] URL: https://bitcoin.org/bitcoin.pdf (датаобращения: 07.11.2021).

[11] Nakamoto S., Bitcoin: A Peer-To-Peer Electronic Cash System. 2008.

огромное внимание ко всей сфере криптовалюты.

На данный момент Биткоин до сих пор занимает первое место в топе криптовалют по мнение сайта «CoinMarketCap». Ряд крупных компаний инвестируют и используют платформу биткоин. К примеру, всем известная компания Microsoft используют платформу во всех своих программах. Они осуществляют продажу за биткоин различный контент из разряда видеоигр, композиций, собственное программное обеспечение и т.д. В саму платформу внедрена BitPay, позволяющая осуществлять транзакции с криптовалютой.

Одна из крупнейших компаний в мире – Expedia стала предлагать услуги бронирования отелей за биткоин уже в 2014 году и, как показывает курс биткоина, компания не прогадала, поскольку сформировала отличную финансовую базу на данной криптовалюте. Сейчас Expedia планирует прейти на бронирование рейсов и иных туристических услуг.

Overstock – компания предлагает товары для дома и электронные устройства за биткоин. Сервис упростил все возможные операции для наиболее быстрой и легких операций с криптовалютой. Сейчас компания интегрирует криптовалютную биржу «ShapeShift» для возможности внесения в перечень допустимых к оплате криптовалют (Эфириум, Лайткоин, Дэш и т.д.).

На настоящий момент, согласно сведениям Интернет-ресурса «Investing.com», насчитывается около 2 867 видом криптовалют. В Топ-10 криптовалют, исходя из их капитализации входят следующие: Биткоин, Эфириум, Рипл, Tether, BitcoinCash, BitcoinSV, Лайткоин, BinanceCoin, EOS, Tezor[12].

С 2017 года особую популярность получила другая криптовалюта - эфириум. В 2003 году Виталий Бутериный, основатель журнала «BitcoinMagazine», предложил создать единую децентрализованную виртуальную машину, которая в дальнейшем стала работать на базе умных

[12] Все криптовалюты [Электронный ресурс] URL: https://investing.com (дата обращения: 19.11.2021).

контрактов. Программа была запущена 30 июля 2015 года. 14 марта 2016 года эфириум перешел на новую версию протокола «Homestead», которая в свою очередь вышла из «сырой» версии «Fronteir». В данной вариации «Homestead» стала на порядок безопаснее и стабильней. Тем самым позволило ускорить процесс появления новых блоков, для последующего хранения информации. Так к примеру, в случае с эфириумом скорость появления составляет от 10 до 15 секунд, когда у того же биткоина целых 10 минут, что очень существенно влияет на процесс осуществления транзакций.

Как и любая другая платформа, эфириум также подвергался хакерским атакам. Разработчиками была создана платформа «DAS», которая была разработана на платформе эфириума, и в момент одной из таких атак, хакеры похитили приблизительно 60 миллионов долларов со счетов пользователей. В связи с этим, Виталий осуществил хордфорк и появился эфириум классик в целях возвращения краденых денег на счета юзеров. На данное время, оба протокола полноценно работают.

Разумным представляется в рамках данной работы не обратить внимание также на национальную российскую криптовалютуРускоин. Согласно сведениям с официального сайта[13], токеныРускоин созданы для привлечения инвестиций в проекты, основанные российскими Фаундерами. Объем эмиссии токеновРускоин $1 050 000 000. Всего 21 млн монет, из них на waves-16 млн монет, на ETH- 5 млн монет. Цена на стадии размещения $50. 2% от собранных средств и 20% ежеквартальной прибыли идут на содержание проекта и выкуп токенов на биржах, остальные собранные средства на покупку акций Мосбиржи. Главная их цель - привлечение инвесторов в различные проекты через механизм ICO2 («Первоначальное предложение монет»). Покупатели токенов Рускоин таким образом становятся совладельцы реальных и существующих предприятий.

Переходя к рассмотрению правового статуса криптовалюты, начнем со

[13]Рускоин. [Электронный ресурс] URL: https://ruscoin.io/ (дата обращения: 19.11.2021).

следующего. В настоящее время ни в зарубежной, ни в отечественных доктринах не сложилось единое мнение относительно криптовалюты. В разных источниках и правовых системах криптовалюта рассматривается как:

1 Объект гражданских прав;

2 Средство платежа;

3 Цифровая валюта;

4 Товар;

5 Обязательственное право.

На настоящий момент справедливости ради следует заметить, что дать однозначно правильный ответ относительно природы криптовалюты не представляется возможным в силу многогранности данного явления, большого количества выполняемых им функции, её нематериальности, незавершенность юридической базы.

Как пишет О.С. Беломытцева, «в мировом сообществе не наблюдается единства мнений о криптовалюте со стороны ни регуляторов, ни ведущих представителей экономической и юридической наук»[14].

По мнению П. Винья и М. Кэйси, биткоин следует рассматривать не только как валюту или процессинговую систему обработки платежей, но и как алгоритм децентрализации общественных отношений, поскольку ключевой фактор ее функционирования - это отсутствие централизованной системы регулирования[15].

По мнению Л.Г. Ефимовой, криптовалюты являются «новой формой частных денег, поскольку они выполняют денежные функции. Такой вывод основывается на экономических исследованиях. Выпуск криптовалюты не нарушает действующее российское законодательство о валютной монополии, поскольку такая монополия распространяется только на выпуск наличных

[14]Беломытцева О.С. О понятии криптовалюты «биткоин» в рамках мнений финансовых регуляторов и контексте частных электронных денег // Проблемы учета и финансов. 2014. № 2. С. 26 - 28.

[15] Кейси М., Винья П., Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. Перевод на русский язык, издание на русском языке, оформление. М., 2017. С. 149.

денег, а криптовалюты (виртуальные валюты) не существуют в наличной форме. По этой причине они не могут признаваться денежными суррогатами»[16].

Ф. Томлинсон, считает, что криптовалюта – это разновидность цифровой валюты, создание и контроль за которой базируется на криптографических методах[17].

По мнению Джерри Брито и Эли Дурадо, криптовалюта – название распределенной и децентрализованной системы безопасного обмена и передачи цифровых денежных знаков, основанной на средствах криптографии[18].

Наиболее распространено мнение об отнесении криптовалют к имуществу и на то имеются довольно веские основания.

Согласно ст. 128 ГК РФ к объектам гражданских прав относятся вещи (включая наличные деньги и документарные ценные бумаги), 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. Именно на эту статью сослался Девятый арбитражный апелляционный суд, в решении от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017. В рамках данного дела рассматривался вопрос о включении содержимого криптокошелька, принадлежащего должнику, в конкурсную массу. Суд удовлетворил заявленные требования и указал, что действующее гражданское законодательство не содержит понятия «иное имущество», упомянутое в ст. 128 ГК РФ, с учетом современных экономических реалий и

[16] Ефимова Л.Г. Некоторые аспекты правовой природы криптовалют //Юрист. 2019. № 3. С. 12.

[17]Хажиахметова Е.Ш. Криптовалюта – деньги XXI век // новая наука: от идеи к результату. Агентство международных исследований, 2016. № 11.

[18]Криптовалюты [Электронный ресурс] URL: https://www.mercatus.org/ (дата обращения: 03.11.2021).

уровня развития информационных технологий допустимо максимально широкое его толкование. По мнению суда, криптовалюта не может быть расценена применительно к ст. 128 ГК РФ иначе как иное имущество.

В тоже время, при определении предмета преступления сложности остаются, так, М.М. Долгиева в своей работе приводит пример, когда предметом преступления фактически признан код (пароль) криптокошелька. Ш. и О., осужденный Сургутским городским судом Ханты-Мансийского автономного округа – Югры по ч. 3 ст. 272, ч. 3 ст. 159 УК РФ. В соответствии с приговором суда Ш. и О. совершили неправомерный доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации, совершенный из корыстной заинтересованности, группой лиц по предварительному сговору, а также мошенничество, то есть хищение чужого имущества путем обмана, совершенное группой лиц по предварительному сговору, в крупном размере. В частности, согласно приговору суда Ш. и О. путем обмана, имея умысел на хищение кодов BTC-e, ввели потерпевшего в заблуждение, пообещав ему обменять код BTC-e на российские рубли, не намереваясь этого делать. В результате чего потерпевший, используя свою учетную запись на созданном подсудимыми сайте, с целью обмена принадлежащего ему BTC-e кода на 10 тыс. долл. США на российские рубли в личном сообщении передал Ш. и О. указанный BTC-e код, рыночная стоимость которого по состоянию на момент совершения преступления, согласно заключению эксперта, составляла 821 100 руб. 00 коп. Тем самым Ш. и О. похитили указанный код и в дальнейшем распорядились им по своему усмотрению, чем причинили потерпевшему материальный ущерб в крупном размере на указанную сумму[19].

Кроме того, в России суд впервые разрешил следователю арестовать украденную криптовалюту. Так Петербургский суд наложил арест на 4 тыс

[19]Долгиева М.М. Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. 2019. №4 (101). С.134.

ETH (криптовалютаЭфириум „Эфир“)— это более 1 млрд рублей, содержащиеся на 24 кошельках обвиняемого в краже криптовалюты.Суд указал, что основным отличием криптоденег от денег является только способ их возникновения, а поскольку понятие криптовалюты не закреплено законодательно, обозначение ее как иное имущество в обвинении, а также в ходатайстве об аресте, допустимо. Криптовалюта используется как средство платежа, инвестиций и накопления сбережений, то есть имеет материальную ценность, соответственно, признается судом как иное имущество и свидетельствует о наличии предмета преступления по смыслу примечания к ст. 158 УК РФ, на которое может быть наложен арест[20].

Отметим, что размер причиненного ущерба по данному уголовному делу определялся путем проведения судебной экспертизы, однако полагаем, что эксперт все же определял не стоимость самого кода, как средства доступа к криптокошельку, а самой по себе криптовалюты.

Е.В. Воскресенская, поддерживая обозначенную позицию указывает, что записи в блокчейне представляют собой абсолютные права и по своей природе схожи с вещами, так как их количество известно, они переходят от владельца к владельцу в строго определенном порядке, не содержат каких-либо прав требования, подобно ценным бумагам[21]. Указанный автор в своей статье предлагает следующее содержание категории «криптовалюты» как дефиниции гражданского права: «Виртуальная валюта (криптовалюта) представляет собой создаваемое и учитываемое посредством применения информационно-телекоммуникационных технологий имущество, не номинированное в валюте Российской Федерации или иностранных государств, которое может использоваться неопределенным кругом лиц для осуществления платежей, не относящееся к электронным денежным

[20]Суд в России разрешил арестовать Ethereum на миллиард рублей URL:https://www.rbc.ru/crypto/news/624c17599a7947515eb896fa (дата обращения 22.04.2022).

[21] Воскресенская Е.В. О необходимости правового регулирования виртуальных валют // Вестник Омской юридической академии. 2018. Том 15. №2. С. 149.

средствам и законным средствам платежа»[22].

С.В. Савельев в своей статье отмечает, что с точки зрения действующего российского законодательства криптовалюты можно рассматривать в качестве иного имущества. При этом они могут также стать валютной ценностью - в случае признания соответствующей криптовалюты в качестве законного платежного средства хотя бы одним иностранным государством. Криптовалюты не являются деньгами в юридическом смысле слова, что, однако, не означает возможность их квалификации в качестве денежных суррогатов при использовании их в качестве оплаты в гражданско-правовых договорах. Он подчеркивает, что квалификация криптовалют в качестве иного имущества не позволяет сама по себе решить вопросы, связанные с определением правовой природы соглашений, заключаемых в отношении их, также сохраняется неопределенность в части возможности отнесения криптовалюты к иному имуществу в принципе[23].

Проанализировав предложенные наукой определения, можно сделать очевидный вывод о том, что они основываются на двух следующих основаниях – это технология, заложенная в основе криптовалюты, то есть технология блокчейн» и назначение данного явления, то есть осуществление платежей, средство платы и т.д. При этом в каждом конкретном определении две указанные информационные составляющие находятся в разном соотношении. По нашему мнению, указание в определениях технической стороны (применительно к криптовалюте) является не совсем удачным ввиду того, что прежде всего предметом нашего внимания является функция криптовалюты, её экономическое и социальное значение. Рассмотрение технической стороны скорее допустимо при анализе содержания самой технологии, на которой криптовалюта базируется. На основании изложенного мы предлагаем авторское определение криптовалюты:

---

[22] Воскресенская Е.В. О необходимости правового регулирования виртуальных валют // Доступ из справ.-прав. системы «КонсультантПлюс».

[23] Савельев А.И. Криптовалюты в системе объектов гражданских прав // Закон. 2019. № 8. С. 138.

«Криптовалюта – это имущество, не являющееся официальной валютой РФ или иной законной формой электронных денег, создаваемое и регулируемое на основе информационно-телекоммуникационных технологий, признанное определенным кругом лиц в качестве средства платежа.

Анализируя имеющиеся законопроекты и положения ГК РФ, можно сделать вывод о том, что законодатель придерживался правильного и последовательного пути по созданию нормативно-правовой базы криптовалюты, начав с фундаментальных позиций, то есть признав (хотя и через понятие «цифровых прав») криптовалюту и иные цифровые активы объектом гражданских прав, тем самым признав законную возможность владения, пользования и распоряжения ими в законном гражданском обороте. При этом следует сказать, что на настоящий момент указанные нормы без принятия специального федерального закона носят, скорее, декларативный характер, поскольку их фактическое применение невозможно.

Подводя итог, следует отметить, что у криптовалют есть перспектива стать основой для фундаментального скачка в развитии цифровой экономики как в России, так и во всем мире, однако для этого необходимо разработать адекватный механизм правового регулирования данного явления. Вместе с тем в настоящее время ни в отечественной, ни в зарубежной доктрине не сложилось единой позиции относительно того, что представляет собой криптовалюта. Действующее на настоящий момент законодательство не учитывает всей специфики этого явления и многогранности понятия. На наш взгляд, в целях удовлетворения постоянно изменяющихся потребностей роста новой цифровой экономики надо обеспечить гибкость при внесении изменений в нормативно-правовую базу в части правового регулирования криптовалют. При этом, определяя правовой режим криптовалют, следует прежде всего учитывать экономическую сущность данного явления. Отсутствие должного правового подхода к регулированию криптовалюты приводит к негативным последствиям, в первую очередь связанным с

увеличением уровня преступности. В этой связи считаем важным рассмотреть вопросы связанные с особенностями использования криптовалютпри совершении преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ, в том числе и как средство конспирации преступной деятельности.

1.2 Использование криптовалют при совершении преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ.

Анализ статистических данных по наркопреступности за последние годы показывает кратное увеличение числа преступлений, совершенных с использованием информационно-телекоммуникационных сетей. Объектами данных преступлений, чаще всего выступают новые синтетические наркотические средства: эфедрон, мефедрон, N-метилэфедрон и синтетические аналоги тетрагидроканнабинола. Предлагаемые к продаже вещества имеют сленговые («скорость», «кристалл», «соль», «мука», «спайс» и т. д.) и торговые названия (MDMB, мефедрон и др.). Средствами совершения являются мессенджеры (Telegram, Brosix, Pidgin, Xabber, Vipole, IM+, Psi), программное обеспечение, шифрующее VPN-соединения, позволяющее обходить блокировку со стороны государственных органов, возможности современных технологий; дистанционные платежные системы (Visa QIWI Wallet, WebMoney, Yandex-Money, QIWI-банк, E-port); приложения для работы с сетью, интернет-программы, поддерживающие OTR-шифрование, а также имеющие специализированные хранилища информации с защитой от несанкционированного доступа (сообщения не сохраняются в системной памяти устройств); приложения, представляющие собой инструмент, обеспечивающий конфиденциальность пребывания в информационно-телекоммуникационной сети «Интернет», с

невозможностью определения IP-адресов выхода на веб-сайты[24].

В последние годы к перечисленным средствам при осуществлении незаконного оборота наркотических средств добавилось и новое: криптовалюта, которая используется как:

а) способ начисления заработной платы «сотрудникам» интернетмагазинов (например, в интернет-магазинах Stuff.store, XTC);

б) средство оплаты за приобретаемые средства (при этом стоимость наркотического средства может снижаться на 10-15 %);

в) способ легализации наркодоходов[25].

Несмотря на высокую практическую значимость, в теории криминалистики до настоящего времени фактически отсутствуют полноценные фундаментальные исследования, раскрывающие механизм использования криптовалюты в преступных целях и методы противодействия указанному виду преступных деяний. Лишь некоторые аспекты процесса расследования отражаются в разрозненных научных публикациях[26].

Лавинообразный процесс интегрирования криптовалюты в механизм незаконного оборота наркотических средств гипотетически возможно объяснить ее основными свойствами:

1. Децентрализацией (нет единого, главного сервера, который бы контролировал все операции).

---

[24]Судницын А. Б., Молоков В. В. Отдельные возможности получения и использования сведений об операциях с криптовалютой при раскрытии и расследовании преступлений // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 213—221.

[25]Земцова С.И. Криптовалюта в незаконном обороте наркотических средств: вопросы деаномизации и ответственности // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 55.

[26]Дворянкин О. А, Клочкова Е. Н. Криптовалюта — новый инструмент наркобизнеса // Наркоконтроль. 2018. № 4. С. 19—22.; Судницын А. Б., Молоков В. В. Отдельные возможности получения и использования сведений об операциях с криптовалютой при раскрытии и расследовании преступлений // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 213—221.; Родивилин И. П., Родивилина В. А. Криптовалюта как объект преступления // Деятельность правоохранительных органов в современных условиях: сб. мат-лов XXIII междунар. научно-практ. конф. В 2-х тт. — Иркутск: Восточно-Сибирский институт МВД России, 2018. С. 262—265.

2. Трансграничностью и транснациональностью.

3. Анонимностью. В частности, «в отдельных альтернативных платежных системах внедрены специальные технологические решения, например, так называемые миксеры, которые создают дополнительные препятствия для идентификации криптовалютных транзакций и их участников. Все это позволяет достаточно успешно скрывать личности отправителей и получателей криптовалюты и утаивать истинные цели и содержание операций. Дополнительно этому способствует полное отсутствие контроля за движением платежных средств, представленных криптовалютой, со стороны каких-либо определенных внутренних органов. Ведь устройство большинства альтернативных платежных систем таково, что ограничивается лишь валидацией транзакций, т. е. проверкой их соответствия протоколу той или иной экосистемы, и не предусматривает наличие механизмов проверки таких транзакций на предмет соответствия законодательству»[27].

4. Совершением транзакций в режиме P2P (равенство пользователей, транзакции осуществляются напрямую), при отсутствии посредников.

5. Высокой скоростью обработки транзакций.

6. Отсутствием банковского, валютно-экспертного и налогового контроля, обязательного контроля, предусмотренного системой противодействия отмывания доходов и финансирования терроризма и незаконного оборота наркотических средств.

7. Использованием криптовалюты в качестве мобильного средства сбережения. «Приватные ключи, представляющие собой сотни миллионов долларов, можно хранить на крошечном USB-накопителе и легко переносить в любое место»[28].

8. Возможностью обмена на другие криптовалюты или фиатные

[27] Кучеров И. И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. 2018. № 12. С. 18.

[28]Долгиева М. М. Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы рос. права. — 2019. № 4. С. 128—139.

деньги.

Указанные признаки крипатовалюты позволяют ей функционировать вне банковского сектора, в связи с чем применение контроля со стороны банков и государственных органов невозможно.

Существует точка зрения, согласно которой криптовалюта выступает характерным примером инновации экономики нракобизнеса. Именно использование криптовалют позволяет наркодилерам посредством задействования новых финансовых механизмов обеспечивать независимость экономики террора от легальных экономических структур в процессе производства и потребления необходимых им товаров и услуг. Создаваемые террористами собственные каналы перемещения финансовых средств на основе использования современных альтернативных платежных систем позволяют доставлять необходимое финансирование преступным группам по всему миру. При этом констатируется, что инновационный характер криптовалюты делает практически бессмысленными все ранее существовавшие меры борьбы международных организаций и государств с финансированием террористических организаций и групп[29].

По данным руководителя рабочей группы Госдумы Российской Федерации по оценкам рисков оборота криптовалюты, доктора юридических наук Э.Л. Сидоренко, в 2015 году количество зафиксированных фактов использования виртуальной валюты для отмывания преступных доходов не превышало 5 % от общего объема криптовалюты, а в 2018 г. этот показатель превысил 40 %[30].

В 2021 году в сфере противодействия легализации (отмыванию) доходов от незаконного оборота наркотиков в отчетном периоде зарегистрировано 554 преступлений по фактам легализации (отмывания) доходов, полученных от незаконного оборота наркотиков, что на 12,1%

[29] Сальников Е.В. Сальникова И.Н. Криптовалюта как иновация экономики терророра // Науковедение. 2016. № 3. С. 33.

[30] Сидоренко Э.Л. Наркотики и криптовалюта: новые криминологические тренды // Наркоконтроль. 2018. № 2. С. 8-13.

превышает показатель прошлого года. Установленная сумма легализованных наркодоходов(денежных средств или иного имущества по оконченным предварительным расследованием уголовным делам) превысила показатель прошлого года, составив 587 млн. 212 тыс. рублей. Значительных результатов удалось достичь благодаря организации эффективного взаимодействия с компетентными органами и подразделениями финансовой разведки государств СНГ и иных зарубежных стран.

Справедливости ради следует оговориться, что использование криптовалюты в преступных целях хотя и имеет место, тем не менее не может быть однозначно охарактеризовано как тотальное. К примеру, Управлением по борьбе с наркотиками США (DEA) констатировано сокращение доли использования Биткойна в преступной деятельности. Как отметили представители этого правоохранительного ведомства, большинство переводов носят преимущественно спекулятивный характер и лишь примерно каждая десятая транзакция имеет криминальную подоплеку, хотя в номинальном выражении объем последних за последние пять лет значительно возрос. Одновременно обращено внимание на то, что отсутствие традиционных финансовых посредников и администраторов в криптовалютных платежных системах создает известные проблемы при расследовании, которые, впрочем, являются устранимыми[31].

В общем виде схема легализации преступных доходов выглядит следующим образом:

1. Конвертирование наркоденег в криптовалюту;
2. Перевод криптовалюты в любую валюту по выбору;
3. Обналичивание денежных средств.

Как отмечает В.А. Ализаде и А.Г. Волеводза, «организаторы и руководители преступных организаций, деятельность которых сосредоточена

[31] Russo, Camila. Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now. Bloomberg. [Электронный ресурс] URL: https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now?srnd=cryptocurriences (дата обращения: 12.11.2021 г.).

в сфере незаконного оборота наркотиков, распределяют денежные средства, полученные от преступной деятельности, между их участниками,предварительно совершая с ними операции по переводу денежных средств в криптовалюту, и в таком виде по каналам сети Интернет направляют конкретным исполнителям на счета их электронных кошельков (чаще всего «QIWI-кошельки»). Получатели криптовалютыв последующем на онлайн-биржах обменивают их на рубли и используют в своих целях. Деньги с использованием программ Интернет-банкинга переводятся с дроблением сумм платежей, а именно — путем проведения финансовых операций через системы денежных переводов без открытия счета в суммах менее 15 000 руб. Это позволяет избежать идентификации участников финансовых операций и обеспечить уклонение от процедур обязательного контроля со стороны кредитной организации[32].

Центральное место в легализации преступных доходов с использованием криптовалюты занимают криптобиржи (криптосервисы) различных типов. К указанным можно отнести следующие варианты:

1) Одноранговых транзакции типа «человек-человек»;

2) «Биткойн»-автоматов (криптоматов, криптотерминалов);

3) Смесителей, позволяющих запутывать цепочки транзакций. Например, некоторые из них устроены так, что один пользователь может купить за криптовалюту товар, необходимый для другого пользователя, а последний, в свою очередь, отправляет преступнику реальные деньги за вычетом определенной суммы (аналогия банковской комиссии). В данном случае выигрывают оба – преступник получает реальные деньги, а покупатель – товар со скидкой;

4) Нелегальных обменных сервисов. К указанным можно отнести 365cash.com, NetEx24.com, Z-exchange.com, 100btc.pro, Buy-Bitcoins.com и

[32]Ализаде В.А. Волеводз А.Г. Судебная практика применения ст. 174¹ УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты // Наркоконтроль. 2017. № 4. С. 9.

другие. Данные сервисы предоставляют возможно обмена криптовалют на рубли;

5) Онлайн-игр. Согласно аналитическому отчету компании «TrendMicro», преступники все чаще стали использовать одновременно виртуальную и игровую валюту ввиду отсутствия их правового статуса для легализации преступных доходов. Дляэтогопокупаетсявалютаигр Minecraft, FIFA, World of Warcraft, Final Fantasy, Star Wars Online, GTA 5, NBA и Diablo. В последующем она продается за криптовалюту, а криптовалюта обменивается на специальных сервисах конвертации[33].

Практика применения судами статьи УК РФ о легализации преступных доходов по уголовным делам, связанным с незаконным оборотом наркотиков, является весьма неоднозначной. В данном случае мы подразумеваем тот факт, что в одних уголовных дел по схожим обстоятельствам виновным лицам дополнительно вменяется ст. 174-174[1] УК РФ, а в других – нет.

Примером легализации преступных доходов может послужить следующая судебная практика. Так, Ленинским районным судом г. Саранска (Республика Мордовия) П.А. Пинчук признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 210, ч. 3 ст. 30, п. «а» и «г» ч. 4 ст. 228[1], ч. 1 ст. 174[1] УК РФ[34]. Согласно приговору Пинчук и иные лица умышленно вошли в состав преступного сообщества (преступной организации), деятельность которого была направлена на совместное систематическое совершение тяжких и особо тяжких преступлений, связанных с незаконным сбытом через информационно-телекоммуникационную сеть Интернет наркотических средств на территории г. Саранска Республики Мордовия. Осуществляя деятельность курьера и закладчика, Пинчук неоднократно оборудовал тайники с наркотиками, о чем посредством

[33]Земцова С.И., Галушин П.В., Карлов А.Л. Указ. соч. С. 30.

[34] Приговор от 3 июля 2017 г. по делу № 1-125/2017 // Судебные и нормативные акты РФ (СудАкт) [сайт] (дата обращения: 20.11.2021). Далее цитирование приговора осуществляется без дополнительных ссылок на него.

интернет-переписки сообщал соответствующему оператору. За осуществленные «закладки» от бухгалтера сообщества он получал оплату в криптовалюте (Биткойнах), дистанционно зачисляемой по сети Интернет на его специальный счет. Совершая преступления в сфере незаконного оборота наркотических средств в составе организованной группы на территории г. Саранска, имея умысел на придание правомерного вида владению, пользованию и распоряжению средствами, полученными от незаконной деятельности в Биткойнах, Пинчук через онлайн интернет-биржу обменивал их на российские рубли, после чего переводил на заведенный им обезличенный «Qiwi-кошелек» в АО «КИВИ-Банк», с которого впоследствии путем совершения неоднократных финансовых операций перечислял на счет банковской карты в ПАО АККСБ «КС Банк», оформленный на его имя. В последующем денежные средства Пинчуком обналичивались через банкоматы, установленные на территории г. Саранска, и использовались им на личные нужды. В описательно-мотивировочной части приговора суд указал: «действия Пинчука суд квалифицирует по части первой статьи 174[1] УК РФ как совершение легализации (отмывания) денежных средств, приобретенных лицом в результате совершения им преступления, то есть совершение финансовых операций и других сделок с денежными средствами, приобретенными лицом в результате совершения им преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами, поскольку Пинчук в период с 9 по 13 ноября 2015 г. совершил неоднократные банковские финансовые операции по переводу денежных средств, полученных им за сбыт наркотических средств в составе организованной группы, а именно криптовалюты — Биткойн, через онлайн интернет-биржу в российские рубли на общую сумму не менее 4466 рублей 06 копеек на обезличенный «Qiwi-кошелек», оформленный в АО «КИВИ-Банк», и перечислению указанных денежных средств с «Qiwi-кошелька», оформленного в АО «КИВИ-Банк», на счет банковской карты, открытой в ПАО АККСБ «КС Банк», оформленной на имя по-

следнего, тем самым легализовал денежные средства, приобретенные в результате преступной деятельности, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами, которые в последующем были использованы им на личные нужды».

Также приведем пример, когда при наличии признаков легализации преступных доходов, указанная статья не вменяется. Так, например, согласно приговору Саратовского районного суда Саратовской области от 31 мая 2017 года по делу № 1-1-76/217, органами предварительного следствия А.А. Даниленко, обвинялась только в совершении преступления, предусмотренного ч.3 ст. 30 и ч.5 ст.228.1 УК РФ. Суд признал ее виновной в этом преступлении и постановил обвинительный приговор. В описательно-мотивировочной части приговора в числе иного указано на исследование доказательств (показаний подсудимой, протокола осмотра и других), из совокупности которых следует, что при задержании у подозреваемой была обнаружена банковская карта, принадлежащая ей. Сама Даниленко пояснила, что через изъятую банковскую карту Сбербанка России она обналичивала денежные средства, которые ей перечисляли в «биткоинах» в качестве заработной платы за незаконный сбыт наркотиков, которые она в дальнейшем конвертировала в системе «Биткойн» в рубли и переводила на свой «QIWI-кошелек» и в дальнейшем выводила на изъятую банковскую карту[35].

Таким образом можно сделать вывод о том, что органы предварительного следствия по каким-то причинам, даже при наличии признаков легализации преступных доходов, по средствомкриптовалюты не инкриминируют данный состав обвиняемым.

[35] Приговор Свердловского районного суда г. Костромы от 11 мая 2017 г. по делу № 1-136/2017 в отношении А.В. Новицкого // Судебные и нормативные акты РФ (СудАкт) [Электронный ресурс] URL: https://sudact.ru/ (дата обращения: 15.11.2021)

Разнообразие следственной и судебной практики Ализаде В.А. и Волеводз А.Г. объясняют следующими причинами:

- правовым вакуумом в части регулирования блокчейн-технологий и оборота криптовалюты»;

- незнанием и непониманием фактической природы последней;

- неверным пониманием правовой сущности оборота криптовалюты»[36].

С.И. Земцова, П.В. Галушин, А.Л. Карлов полагают, что основной причиной является отсутствие методики расследования наркопреступлений, совершенных с использованием криптовалюты»[37].

С предложенными позициями нельзя не согласиться. Кроме того, криптовалюта в настоящее время является достаточно неизведанным явлением (особенно для российских правоприменителей, чей круг знаний и опыта ограничивается юридической сферой). Вместе с тем и статьи, регламентирующие уголовную ответственность за легализацию преступных доходов, не являются распространенными. Так, согласно сведениям Судебного департамента при ВС РФ, за 2021 год по статьям 174-174[1] УК РФ осуждено 18 человек, 2 человек оправдано, за 2020 год 33 человека осуждено, 2 человек оправдано; за 2018 год осуждено 33 человека, оправдано – 0.

Подводя итог, следует сказать, чтокриптовалюта выступает характерным примером инновации экономики нракобизнеса. Именно использование криптовалют позволяет наркодилерам посредством задействования новых финансовых механизмов обеспечивать независимость экономики террора от легальных экономических структур в процессе производства и потребления необходимых им товаров и услуг. Использование криптовалюты в качестве средства легализации преступных

[36]Ализаде В.А., Волеводз А.Г. Неприменение ст. 174.1 Уголовного кодекса РФ по делам о наркопреступениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. 2018. № 1 (50). С. 5-13.

[37]Земцова С.И., Галушин П.В., Карлов А.Л. Указ. соч. С. 33.

доходов позволяет осуществлять сделки по купле-продаже наркотических средств без оставления значительных следов в информационной среде. В целях минимизации использования криптовалюты в преступных целяхнеобходимо выполнение следующих мероприятий:

1. Идентификация клиентов сервисов, связанных с криптовалютными операциями на основании Федерального закона от 7 августа 2001 г. N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

2. Передача указанных выше сведений о клиентах и их операциях Федеральной службе по финансовому мониторингу, Федеральной налоговой службе и иным уполномоченным органам власти. Данные положения наиболее полным образом соответствуют относительно недавно обновленным рекомендациям ФАТФ[38];

3. Вменение обязанности получения сервисами по операциям с криптовалютой лицензии на осуществление деятельности, а также обязанности взаимодействия аккредитованными провайдерами. Указанное способствует минимизации риска трансграничного характера криптовалют;

4. Вменение обязанности страхования рисков утраты средств клиентов и выплаты компенсаций клиентам в случае утраты их средств. Данное положение должно способствовать повышения информационной безопасности сервисов при оказании ими услуг.

1.3. Криптовалюта как средство конспирации преступных действий.

Сегодняшнее положение вещей таково, что современная преступность представляет собой условную «лакмусовую бумажку», которая отражает состояние общественных отношений, развитие технологий и т.д. Указанная

[38] FATF/GAFI. Regulation of virtual assets. Paris, 19 October 2018. [Электронный ресурс]
URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html (дата обращения: 20.11.2021).

зависимость особенно хорошо прослеживается в сфере наркопреступности. С развитием телекоммуникационных технологий покупка-продажа наркотиков стала быть «бесконтактной», что создало достаточно серьезные сложности для правоохранительных органов в силу того, что возникла потребность разработки и использования новых методик раскрытия и расследования преступлений в сфере наркотических средств.

Центральное место в современной наркопреступности занимает интернет-сеть Даркнет, которая изначально преследовала благие цели. Данная сеть состоит из интернет-сайтов, доступ к которым невозможен через общеизвестные поисковые системы («Google», «Yandex», «Rambler»).Информациявнутри данных сайтов спрятана от большинства обычных пользователей обычной сети Интернет («Чистой сети»). Особенность ДаркНета состоит в том, что в ней практически невозможно отследить злоумышленника.

Дремлюга Р.И. отмечает, что использованию ДаркНета в преступных целях способствуют его следующие особенности[39]:

1. Анонимность, которая основана на так называемой «луковой» маршрутизации, обуславливающая невозможность отследить пользователя сети. Используя в качестве средства платежакриптовалюту, преступник делает невозможным отслеживание движения своих финансовых потоков.
2. Шифрование информации, передаваемой в Даркнете. Указанное обуславливает трудности в противодействии нелегальнойдеятельности;

3. Трансграничная природа Даркнета, обусловленной стукнутой самой сети. Интернет позволяет совершатьпреступления на территории другого государства испособствует кооперации и консолидации международных преступных группировок и сообществ независимо от вида деятельности, но интернет-ресурсы (сайты) в сети Интернет, так или иначе, обладают географической или национальной привязкой. В отличие от сети Интернет

[39]Дремлюга Р.И. Незаконный оборот наркотиков и крипторынки: угрозы и вызовы правоохранителю // Международное сотрудничество и зарубежный опыт. 2018. № 2. С. 33.

именасайтов Даркнетаникак не отражают национальнуюпринадлежность, а так как данные о сети хранятсяраспределенно на территории многих стран. Для открытия сайтане требуется регистрация и следование национальным нормам.

Для того, чтобы подчеркнуть взаимосвязь Даркнета и наркопреступности, обратимся к отчету Управления по всемирному состоянию спроса и предложения на наркотики, опубликованному в 2017 г.. Согласно нему, торговля наркотиками через Даркнетпрогнозируемо будет демонстрировать беспрецедентный рост (около 50 процентов вгод)[40]. В Великобритании 25% из всех наркотиков, приобретаемых через Интернет, покупается в Даркнете. В США эта цифра достигает 13%. Среднее значение за пределами этих стран — 8%[41].

Около 70% всех продавцов на крипторынкахДаркнетапредлагают наркотики, а не другие видынелегального товара. Исследование, проведенноев январе 2016 г., показало, что на 8 крупнейшихкрипторынках (AlphaBay, Cryptomarket, DarkNetHeroesLeague, Dreammarket, FrenchDarkNet, Hansa,NucleusandPython) было размещено более 100 000объявлений о продаже наркотиков и психоактивных веществ[42].

В связи с изложенным мы можем сделать вывод о том, что технология Даркнета была воспринята людьми как средство, которые может быть использовано в преступных целях, что не оправдало надежд, которые преследовались изначально создателями принципов его работы. А ведь на начальном этапе главными спонсорами разработок являлись ВМС США (2001-2006), Национальный научный фонд (2007), Google(2008-2009), Национальная исследовательская лаборатория США (2006-2010),

[40] World Drug Report 2017, Presentation, UNDOC. [Электронныйресурс] URL: http://www.unodc.org/wdr2017/field/WDR_2017_presentation_lauch_version.pdf (датаобращения: 22.11.2021)

[41]Дремлюга Р.И. Незаконный оборот наркотиков и крипторынки: угрозы и вызовы правоохранителю // Международное сотрудничество и зарубежный опыт. 2018. № 2. С. 33.

[42]Дремлюга Р.И. Незаконный оборот наркотиков и крипторынки: угрозы и вызовы правоохранителю // Международное сотрудничество и зарубежный опыт. 2018. № 2. С. 35.

Национальная христианская организация (2010-2012), Фонд Форда (2012-2014), Департамент США по защите прав (2013-2016), Министерство иностранных дел Германии (2015)[43].

В подавляющем большинстве случаев криптовалюта является основным средством оплаты наркотиков. Первое серьезное упоминание криптовалюты в указанном качестве датируется 2013 годом в связи с расследованиями уголовного дела, связанного с Интернет-рынком «SilkRoad» (Шелковый путь). Оплата за товары в подавляющем большинстве случаев производилась с использованием криптовалюты, а выбор в её пользу был сделан ввиду ее анонимности и трудностей технического характера установления и отслеживания финансовых транзакций[44]. Что примечательно, последующие проекты такие как «Evolution» и «SilkRoad 2.0» посредством учета и устранения ошибок первого Интернет-рынка, смогли увеличить собственный доход на целых 100 млн. долларов США. При этом данные площадки обладали схожим функционалом, но лучшим дизайном, маркетингом и надежностью[45].

Если говорить о РФ, то на территории нашей страны в Даркнете действуют два крупнейших русскоязычных интернет-форума: «LegalRC» и «WayAWay». Цель данных форумов – реклама и продажа наркотических средств. Они содержат информацию о видах наркотиков, ценах, способах их приобретения, а также иных предметов и документов, запрещенных к в законном гражданском обороте. С конца октября 2016 г. также действует крупнейшая торговая площадка «HYDRA», в состав которой входит около 400 магазинов. Данный сайт имеет структуру, схожую с аналогичными ресурсами, действующими в ЕС и США. Сделки и оплата происходят непосредственно на площадке. Оплата производится исключительно с

[43] Безопасность электронного банкинга / А.М. Сычев, П.В. Ревенков, А.Б. Дудка. М., 2017. 293.

44 Тумаков А.В., Петраков Н.А. Правовой режим криптовалюты // Государственная служба и кадры. 2021. № 5. С. 174.

[45]Земцова С.И., Галушин П.В., Карлов А.Л. Указ. соч. С. 21.

использованием криптовалютыБиткоин. Площадка охватывает все сферы теневого бизнеса, от продажи всех видов наркотиков до торговли поддельными документами, банковскими картами, оформленными на подставные данные, специального оборудования для слежки и съема информации, а также предоставления различных информационных услуг. Ресурсы сайта «HYDRA» размещаются на технических площадках хостинг-компании «Cloudflare» (США, Сан- Франциско)[46].

Использование криптовалюты для покупки ипродажи наркотиков на крипторынкахозначает,что операции в сети Даркнетстановятся еще болееанонимными. Именно поэтому все больше и большепреступников выбирают криптовалюты и крипторынки для своей нелегальной активности, сводя на нетпопытки правоохранительных органов по пресечениюих деятельности и обходя блокировки доступа к сетевым ресурсам.

Имеющиеся данные и прогнозы, сделанные ООН, позволяют нам сделать вывод, что криптовалюта оказала достаточно серьезное влияния на развитие наркопреступности, расширив сферу влияния последней, её возможности, каналы поставок и сбыта. Приобретение наркотиков стало более анонимным, и, как следствие, безопасным как для потребителей, так и для организаторов.

Человеческое общество так устроено, что на каждое действие (технологию, явление и т.д.), создается противодействие, нивелирующее плюсы и достоинства первого. Указанное философское положение справедливо и для криптовалюты. В данном случае мы говорим о разработке программ по идентификации пользователей криптовалютных сервисов.

Одним из таких сервисов является «Crystal»от поставщика блокчейн-решений «BitfuryGroup». Цель данного сервиса состоит в выявлении и расследовании криминальной деятельности в блокчейне «Биткойн»путем отслеживание перемещения подозрительных транзакций до конечного

[46]Трунцевский Ю. В. Цифровая (виртуальная) валюта и противодействие отмыванию денег: правовое регулирование // Банковское право. 2018. № 2. С. 18—28.

получателя или точки сбыта криптовалюты правоохранительными органами. Структура блокчейна Биткойна содержит информацию обо всех транзакциях, доступную всем участникам сети. Алгоритмы сервиса «Crystal» загружают и обновляют данные из блокчейна, а также собирают в сети Интернет публично доступную информацию о владельцах кошельков криптовалюты. При этом вся информация обрабатывается так, что данные в дальнейшем были пригодны для аналитики и могли быть представлены пользователю в удобном формате. Результаты обработки сохраняются в заде данных[47].

Основными критериями назначения степени риска являются подтвержденная публичная информация о нелегальной деятельности конкретных участников блокчейнаБиткоина и наличие транзакций с ними прочих участников. Например, если участник А. взаимодействовал с известным высокорисковым участником В., то участник А. также «попадает под подозрение», то есть алгоритм присваивает ему некий повышенный уровень риска. Наличие или отсутствие риска отображается в интерфейсе приложения с помощью красных и зеленых меток соответственно.При этом «Crystal» является аналитическим инструментом и не дает оценок законности транзакций. Считать ту или иную транзакцию сомнительной или незаконной прерогатива правоохранительных органов.

Отслеживать информацию о транзакциях может либо сам пользователь «Crystal», либо сторонняя программа: «Crystal» содержит API для интеграции с аналитическим программным обеспечением пользователя. Сбор персональных данных «Crystal» не производит[48].

Разработчики отмечают, что лежащие в основе анализа данных эвристические алгоритмы, по своей природе не дают стопроцентного результата. Поэтому решения, выносимые сервисом «Crystal», не являются

[47]В компании Bitfury появилась технология по отслеживанию ненадежных транзакций URL:https://crypt-mining.net/news/v-kompanii-bitfury-poyavilas-texnologiya (дата обращения 18.05.2022).

[48]В компании Bitfury появилась технология по отслеживанию ненадежных транзакций URL:https://crypt-mining.net/news/v-kompanii-bitfury-poyavilas-texnologiya (дата обращения 18.05.2022).

категоричными – все остается в зоне ответственности пользователя. Интерес к данному инструменту с момента создания был проявлен со стороны финансового сектора (банков, консалтинговых компаний, финансовых регуляторов), а также киберподразделений силовых структур[49].

Наряду с ним, в конце 2018 года был представлен «KnowYourTransaction» (KYT) компанией «Chainalysis». Цель данного сервиса состоит в отслеживании людей, которые участвуют в незаконной деятельности, связанной с криптовалютами. Среди постоянных клиентов «Chainalysis» – Федеральное бюро расследований США (ФБР), Администрация по борьбе с наркотиками (DEA) и Европол.Продукт «KYT» от «Chainalysis» предоставляет обратную связь по транзакциям в реальном времени и отправляет соответствующую информацию на биржу в «движок обработки транзакций»[50].

Подводя итоги настоящего вопроса хотелось бы отметить следующее:

а) широкое распространение криптовалюты в сфере наркобизнеса обусловлено теми преимуществами, которыми её наделяют принципы работы самой технологии блокчейн. К таким чертам мы отнесли следующее: анонимностью, трансграничностью, доступность, скорость транзакций и т.д.;

б) современные тенденции таковы, что роль криптовалюты «Биткойн» в настоящее время в преступной среде уменьшается по причины разработки и совершенствования сервисов, направленных на деанонимизацию сделок данной криптовалютой. В связи с этим набирают популярность иные виды криптовалют, которые обладают более высокими конспиративными характеристиками;

---

[49]В компании Bitfury появилась технология по отслеживанию ненадежных транзакций URL:https://crypt-mining.net/news/v-kompanii-bitfury-poyavilas-texnologiya (дата обращения 18.05.2022).

[50]Земцова С.И., Галушкин П.В., Карлов А.Л. Криптовалюта как объект криминалистического исследования при расследовании преступлений в сфере незаконного оборота наркотических средтсвт и психотропных веществ. Красноярск. 2020. С. 37.

в) имеется высокая потребность в рассмотрении и принятии комплекса нормативных положений, изложенных в проекте федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях (в части установления ответственности для владельцев интернет-ресурсов, а также хостинг провайдеров за размещение (распространение) запрещенной информации о наркотических средствах и психотропных веществах)», разработанного МВД России совместно с Минкомсвязью России, ФСБ России и Минюстом России.

Глава 2. Вопросы доказывания по уголовным делам с использованием криптовалют.

2.1 Выявление и документирование преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, совершенных с использованием криптовалют.

Рассматривая вопросы особенностей выявления и документирования преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, совершенных с использованием криптовалют стоит отметить, наша страна является правовым государством. Согласно Конституции РФ, высшей ценностью является права и свободы гражданина и человека, в связи с чем такие права и свободы человека могут быть ограничены только лишь судом путем вынесения соответствующего решения. Указанное является конституционной гарантией каждого от незаконного преследования и нарушения его прав.

Оперативно-розыскная деятельность – это, прежде всего, деятельность поискового характера. Её главной целью является поиск информации о признаках преступной деятельности во всем многообразии общественных отношений, в том числе и среди государственных структур и органов. Достаточно часты случаи, когда информация, представляющая интерес входит в охраняемую государством сферу, а ознакомление с ней предполагает ограничение конституционного права физического лица или организации. Изложенное обуславливает необходимость среди проводимых оперативно-розыскных мероприятий выделять такие, которые осуществляются на основании судебной санкции (судебного решения). Без судебного решения подобного рода оперативно-розыскные мероприятия будут являться незаконными, а действия должностных лиц будут содержать признаки правонарушений или преступлений.

Однако для наибольшего понимания настоящего вопроса определимся для начала с правами, которые чаще всего ограничиваются в рамках

оперативно-розыскной деятельности. Согласно опроса сотрудников оперативных подразделений, чаще всего предметом судебного санкционирования являются следующие конституционные права граждан:

1. Право граждан на тайну переписки и телефонных переговоров;
2. Право граждан на охрану банковской тайны;
3. Право граждан на тайну персональных данных;
4. Право граждан на неприкосновенность жилища.

Анализ данной нормы Конституции РФ позволяет нам выделить следующие ОРМ, которые затрагивают права граждан при выявлении и документировании преступлений в сфере незаконного оборота накротических средств и психотропных веществ, совершенных с использованием крипотвалют, и соответственно, проводимые на основании судебной санкции.

Контроль почтовых отправлений, телеграфных или иных сообщений. Порядок проведения данного мероприятия заключается в том, что сотруднику при проведении данного мероприятия необходимо подготовить постановление о возбуждении перед судом ходатайства на проведение данного мероприятия, за подписью руководителя правомочного на осуществление ОРД, после чего подготовить постановление о разрешении суда на проведение мероприятия и идти получать судебное санкционирование на проведение мероприятия. Фактически провести данное мероприятие возможно лишь на таких почтовых сервисах как mail.ru или yandex.ru. ввиду того, что сервера данных сервисов находятся на территории РФ, и соответственно, подчиняются юрисдикции нашей страны. Все остальные почтовые сервисы, как правило, отказывают в предоставлении запрашиваемой информации. Конечно, методы контроля почтовой корреспонденции, связанной с «Почтой России», отличаются от контроля сообщений на «электронной почте» в сети «Интернет». Тем не менее, данное ОРМ позволяет не только контролировать электронные сообщения, но и в

определенных случаях, создавать препятствия для обмена сообщениями между разрабатываемыми лицами.

Немаловажным в сети «Интернет» является ОРМ, именуемое **«Наведение справок».**Различные доктринальные толкования данного ОРМ определяют его по-разному. Так, А.С. Бахта под данным ОРМ понимает «непосредственное изучение документов, содержащих сведения, представляющие оперативный интерес, а также направление запросов о предоставлении таких сведений в государственный органы, предприятия, учреждения и организации, имеющие информационные системы»[51];

По мнению И.Ю. Климова под данным мероприятием следует понимать: «способ сбора информации, необходимой для решения задач ОРД, путём непосредственного изучения документов, а также направления запросов в организации, учреждения»[52];

К.К. Горяинова, В.С. Овчинского, Г.К. Синилова считают, что наведение справок: «мероприятие, направленное на получение информации о физических лицах, о фактах и обстоятельствах, имеющих значение для решения задач ОРД, путем непосредственного изучения документов, материалов, баз данных, направления запросов на предприятия, в учреждения и организации, другим юридическим, а также физическим лицам, которые располагают или могут располагать указанной информацией»[53];

А.Ю. Шумилов считает, что наведение справок есть «получение фактической информации, имеющей значение для решения задач ОРД, путем направления запроса (официального или неофициального характера) соответственно юридическому или физическому лицу, располагающему или

[51]Федеральный закон «Об оперативно-розыскной деятельности»: научно-практический комментарий / под ред. д-ра юрид. наук, проф А.С. Бахты. Хабаровск, 2013. С.54.

[52]Оперативно-розыскная деятельность: учебник для студентов вызов, обучающихся по специальности «Юриспруденция» / под ред. И.А. Климова. М., 2014. С.311.

[53]Теория оперативно-розыскной деятельности / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. М., 2006. С.182

могущему располагать таковой, а равно её получение путем непосредственного ознакомления с соответствующим материальным носителем»[54].

По мнению Шумилова И.И., наведение справок – это «ОРМ, заключающееся в сборе информации о лицах и фактах, представляющих оперативный интерес, в целях решения задач ОРД, осуществляемое путем изучения документов (в том числе архивных) и (или) направления запросов как в государственные, включая правоохранительные, органы, так и в любые учреждения и организации, независимо от их принадлежности, имеющие информационные системы, располагающие информацией, сохраняемой в других формах»[55].

По мнению Дубоносова Е.С., его следует трактовать как «способ сбора информации, необходимой для решения задач ОРД путем непосредственного изучения документов, а также направления запросов в организации, учреждения»[56] и т.д.

Анализ указанных выше определений показывает, что все авторы выделяют две основных формы реализации рассматриваемого ОРМ:

1. Сбор информации;

2.Непосредственное ознакомление оперативного сотрудника с материальными носителями или документами;

3. Направление запроса.

По нашему мнению наиболее верной является позиция предложенная А.В. Агрковым, согласно которой: «наведение справок — изучение оперативной информации, получаемой путем ознакомления с содержанием ее имеющихся носителей, либо направления запросов о предоставлении оперативной информации юридическим и (или) физическим лицам,

[54]Оперативно-розыскная энциклопедия / Авт. – сост. проф. А.Ю. Шумилов. М.: Изд-ль Шумилова И.И., 2004. С.159-160.

[55] Ривман Д. В. Комментарий к Федеральному закону «Об оперативно-розыскной деятельности». СПб., 2003. С.98.

[56] Дубоносов, Е. С. Оперативно-розыскная деятельность: учебник и практикум для прикладного бакалавриата. 5 изд., перераб. и доп. М., 2016. С.81.

возможно ей располагающим, с последующим ознакомлением с ответами на запросы, либо введения поисковых запросов в электронныхинформационных сетях в целях решения тактических задач ОРД»[57].

Сразу обозначим, что данное мероприятие в раде случаев действительно требует судебного санкционирования. В частности, при направлении запросов, направленных на ограничение банковской и иной охраняемой государством тайны. Применительно к сети «Интернет» могут возникнуть следующие ситуации, когда для того, чтобы получить информацию, оперативный сотрудник должен обратиться в суд:

- при направлении задания в БСТМ, для проведения СТМ, предоставляется возможным получить сведения об ip-адресе, который используется для совершения преступлений.

- для получения выписок по расчетному счету, на который перечислялись похищение денежные средства.

В ходе проведения научного исследования нами был проведен опрос оперативных сотрудников, которые пояснили что очень активно проводят данное оперативно-розыскное мероприятие в сети «Интернет».

Стоит отметить, что оперативность передачи запросов и ответов на них является одной из проблем указанного мероприятия на сегодняшний день. В связи с этим с рядом организаций создаются специальные каналы быстрой связи и ответа на запросы. Например, в Омской области налажена работы с предоставлением запросов с ПАО «Сбербанк России», так при УМВД России по Омской области создана специальная группа, которая работает с данным банком путем направления запросов и предоставления ответов в онлайн режиме. Сотрудникам, которым необходимо истребовать ответ из ПАО «Сбербанк России» передают свой запрос в данную группу, и они далее его обрабатывают и передают запрос адресату, ответ на запрос поступает в течении 2-3 дней, что существенно сокращает истребование ответа, ответ

[57]Агарков А.В. Содержание оперативно-розыскного мероприятия наведение справок» в современные условия // Вестник Кузбасского института. 2018. № 2 (35). С.123.

направляется в электронном виде с электронной подписью, а далее может быть перенесен на бумажный или электронный носитель. Считаем, что такая практика очень успешна и актуальна, поскольку указанный банк является одним из лидеров на рынке и очень часто денежные средства снимаются именно с счетов, открытых в ПАО «Сбербанк России», вместе с тем полагаем, что указанная практика может быть использована и другими организациями.

Получение компьютерной информации.

Федеральным законом от 6 июля 2016 г. № 374-ФЗ[58] введено новое оперативно-розыскное мероприятие – «получение компьютерной информации». Ни федеральный закон, ни подзаконные акты, в том числе ведомственные нормативные правовые акты МВД России, не раскрывают содержания данного мероприятия. Нет его и в модельном законе об оперативно-розыскной деятельности[59].

Несмотря на относительную новизну этого мероприятия, подходы к уяснению его содержания в научной литературе уже сформулированы. Так, Р. Р. Мамлеев дает следующее определение получению компьютерной информации: «Это совокупность средств и способов исследования компьютерной системы с целью обнаружения и документирования материальных следов, сопутствующих подготовке или совершению преступлений, которые могут содержаться в компьютерной системе в форме

[58] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : федеральный закон от 6 июля 2016 г. № 374-ФЗ // СПС «КонсультантПлюс».

[59] Модельный закон об оперативно-розыскной деятельности (в редакции Постановления Межпарламентской Ассамблеи государств — участников СНГ от 16 ноября 2016 г. № 27-6). URL: docs.cntd.ru/document/902050857 (дата обращения: 16.05.2022)

электрических сигналов, независимо от средств их хранения, обработки и передачи»[60].

По утверждению С.В. Баженова руководство ФСБ России в своих ведомственных актах разъясняя данное мероприятие полагает, что оно провидится по решению суда соответствующими оперативно-техническими подразделениями, что позволит осуществлять копирование виртуальной информации, ее изъятие с жестких дисков сетевых компьютеров или серверов в информационно-телекоммуникационной сети Интернет, в том числе из «облачных» хранилищ то есть сводит его получению информации путем удаленного доступа к компьютеру или серверу сети Интернет[61]. Вместе с тем самого определения данного ОРМ в законе не определено.

Его можно интерпретировать как возможность осуществления различного рода действий в сети «Интернет», проводимых в оперативных целях. Чаще всего подобного рода действия сводятся к получению сообщений определенного абонента у провайдера, администрации мессенджеров и электронной почты, т.е. те действия, которые предполагались изначально по антитеррористическому пакету, в результате принятия, которого появилось это ОРМ.

Данное мероприятие является достаточно специфическим оперативно-розыскным мероприятием и заключается не только в получении информации посредством считывания и её перемещения на цифровой носитель, но и в дистанционном получении информации с мобильного телефона, ноутбука, планшета или персонального компьютера, как правило посредством сети «Интернет». Для проведения такого рода мероприятия необходима специальная техника, которую использует исключительно специальные оперативные подразделения, в том числе для выявления мошенничеств в сети

[60]Мамлеев Р. Р. Средства и методы осуществления оперативно-разыскного мероприятия получение компьютерной информации // Полицейская и следственная деятельность. 2016. № 4. С. 37—45.

[61] Баженов С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России № 2 (65), 2017. С. 32.

«Интернет», которые набирают все большую популярность и затрагивают все важные сферы жизни общества в цифровом мире.

Для того чтобы получить судебное санкционирование для проведения такого рода мероприятий, необходимо обосновать существенность совершаемого преступником деяния, так как всем известно, что оперативно-розыскные мероприятия, посягающие на Конституционные права человека можно проводить только по тяжким и особо тяжким составам преступления, для чего и заводятся соответствующие дела оперативного учета по таким составам.

Вместе с тем по справедливому утверждению А.В. Серова и А.С. Дубинина: «внесение в ФЗ «Об ОРД» давно назревших изменений, позволяющих более эффективно получать компьютерную информацию в целях борьбы с преступностью и обеспечением безопасности, было сделано неверно с точки зрения юридической техники. Получение такой информации в зависимости от сложившейся оперативно-тактической ситуации и от состояния, в котором данная информация находится, может и должно происходить в рамках мероприятий СИТКС, обследования, наблюдения, исследования предметов и документов. Проблема ограниченности возможностей получения компьютерной информации в рамках ОРМ «обследование помещений, зданий, сооружений, участков местности и транспортных средств» должна решаться уточнением названия данного мероприятия путем исключения из него перечня обследуемых объектов. При таком подходе ПКИ следует исключить из перечня оперативно-розыскных мероприятий»[62]. Таким образом мы можем видеть, что законодательные упущения являются помехой в правильном использовании рассматриваемого оперативно-розыскного мероприятия.

Обследование помещений, зданий, сооружений, участков местности и транспортных средств. Отметим, что данное мероприятие

[62] Серов А.В., Дубинин А.С. Получение компьютерной информации как самостоятельное оперативно-розыскное мероприятие // Вестник Воронежского института МВД России. 2018 № 3. С. 170.

также может проводится и в сети Интернет. Подготовительный этап данного ОРМ, объектом по которому выступает информационная среда сети «Интернет», состоит из решения следующих вопросов:

1. Каков характер предполагаемой к осмотру информации: является ли она общедоступной или представляет собой конфиденциальную информацию, имеющую закрытый характер;

2. Подпадает ли указанная информация под действие конституционных норм о тайне переписки, предусмотренных статьей 23 Конституции РФ, и, следовательно, необходимо ли судебное решение на ограничение конституционных прав конкретных лиц, которое является неизбежным при проведении следственного осмотра;

3. Определение круга участвующих лиц и обеспечения их присутствия;

4. Решение вопроса о необходимости использования специальных технически-криминалистических средств и программного обеспечения, подготовки специальных бланков документов;

5. Определение иных способов фиксации информации в сети «Интерне» в ходе обследования (за исключением протоколирования);

В зависимости от характера предполагаемой к осмотру информации и поставленных целей, возможно наличие следующих практических ситуаций:

1. Ситуация, когда необходимо путем закрепить информацию, имеющую общедоступный характер, не имеющей ограничений по количеству лиц, допущенных к ознакомлению с ней. Указанные ситуация могут возникать при раскрытии преступлений, связанных с незаконным оборотом наркотических средств (например, обследование Интернет- сайтов, на которых выложена информация о продаже наркотиков, способах оплаты и получения, а также контактные данные); по делам экстремисткой направленности (например, обследование коммуникационных групп в различных социальных сетях, содержащих материалы, признанные в установленном законом порядке экстремистскими);

2. Ситуация, когда необходимо закрепить информацию, имеющую конфиденциальный характер. Чаще всего такая информация содержится в личных электронных переписках (на различных интернет-площадках), на электронных почтовых ящиках или иных «облачных» хранилищах, содержащих фото и видеофайлы конкретных лиц.

Соответственно, если информация находится на удаленных серверах, то есть в сети «Интернет» и имеет ограниченный характер, направленный на ознакомление некоторого круга лиц, то на проведение данного ОРМ требуется получение судебной санкции. Указанный вывод актуален лишь в ситуации, когда со стороны правообладателя информации отсутствует волеизявление на ознакомление с ней третьих лиц.

Признав решенным вопрос о необходимости получения судебной санкции встает не менее важный вопрос, определяющий допустимость последующих результатов ОРД с позиций требований уголовного процесса, то есть определения круга участников данного следственного действия.

По нашему мнению, для проведения обследования информации в сети «Интернет»необходимо привлечь следующих лиц:

1. Понятых при этом понятые должны иметь хотя бы общее представление об информационных технологиях (на уровне простого пользователя) для понимания характера совершаемых действий[63].

2. Собственника информационного ресурса (если это возможно и представляется необходимым), а также правообладателя информации конфиденциального характера. Указанные лица призваны дать в ходе осмотра информацию ориентирующего характера о том, в каком разделе информационного ресурса, на какой вкладке имеется та или иная информация, а также для преодоления средств защиты в виде идентификации, ввода паролей и тому подобное.

[63] Романенко М.А. Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения // Вестник Омского университета. 2008. № 1. С. 172.

3. Специалиста, то есть лица, обладающего специальными знаниями в области информационных технологий и способного помощь в наиболее полном и достоверном отражении в протоколе информации, имеющей доказательственное значение. Для определения содержания понятия специалиста можно обратиться к статье 58 УПК РФ, согласно которой, специалистом является лицо, «обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию»[64]. Применительно к сфере работы с электронными носителями, В.Ф. Васюков и А.В. Булыжкин сформулировали два основных требования, предъявляемых к соответствующим специалистам[65]:

1. Диплом о высшем техническом образовании (с указанием учебных дисциплин, направленных на получение знаний, умений, навыков в исследовании, разработке, внедрении и сопровождении информационных технологий и систем);

2. Опыта работы в должности не менее одного года. При этом в соответствии с должностными обязанностями такого сотрудника он должен наделяться функциями по обеспечению правильной технической эксплуатации, бесперебойной работы компьютерного оборудования организации на профессиональном уровне.

Необходимым следует отметить положения Приказа Министерства труда и экономического развития РФ от 01.11.2016 № 598Н «Об утверждении профессионального стандарта «специалист по безопасности компьютерных

[64]«Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ (ред. от 24.04.2020) // СПС «Гарант».

[65]Васюков В. Ф., Булыжкин А. В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения. Российский следователь. 2016. № 6. С. 7.

систем и сетей». К трудовым функциям данного специалиста настоящий документ относит: обслуживание, администрирование средств защиты информации в компьютерных системах и сетях, оценивание их уровня безопасности, разработка программно-аппаратных средств защиты информации, проведение инструментального мониторинга защищенности компьютерных систем и сетей, проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов[66].

С учетом положений настоящего приказа можно сформулировать следующие требования, соблюдение которых позволяет утверждать о компетентности специалиста:

1. Высшее образование – специалитет или магистратура в области информационной безопасности;

2. Наличие допуска к государственной тайне (при необходимости);

3. Дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности.

4. Трудоустройство по соответствующей технической специальности.

Аналогичную позицию по поводу данному поводу занимает Ю.В. Гаврилин[67].

Основными задачами специалиста в рассматриваемой ситуации является:

1. Выполнение всех манипуляций с компьютерной техникой (включение - выключение, разборка - сборка и пр.);

2. Оказание помощи оперативнику в описании компьютерной техники и периферийного оборудования в протоколах ОРМ;

3. Проведение экспресс-анализа компьютерной информации;

---

[66]Приказ Министерства труда и социальной защиты РФ от 1 ноября 2016 г. № 598н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» // СПС «Гарант».

[67]Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве. Труды Академии управления МВД России. 2017. № 4. С. 47.

4. Обнаружение информационных следов преступления; предотвращение уничтожения или повреждения компьютерной информации; изъятие компьютерной информации и др.

Следует отметить, что информационные технологии весьма многогранны и выбор того или иного специалиста для решения конкретных задач расследования должен осуществляться индивидуально. При решении в ходе ОРМ задач, связанных с изъятием технических средств, может быть полезен специалист, знающий элементы и устройства вычислительной техники и систем управления, знакомый с вопросами функционирования автоматизированных систем управления. Для установления фактов проникновения извне в информационные системы специалист должен обладать познаниями в области программного обеспечения вычислительных систем и организации вычислительных процессов, а также обязан знать основы методов защиты информации и информационной безопасности. При исследовании систем ЭВМ и их сетей специалист должен иметь специализацию в области математического и программного обеспечения вычислительных комплексов, систем и сетей, ему также необходимы познания в области компьютерных сетей, узлов связи и средств коммуникаций, организации и распределения информационных потоков.

Поиском специалистов следует заниматься заблаговременно на предприятиях, в учреждениях, фирмах и компаниях, осуществляющих обслуживание и эксплуатацию компьютерной и коммуникационной техники, разработку программного обеспечения, средств защиты компьютерной информации. Допустимо приглашение специалистов из учебных заведений и научно-исследовательских организаций.

Практика показывает, что чаще всего специалисты приглашаются непосредственно из системы органов внутренних дел. В экспертно-криминалистическом центре МВД России создан отдел по проведению программно-технических экспертиз, сотрудники которого могут быть приглашены в качестве специалистов по делам наибольшей сложности.

Аналогично по данному поводу отмечает В.Е.Козлов: «целесообразно по делам о киберпреступлениях привлекать к осмотру места происшествия специалистов из числа:

1. Сотрудников экспертных подразделений всех уровней и различной ведомственной принадлежности;

2. Представителей научных и педагогических коллективов, обладающих глубокими познаниями в области информационных технологий;

3. Частных лиц, не состоящих в штате каких-либо официальных структур»[68].

После определения круга участвующих лиц оперативнику необходимо определить перечень необходимых технико-криминалистических средств, необходимых для производства обследования ОРМ. При этом необходимо понимать, что в процессе производства может возникнуть потребность в копировании информации, а также её фиксации иными способами наряду с протоколированием.

В содержание данной стадии входит подготовка соответствующей компьютерной техники и программного обеспечения, которые будут использоваться для считывания и хранения изъятой информации, при обнаружении изменений в компьютерной информации, исследовании полученной информации, обнаружении информационных следов преступления. Указанными средствами может быть персональный компьютер, исполненный в переносном варианте Notebook.

Кроме компьютера, необходим кабель, а также специальное программное обеспечение, позволяющее осуществлять копирование и экспресс-анализ информации на месте.

Следует иметь в виду, что для полного и качественного копирования информации необходимо соответствие не марок компьютеров, а объемов используемых жестких дисков (у переносного компьютера этот объем

[68]Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М., 2012. С. 182.

должен быть не меньше, а в идеальном случае равен объему диска осматриваемого компьютера). Помимо переносного компьютера типа Notebook, при производстве осмотра могут быть использованы иные носители информации, обладающие большой емкостью: лазерные и DVD диски, внешние жесткие диски и тому подобное.

Центральное место во всем ОРМ занимает рабочий этап, поскольку именно в его период производится непосредственное исследование информации, позволяющей установить обстоятельства, имеющие значение для уголовного дела.

Непосредственное исследование информации в сети «Интернет» должно происходить по заранее выстроенной схеме. Очевидным является, что веб-ресурсы могут иметь различную структуру. Потребность в осмотре того или иного сайта возникает в зависимости от категории уголовного дела. Так, по делам о преступлениях в сфере незаконного оборота наркотических средств и психотропных веществ, актуальным может являться осмотр сайта в виде «Интернет - магазина». В свою очередь такой тип сайтов имеет определенную структуры, некоторое количество разделов по категориям, на которые может осуществляться как последовательный, так и случайный переход.

По делам о компьютерных преступлениях или преступлениях в сфере мошеннических действий может возникнуть потребность в производстве осмотра сайта, имеющего линейную структуру. Такая структура подразумевает под собой последовательный переход со страницы на страницу в пределах одного веб-ресурса. На рабочем этапе такого осмотра фиксируется текущее состояние компьютерной информации, делается вывод о произошедшем событии и его последствиях: уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ, их системы или сети; устанавливается способ совершения преступления. Для этого с помощью специалиста наблюдается действие программ, содержимое текстовых файлов и баз данных. При этом особое внимание следует уделить

изучению имеющихся в большинстве компьютерных систем файлов регистрации. Какое бы событие не произошло в системе, информация о нем (в том числе, кто инициировал его, когда и в какое время оно произошло, какие при этом были затронуты файлы) регистрируется в этих файлах. В частности, в файлах регистрации может получить отражение информация о паролях пользователей, их именах, идентификационных номерах. В последствии данная информация может быть использована для установления компьютера, с которого произошел неправомерный доступ к компьютерной информации.

Вышеуказанное подтверждает необходимость наличия у оперативника предварительного плана в части последовательности действий при производстве осмотра Интернет-ресурса.

В научной литературе отмечается, что в целях получения допустимых доказательств, необходимо соблюсти не только требования, прямо предъявляемые законом, но и удостовериться, что[69]:

1. Устройство, при помощи которого производится обследование, на протяжении всего мероприятия имеет связь с сетью Интернет, а передаваемая и получаемая информация не искажается или подменяется кем - либо;

2. Информация получается непосредственно из сети Интернет, а не из временного буферного хранилища;

3. Пользователям, которые обращаются к осматриваемому веб - сайту с разных адресов, передается одинаковая информация;

4. Осматриваемая веб - страница одинаково отображается в различных браузерах.

По нашему мнению, указанные требования являются необходимыми для соблюдения положениями, поскольку прямо влияют на достоверность отраженных данных.

[69]Санчат Ч.А. К вопросу о допустимости в качестве доказательств компьютерной информации, размещенной в сети интернет // Новая наука: от идеи к результату. 2017. № 3. С. 189.

В некоторых ситуациях также может возникнуть потребность в выяснении вопрос о правах на домен, на котором размещена исследуемая страница. Имя или фирменное наименование администратора домена и некоторые другие его данные можно получить в официальной базе данных доменных имен регистратора российской доменной зоны «RU» Российского научно-исследовательского института развития общественных сетей (РосНИИРОС) с помощью сервиса WhoIs. Для того чтобы это выполнить, в поисковом окне браузера указываем наименование сервиса, то есть WhoIs, в появившемся диалоговом окне указываем имя сайта, получаем информацию. Информация РосНИИРОС–достоверна.

Также оперативник должен указывать и URL адрес. При необходимости узнать конкретную информацию на странице, оперативнику нужно описывать все фрагменты, имеющие значение и приводить их описание. При этом хочется акцентировать внимание, что фиксация тех или иных данных осуществляется самостоятельно по собственному усмотрению.

Поскольку каждый Интернет-ресурс имеет свой определённый адрес, который имеет как численное выражение, так и буквенное, выступающее определенной альтернативой, важным является установления соответствия между указанными формами выражения адреса. В связи с изложенным не лишним будет привести позицию Бегичева А.В. относительно нотариальной практики по обеспечению доказательственной базы. Как указывает автор, к задачам нотариуса в ходе процедуры обеспечения доказательств в обязательном порядке относятся следующие положения:

1. Установление администратора домена (владельца сайта), т.е. информацию о принадлежности доменного имени информационного ресурса;

2. Проверка соответствие символьного адреса сайта его настоящему IP-адресу (трассировка), чтобы убедиться в том, что браузер отображает страницы подлинного сайта;

3. Фиксация содержание конкретного интернет-сайта.

Изложенное обязывает нас особенно акцентировать внимание на процедуру трассировки. Как отмечает А.В.Бегичев, «трассировка, прежде всего, производится с целью исполнения мер защиты от возможных фальсификаций. Технически она позволяет осуществить следующее: установить IP-адрес, на котором размещен сайт; проверить принадлежность этого IP-адреса; провести трассировку от компьютера нотариуса до сервера, содержащего сайт; собрать информацию об DNS-записях домена интернет-сайта; установить принадлежность домена на момент осмотра и др.[70]«

Относительно установления IP – адреса хотелось бы отметить высказывание К.С. Сидоровой, которая отметила обязательность доподлинного установления последнего. В своей работе она отметила, что « с целью всестороннего изучения всех обстоятельств уголовного дела, а также получения как ориентирующей, так и доказательственной информации, возникает необходимость установления IP-адреса, а в последующем и сведений о нем и использования в деятельности по расследованию преступлений»[71].

По - нашему мнению, в ходе исследования информации могут решать следующие специальные задачи:

1. Фиксация наличия (отсутствия) материалов определенного содержания. Доказывание настоящего факта может иметь место по делам об экстремизме или нарушению авторских прав;

2. Определение работоспособности Интернет- ресурса, возможности или необходимости совершения определенных действий, в том числе скачивания в память устройства, через которое осуществляется доступ к сайту, определенных данных. При этом частной задачей является определение следующего - является ли скачивание информации

[70]Бегичев А.В. Использование протоколов осмотров Интернет-сайтов в судебной практике // Вестник московского университета МВД России. 2014. № 11. С. 208.

[71]Сидорова К.С. Способы установления ip-адреса и сведений о нем при расследовании уголовных дел // Вестник Сибирского института бизнеса и информационных технологий. 2018. № 2. С. 88.

добровольным, то есть посредством действий посетителя Интернет – ресурса, или принудительным, то есть скрытно от пользователя. Фиксация указанного факта может быть важным обстоятельством по уголовным делам в сфере распространения вредоносного программного обеспечения или же Интернет – мошенничества, направленного на хищение персональных данных, данных банковских карт или иной информации, позволяющей в дальнейшем совершить конкретное хищение;

3. Поиск и фиксации IP-адресов, через которые осуществляется управление сайтом, персональных данных и иной информации, позволяющей установить владельца сайта и иных лиц, причастных к совершению преступлений указанных категорий.

По – нашему мнению, заключительный этап обследования информации в сети «Интернет» должен соответствовать следующим критерием:

1. Полнота отражения информации, установленной в ходе следственного осмотра;

2. Доступность отражения. Смысл данного требования сводится к тому, что, на оперативника ложится задача доступного изложения его результатов, отражение которых не будет носить сугубо технический характер;

Переходя к раскрытию содержания способов фиксации информации следует отметить, что к списку основных способов следует отнести протоколирование, фотосьемку, а также сохранение посредством специального или встроенного программного обеспечения содержания Интернет-ресурса целиком в неизменном виде и последующую запись такого файла на неизменяемый оптический диск.

Наиболее распространенным способом фиксации ОРМ является протоколирование. Вопрос о моменте составления протокола является достаточно дискуссионным и разрешается каждым сугубо индивидуально. По-нашему мнению, поскольку рассматриваемый вид ОРМ предполагает большое количество информации, затруднительной для запоминания и точного воспроизведения, целесообразным является составление протокола

по ходу производства. Составление протокола по окончанию ОРМ считаем возможным лишь при условии ведения черновых записей, отражающих ход и результаты мероприятия. Любые другие варианты исполнения повышают вероятность упущения и невнесения в протокол информации, имеющей значения для дела и определяющей такое свойство доказательств как допустимость.

В литературе отмечается, что протокол должен в обязательном порядке содержать следующую информацию[72]:

1. Описание использовавшихся технических средств;

2. Описание использовавшихся программных средств;

3. Указание на провайдера, предоставляющего услуги доступа к сети Интернет.

4. Маршрута доступа к странице в следующем виде: через доменные имена и по IP.

Составленный протокол должен быть подписан всеми участвующими лицами, в том числе каждая страница, содержащая описательную часть. Целесообразным является собственноручное исполнение такого заявления лицом. При этом желательно, чтобы каждая страница протокола была пронумерована.

В зависимости от типа, осматриваемого Интернет – ресурса, его структуры, протокол должен дословно отражать названия всех разделов и вкладок, к которым осуществлялся доступ. В протоколе также должны найти отражения все действия, связанные с осуществлением фото, свершением скриншота, сохранением файлов на конкретный носитель.

Неотъемлемой составляющей протокола является фототаблица. При этом практика составления фототаблиц является достаточно разнообразной, поскольку в качестве основы используются как полноценные фотографии изображения монитора, так и скриншоты, свершенные стандартным или

[72]Еськов В.Д., Чеботарев С.А. Особенности осмотра страниц в сети Интернет // Материалы VI Международной научной конференции студентов и магистрантов. 2017. С. 39.

специальным программным обеспечением. Вопрос о предпочтении того или иного способа фиксации является достаточно спорным и как в научном мире, так и в практической деятельности не нашего единого подхода к решению.

Под скриншотом следует понимать изображение, полученное компьютером (или иным электронным устройством) и показывающее в точности то, что видит пользователь на экране монитора в конкретный момент времени. Простейший способ получения скриншота для операционных систем MicrosoftWindows– использование клавиши PrtScr. С помощью данной клавиши лицо может зафиксировать обстановку как на его электронном устройстве (сведения о данном устройстве, какие-либо файлы), так и интернет-страницы. Как отмечает Е.А.Денисов, особую популярность приобрели скриншоты именно интернет-страниц (например, скриншоты переписки в социальных сетях при расследовании доведения до самоубийства, развратных действий, нарушения неприкосновенности частной жизни и др.)[73].

Единственным и существенным недостатком скриншота является возможность редактирования его содержания, что автоматически ставит под сомнение достоверность отраженной информации. Несомненным плюсом скриншота является простота его свершения и наиболее полная четкость отражаемого на экране изображения.

Обратными характеристиками в данной ситуации обладает фотография, что связано с затратой достаточных усилий на её скрытное редактирование. Минус фотографий состоит в том, что фотокамера любого электронного устройства при генерации изображения фиксирует невидимые человеческому глазу мерцания и помехи, которые создаются экранами ноутбуков и мониторами персональных компьютеров. В связи с этим фотография не может обладать той же четкостью изображения, что и скриншот.

[73]Денисов Е.А. Скриншоты в системе уголовно-процессуальных доказательств: вопросы теории и практики // Вопросы студенческой науки. 2017. № 15. 180.

В связи с изложенным, вопрос о выборе способа дополнительной фиксации информации в ходе ОРМ решается оперативником индивидуально с учетом конкретных обстоятельств.

При наличии большого количества информации, которую необходимо с абсолютной точностью отразить, при этом, не используя способ простого переписывания в протокол либо фотографирования любых изменений на мониторе, возможно сохранение содержимого Интернет - ресурса в первоначальном виде посредством стандартных программных возможностей Интернет - браузера либо использования специализированных утилит.

Так, посредством использования специальной программы MagneticWebPageSaver производится сохранение интернет - страницы целиком в файле.

Опция сохранения содержимого может быть предусмотрена непосредственно функционалом самого сайта. К таковым можно отнести почтовый сервис от mail.ru.

При этом обязательным является подробное отражение в протоколе факта скачивания информации, директории скачивания. В последующем такая информация должна быть скопирована на какой – либо носитель, в том числе flash- накопитель либо неизменяемый оптический диск.

При записи файлов на оптический диск необходимо убедиться, что диск относится к категории DVD-R или CD-R, то есть является не перезаписываемым. В обязательном порядке в протоколе должно найти отражение, присвоенное диску название, номер или иные реквизиты, позволяющие его индивидуализировать, дата и время записи диска, используемое программное обеспечение, операционная система компьютера или ноутбука. После записи диск должен быть упакован способом, исключающим несанкционированный доступ и его замену, оклеен биркой с пояснительной надписью, заверен подписями всех участвующих лиц и опечатан печатью.

В связи с тем, что память стандартного оптического диска ограничена 4,7 гигабайтами информации, в практике допускаются случаи сохранения информации на flash – носители, обладающие большим объёмом. Способность указанных запоминающих устройств к многоразовой перезаписи обуславливают определенные действия следователя.

Подводя итоги рассмотрению данного вопроса отметим, что, рассматривая вопросы особенностей выявления и документирования преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, совершенных с использованием криптовалют стоит отметить, наша страна является правовым государством. Согласно Конституции РФ, высшей ценностью является права и свободы гражданина и человека, в связи с чем такие права и свободы человека могут быть ограничены только лишь судом путем вынесения соответствующего решения. Указанное является конституционной гарантией каждого от незаконного преследования и нарушения его прав. В сети Интернет могут проводится следующие мероприятия, требующие судебного санкционирования: 1. Контроль почтовых отправлений, телеграфных или иных сообщений; 2. «Наведение справок». 3. Получение компьютерной информации. 4. Обследование помещений, зданий, сооружений, участков местности и транспортных средств. Это те основные мероприятия, которые чаще всего применяются на практике, при выявлении и раскрытии преступлений, совершенных в сети Интернет, в том числе с использованием криптовалюты. Особенность данных мероприятий заключается в том, что посягают на права и законные интересы граждан в связи с чем их проведение ограничено судебным санкционированием.

2.2 Использование сведений об операциях с криптовалютами в доказывании по уголовным делам в сфере незаконного оборота наркотических средств и психотропных веществ.

Использование криптовалюты обуславливает необходимость пользователя работать с различного рода устройствами из сферы высоких технологий. Приобретение валюты, её обмен, майнинг и т.д. – все это невозможно без электронных носителей информации и определенных программ. Указанное обстоятельство обуславливает наличие цифровых следов, которые представляют собой достаточно новое явление для криминалистики и правоприменительной деятельности. В связи с этим ни одно уголовное дело не обходится без изъятия и исследования электронных носителей информации, Интернет-ресурсов, программ и т.д.

Современные электронные носители весьма разнообразны, однако функционал каждого из них достаточно схож: они предоставляют широкие возможности по обмену информацией, выходу в Интернет, передаче сообщений. Подобного рода исследование может осуществляться в рамках такого уголовно-процессуального средства как следственный осмотр. Данное следственное действие является наиболее универсальным (то есть предмет исследования в рамках него практически не ограничен) и простым (с позиции подготовки к нему и его производства).

Указанное означает, что следователи (дознаватели) по делам о незаконном обороте наркотиков, совершаемых с использованием криптовалюты, должны в совершенстве владеть тактикой осмотра данной категории предметов и объектов. При отсутствии таких знаний либо же их недостаточности следователи имеют право на приглашение специалиста для участия в осмотре различных электронных носителей.

Согласно ч. 1 ст. 58 УПК РФ, специалист - лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в порядке, установленном Кодексом, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для

постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию[74].

В свою очередь, исходя из норм закона, мы можем сформулировать собственные основания привлечения лица в качестве специалиста:

1. Необходимость в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела;

2. Необходимость в формулировании и постановке вопросов эксперту;

3. Разъяснение сторонам и суду вопросов, входящих в его профессиональную компетенцию.

Исходя из понятия «специалист», можно сделать вывод, что специалистом может быть любое лицо, обладающее необходимыми специальными знаниями и незаинтересованное в исходе уголовного дела, то есть он должен удовлетворять двум требованиям: незаинтересованность и компетентность. Незаинтересованность означает отсутствие как общих, так и специальных оснований для отвода специалиста. А компетентность — это наличие у него необходимых знаний. Никаких иных требований к специалисту УПК РФ не предъявляет. Специалист дает свое заключение в интересах той стороны, которая его привлекает. Специалист не предупреждается об уголовной ответственности за дачу заведомо ложного заключения.

Теперь рассмотрим этапы осмотра сотового телефона с целью обнаружения следов использования криптовалюты.

Подготовительный этап, как правило, сложности не представляет и заключается в:

– выполнении стандартного алгоритма действий, связанных с определением места и времени проведения следственного действия;

[74] «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ // Доступ из справ.- прав. системы «КонсультантПлюс».

– выполнении процессуальных требований;

– приглашении специалистов в области информационных технологий, информационной безопасности, специалиста-криминалиста, других участников;

– разъяснении им прав и обязанностей, предупреждении об ответственности.

Однако следует рассмотреть немаловажный момент, касающийся пределов производства осмотра. Нередко в правоприменительной практике возникает банальный вопрос, который разрешается достаточно противоречиво и необоснованном. В данном случае мы говорим о следующем. В зависимости от характера предполагаемой к осмотру информации и целей, поставленных следователем, возможно наличие следующих практических ситуаций:

1. Ситуация, когда следователю необходимо путем следственного осмотра процессуально закрепить информацию, имеющую общедоступный характер, не имеющей ограничений по количеству лиц, допущенных к ознакомлению с ней. Указанные ситуация могут возникать при расследовании преступлений, связанных с незаконным оборотом наркотических средств (например, осмотр Интернет- сайтов, на которых выложена информация о продаже наркотиков, способах оплаты и получения, а также контактные данные);

2. Ситуация, когда следователю необходимо путем следственного осмотра процессуально закрепить информацию, имеющую конфиденциальный характер. Чаще всего такая информация содержится в личных электронных переписках (на различных интернет-площадках), на электронных почтовых ящиках или иных «облачных» хранилищах, содержащих фото и видеофайлы конкретных лиц.

Вторая из указанных ситуаций также очень сильно варьируется в зависимости от волеизъявления обладателя такой конфиденциальной информации, что связано с распространением на нее действий

конституционных норм о тайне переписки, предусмотренных статьей 23 Конституции РФ.

Так, часть 2 указанной статьи закрепляет следующее: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения».

Указанное толкование конституционный норм с учетом позиции Конституционного Суда РФ, позволяет утверждать, что право человека и гражданина, закрепленное в ч.2 ст. 23 Конституции РФ – это фактически обеспеченная государством обязанность оператора любого вида связи не допускать ознакомления и разглашения информации, передаваемой по каналам его связи или сохраняемой на материальных носителях оператора.

Отсюда мы можем сделать вывод о том, что если информация находится на удаленных серверах, то есть в сети «Интернет» и имеет ограниченный характер, направленный на ознакомление некоторого круга лиц, то на осмотр указанной информации (то есть на ограничение конституционного права гражданина) требуется получение судебной санкции. Указанный вывод актуален лишь в ситуации, когда со стороны правообладателя информации отсутствует волеизявление на ознакомление с ней третьих лиц.

Более сложным и трудоемким является **рабочий этап,** включающий две стадии – статическую и динамическую.

Согласно общим положениями криминалистики, сущность ***первой стадии (статической)*** заключается в изучении внешнего вида сотового телефона или персонального компьютера. Незаменимыми при выполнении данного элемента являются знания специалиста в области информационных

технологий или вычислительной техники. Именно он сможет оказать помощь при выявлении как общих, так и частных признаков[75].

К *общим* признакам средства вычислительной техники можно отнести: тип (персональный компьютер, ноутбук, смартфон, планшет), наименование, марку (как правило, нанесена корпусе), его размеры, цвет, конструкцию, внешний вид, материал, из которого изготовлен корпус, модель, характеристику клавиатуры, используемую операционную систему. *К частным* – наличие повреждений (царапин, потертостей, сколов на корпусе или дисплее), наклеек или украшений.

Для идентификации конкретного экземпляра сотового телефона необходимо установить IMEI (англ. InternationalMobileEquipmentIdentity – международный идентификатор мобильного оборудования) – уникальный идентификатор, представляющий собой 15-значное число. Он служит для идентификации устройства в сети и хранится в прошивке аппарата. Как правило, IMEI указывается в четырех местах:

– в самом аппарате (в большинстве случаев его можно вывести на экран набором *#06# на клавиатуре);

– под аккумуляторной батареей;

– на упаковке;

– в гарантийном талоне.

Далее необходимо провести распознавание модели сотового телефона, серийного номера телефона, операционной системы, версии прошивки, телефонного номера сим-карты, IP-адреса, MAC-адреса[76].

Для просмотра модели телефона в ОС Android необходимо воспользоваться меню «Настройки» – «Об аппарате» – «Общая информация». В данном разделе может располагаться следующая

[75]Козулепенко А.Р. К вопросу о роли специалиста при осмотре мобильного устройства по уголовным делам, связанным с незаконным оборотом наркотиков // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 4. С. 53.

[76]Козулепенко А.Р. К вопросу о роли специалиста при осмотре мобильного устройства по уголовным делам, связанным с незаконным оборотом наркотиков // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 4. С. 53.

криминалистически значимая информация: IMEI, модель телефона, серийный номер телефона, операционная система, версия прошивки, телефонный номер сим-карты, IP-адрес, MAC-адрес.

Для персонального компьютера и ноутбука необходимо установить серийные номера (как правило, указывается на корпусе) и используемую операционную систему (определяется по внешнему виду рабочего стола).

Также необходимо установить наличие сетевых подключений компьютера и соответствующие сетевые адреса. Установление IP- и MAC-адресов и сопоставление их с данными, полученными от провайдеров интернет-услуг и платежных систем, позволяют установить причастность пользователя (например, выполняющего функции оператора) к совершению преступления. Для определения IP- и MAC-адресов в операционной системе MicrosoftWindow 7 (для других операционных систем этого семейства действия аналогичны) можно предложить следующий алгоритм:

а) нажать левой кнопкой мыши в области уведомлений (рядом с часами) по значку сетевого соединения и выбрать пункт «Центр управления сетями и общим доступом.

б) в открывшемся окне нажать левой кнопкой мыши по ссылке «Подключение по локальной сети», после чего откроется диалоговое окно «Состояние – подключение по локальной сети».

в) далее «щелкнуть» по кнопке «Сведения», откроется диалоговое окно «Сведения о сетевом подключении». В этом окне отобразится MAC-адрес (строка «Физический адрес») и IP-адрес данного компьютера (строка «Адрес IPv4»).

Перейдём теперь к ***динамической стадии рабочего этапа*** следственного осмотра с участием специалиста в области информационных технологий.

1. Управление счетами в криптовалюте возможно либо с использованием программ кошельков, либо через специализированные сайты сети Интернет. Второй вариант будет рассмотрен позже, сейчас же

остановимся на варианте использование специализированного программного обеспечения – программ-кошельков. Наличие таких программ может быть установлено по наличию на экране или в меню ярлыков данных программ.

Обнаруженные программы-кошельки позволяют определить, какими криптовалютами пользовался подозреваемый, номера кошельков в этих криптовалютах, а также историю операций с данными кошельками.

2. При осмотре компьютера или сотового телефона могут быть выявлены один или несколько веб-браузеров – программ для просмотра содержимого компьютерных сетей, в частности – сети Интерент, (например: GoogleChrome, AndroidBrowser, Opera, Яндекс.Браузер и др.).

При этом специалистом особое внимание следователя должно быть обращено на наличие программ, обеспечивающих анонимность работы в сети Интернет (браузер Tor и I2P, ORBOT и др.), поскольку их наличие может свидетельствовать о наличии умысла на сокрытие виртуальных следов преступной деятельности. Подробный осмотр браузеров, предназначенных для обеспечения анонимности, нецелесообразен, так как эти браузеры не ведут историю посещённых страниц. Внимание следует сосредоточить на стандартных браузерах.

Важную криминалистическую информацию можно получить при изучении *истории просмотра веб-страниц и закладок в браузере.* Пример истории просмотра веб-страниц в браузере Chrome показан на рисунке ни же.В частности, детальному анализу должны быть подвергнуты:

– социальные сети («ВКонтакте», «Facebook», «Одноклассники» и т.д.), а также форумы. В рамках дел рассматриваемой категории интерес представляют форумы и сообщества социальных сетей, посвященные криптовалютам.

– сайты криптобирж (например: bitmex.com, binance.com, localbitcoins.net, livecoin.net);

– сайты, предоставляющие возможность создания и удалённого управления кошельками в криптовалюте (например, Coin.Space, BTC.com,

https://www.bitgo.com/, https://xapo.com/, https://coinapult.com/, https://www.coinbase.com/);

– сайты электронных платёжных систем (PayPal, QIWI, WebMoney, Яндекс.Деньги и т.д.);

– информация с иных сайтов, которые посещал подозреваемый (обвиняемый): раскрывающая способы противодействия в процессе уголовного и административного судопроизводства, методы работы правоохранительных органов; содержащая сведения о криптовалютах и технологии блокчейн (например, https://forklog.com/), детализирующая схемы легализации денег от наркодоходов и иных видов незаконной деятельности; описывающая возможности электронных платежных систем и криптобирж.

3. Электронная почта представляет собой традиционной способ обмена информацией через компьютерные сети, который активно используется до настоящего времени. К электронной почте привязываются учётные записи на многих сайтах, в том числе – на криптобиржах.

Управление электронной почтой может осуществляться с использованием сайта (gmail.com, mail.ru, mail.yandex.ru и т.д.) или специализированной программы – почтовые клиенты (Mozillathunderbird, TheBat!,MicrosoftOutlook и т.д.). Почтовые клиенты, как правило, позволяют получить доступ к электронной почте без ввода пароля (пароли сохраняется при регистрации или настройке почтового клиента). Если же доступ к электронной почте осуществлялся через сайт, то может потребоваться (если пользователь давно не авторизировался на данном сайте или специально вышел из учётной записи) ввод пароля от ящика и, возможно, проверочного кода, отправляемого на привязанный к ящику электронной почты сотовый телефон. В этом случае можно предложить задержанному лицу назвать пароль добровольно, либо попытаться найти его в записных книжках, наклейках и т.п.

При осмотре содержимого ящиков электронной почты необходимо обращать внимание на сообщения от сайтов, рассматриваемых на

предыдущем шаге. Это могут быть электронные письма, содержащие сведения о регистрации и/или активации учётной записи на сайте, смене пароля, входе в учётную запись, выполнении тех или иных операций с криптовалютами и традиционными электронными платёжными системами, об обмене криптовалюты и фиатных денег на криптобирже, квитанции интернет-банков.

4. Изучение программ обмена мгновенными сообщениями и IP-телефонии. В настоящее время все чаще общение участников преступных групп осуществляется не через традиционные телефонные звонки и СМС-сообщения, а с использованием программ для общения через Интернет (WhatsApp, Viber, Brosix, Telegramи др.), называемых «мессенджеры» или, более строго, «программы обмена многовенными сообщениями». Это связано с тем, что данные программы создают дополнительный уровень посредничества в окозании услуг связи, что повышает консирацию. Многие программы данной категории позволяют своим пользователям общаться не только с помощью текстовых сообщений, но и с помощью голоса, причём информация передаётся через протколы сети Интернет, а не по традиционной сети сотовой телефонной связи (IP-телефония).

При этом следует отметить, что в последнее время с целью повышения безопасности коммуникации преступниками осуществляется переход от ICQ, Jabber, Skype к приватному мессенджеру Telegram с более сложным алгоритмом шифрования. Популярность данного приложения обусловлена нахождением его серверов за пределами Российской Федерации, что повышает конспиративность.

В рамках поиска доказательств и следов использования криптовалют и криптобирж интерес представляет не традиционная функция месседжеров – общение с другими пользователями, а так называемые «каналы», аналогичные группам в социальных сетях. Целесообразно выполнить поиск как каналов конкретных криптовалют и криптобирж, так и распространяющих общую информацию о функционировании криптовалют и

технологии блокчейн, рекомендации по покупке или продаже тех или иных криптовалют, выбору криптобиржи и другую аналитическую информацию о криптовалютах.

5. Изучение СМС-сообщений. В отличие от остальных шагов, это применимо только для сотовых телефонов, но не для персональных компьютеров. Телефонный номер сетей сотовой связи используется как имя учётной записи на многих сайтах (уступая, пожалуй, только электронной почте). Даже если телефон не является основным идентификатором пользователя, очень часто он используется для отправки одноразовых паролей в рамках так называемой двухфакторной авторизации, либо при осуществлении платежей в электронных платёжных системах или системах интернет-банкинга с целью повышения безопасности этих операций и уменьшения вероятности взлома соответствующих учётных записей.

На заключительном этапе следственного осмотраспециалист-криминалист и (или) специалист в области информационных технологий и (или) информационной безопасности могут оказать содействие следователю в упаковке осмотренного объекта. После этого должно быть принято процессуальное решение о приобщении компьютера или сотового телефона в качестве вещественного доказательства и определении места хранения[77].

Ранее нами уже было сказано, что основным средством платежа за наркотики в Даркнете является криптовалюта. В связи с этим логичным является тот факт, что конечному потребителю наркотиков необходимо сначала приобрести криптовалюту, а после выполнить операции по приобретению наркотиков. Обратной ситуаций является необходимость продавца наркотиков обменять криптовалюту на фиатные деньги, которые можно использовать в гражданском обороте. Одним из уголовно – процессуальных средств, с помощью которого могут быть закреплены

[77]Козулепенко А.Р. К вопросу о роли специалиста при осмотре мобильного устройства по уголовным делам, связанным с незаконным оборотом наркотиков // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 4. С. 53.

операции с криптовалютой в качестве доказательственной информации, является следственный эксперимент.

Согласно УПК РФ, «в целях проверки и уточнения данных, имеющих значение для уголовного дела, следователь вправе произвести следственный эксперимент путем воспроизведения действий, а также обстановки или иных обстоятельств определенного события. При этом проверяется возможность восприятия каких-либо фактов, совершения определенных действий, наступления какого-либо события, а также выявляются последовательность происшедшего события и механизм образования следов. Ключевым для нашей ситуации является выявление последовательности события, фиксации его следов.

Во избежание повторений отметим, что общие тактико-криминалистические правила производства следственный действий для следственного эксперимента аналогичны следственному осмотру, ввиду чего в настоящем параграфе повторно освещаться не будут, аналогичным образом, как и требования к специалисту, порядок обеспечения его участия и т.д.

Неофициальное интервьюирование сотрудников следственных подразделений показало, что большинство правоприменителей в принципе не предполагают о наличии возможностей производства следственного эксперимента в данном ключе, хотя тактические приемы и средства, допустимые для применения в ходе его производства, являются существенным подспорьем во всей совокупности доказательственной базы.

Первый блок действий, которые могут быть проверены и уточнены в ходе следственного эксперимента, составляют действия по приобретению криптовалюты на ранее обозначенных криптобиржах. Действия, требующие затрат денежных средств, могут быть выполнены условно (подозреваемый открывает необходимые страницы сайта, заполняет поля и объясняет, что произойдёт после завершения операции), либо с использованием незначительных сумм.

Итак, основными действиями на криптобирже являются:

1. Регистрация, подразумевающая выбор логина, то есть условного имени пользователя на сайте, указание адреса электронной почты, а также создание пароля, который чаще всего вводится два раза для подтверждения его правильности;

2. Приобретения криптовалюты. В общем виде действия на криптобиржах выглядят следующим образом. Осуществляется вход на сайт криптобиржи. Её интерфейс чаще всего предполагает наличие сведений о состояние курса конкретных видов криптовалюты, сведений о состоянии баланса и возможных операций с ним. Прежде всего, осуществляется пополнее баланса фиатными деньгами. Чаще всего для этого в России используются сервисы QIWIWallet и Яндекс.Деньги. После выполнения команды в интерейсе биржи о пополнении баланса, чаще всего на ранее указанный почтовый ящик приходят реквизиты для пополнения: номер телефона (привязанный к счету в системе QIWI или Яндекс.Деньги), а также идентификатор платежа. Для выполнения описанных действий при практическом проведении следственного эксперимента может быть создана специальная временная учётная запись электронной почты (одноразовые почтовые ящики). Дальнейшие действия представляют собой обычный перевод средств в электронной платежной системе QIWI со счета пользователя на счет, принадлежащий бирже криптовалют. Подозреваемый должен продемонстрировать процесс заполнения данных форм. Если все действия выполнены правильно и платеж в пользу биржи прошел успешно, в интерфейсе последней изменятся сведения о балансе. Кроме того, пользователь получит на адрес электронной почты, указанный при регистрации, электронную квитанцию об операции, которая содержит дату и время совершения операции, сумму платежа, реквизиты квитанции, счета списания и зачисления. Соответственно, после пополнения баланса, пользователь может осуществить обменные криптовалютные операции по курсу, установленному биржей.

В случае расследования уголовного дела о лица, сбывающих наркотические средства, актуальным также может быть проведение следственного эксперимента в целях фиксации действий о выводе средств с биржи на счета пользователя. Актуальность только для сбытчиков обусловлена тем, что лишь данные лица получают суммы в криптовалюте от наркопотребителей. Соответственно, у них возникает потребность обмена криптовалюты на обычные деньги. В данном случае на бирже используется функция вывода, которая чаще всего предоставляется право выбора платежной системы: банковских (систем Visa или Mastercard), либо же QIWI и Яндекс.Деньги. Во всех способах предполагается вывода необходимо указать сумму вывода. Разница между способами вывода заключается в том, что при использовании банковской карты нужно указать номер карты, а при выводе через QIWI – номер телефона, к которому привязан счет в данной электронной платежной системе.

Следующий блок действий, которые могут быть зафиксированы в рамках следственного эксперимента, составляют действия по приобретению наркотических средств. Данный блок представляет собой следующие действия:

1. Установка необходимого программного обеспечения (браузера Tor, VPN-сервисов (при необходимости) либо же скачивание текстового мессенджера (чаще всего в качестве такового выступает Телеграмм);

2. Регистрация аккаунта в текстовом мессенджере либо в интернет-магазине в пределах Даркнета;

3. Выбор наркотического средства и его оплата (данные действия выполняются подозреваемым, обвиняемым условно). Ввиду условности данного блока путем следственного эксперимента не могут быть зафиксированы последующие действия, связанные с получением координат и фотографий, содержащих местонахождение «закладки».

Что же дает нам данное следственное действие с позиции доказывания? По нашему мнению, посредством его производства может быть установлен и

должным уголовно-процессуальным способом закреплен механизм совершения преступления, действия подозреваемого (обвиняемого), а также установлены иные обстоятельства, которые могут служить сведениями, имеющими значение для данного уголовного дела. Роль специалиста в данном случае, может быть, как аналогичной со следственным осмотром (когда специалист указывает на дополнительные детали, которые могут иметь отношение для уголовного дела), так и выступать в рамках «негласного» контроля действий подозреваемого, обвиняемого (или иного лица, чьи действия проверяются в ходе следственного действия). В данном случае мы имеем ввиду тот факт, что сторона защиты может воспользоваться банальным незнанием тонки рассматриваемых выше сервисов (сайтов) и ввести следователя в заблуждения относительно механизма его работы, в связи с чем в данном случае специалист своим устным заключением в ходе следственного действия может пресечь данную тактику поведения.

По уголовным делам, связанным с незаконным оборотом наркотиков, в том числе с использованием криптовалюты, актуальным является проведение ряда экспертиз.

Одним из ключевых исследований, проводимых в рамках данной категории уголовных дел, является компьютерная экспертиза. Указанное обусловлено большим количеством электронных носителей информации, на которых может находится информация, имеющая значение для уголовного дела.

Компьютерная экспертиза представляет собой комплексное исследование, и для понимания возможностей данного вида экспертизы целесообразно ее возможности условно разделить на:

1) получение информации, содержащейся на устройстве, и ее исследование;

2) изучение программного обеспечения, которое установлено на устройстве;

3) исследование самого объекта на принадлежность к определенным устройствам;

4) так называемая компьютерно-сетевая экспертиза, которая позволяет установить соединения устройства с Интернетом или сетью.

Объектами данного вида экспертного исследования могут выступать персональные компьютеры, периферийные устройства, мобильные телефоны, сетевые аппаратные средства (серверы, рабочие станции), любые комплектующие средств связи (платы расширения, микросхемы, сим-карты), запоминающие устройства и носители данных, включая все известные на момент проведения экспертизы электронные носители данных: микросхемы памяти, диски, флэш-карты и т.д.

Данный вид экспертизы может разрешать следующие обстоятельства:

1. Блок вопросов технического (аппаратного) характера: марка, модель устройства, конфигурация, характеристики;

2. Информационный блок: какая информацияимеется (по ключевым словам), форматнайденных данных (текстовые документы, графические файлы, базы данных и т.д.), сведения о собственнике (пользователе), в том числе имена, пароли, права доступа и пр.;

3. Программно-сетевой блок вопросов: работа устройства в сети Интернет, содержание установок удаленного доступа и протоколов соединений, наличие адресов Интернета, по которым осуществлялся доступ, наличие почтовых отправлений, иных видов переписок, программ для них,

В случае, если в ходе расследования уголовного дела будут установлены признаки легализации доходов от совершения наркопреступлений, актуальным также будет являться судебно-экономическая экспертиза. В рамка данной экспертизы может быть установлен:

1. Преступный доход;
2. Движение денежных средств;
3. Способы легализации.

Достаточно удачный пример судебной практики приводится в пособии С.И. Земцовой, П.В. Галушина, А.Л. Карлова: «При расследовании преступлений совершенных группой лиц по предварительному сговору в период с апреля 2018 года по 22 мая 2018 года, было установлено, что К., М. и Н. получали преступным путем денежные средства в криптовалюте «Luxcoin» на кошелек с № Р- «..» на интернет сайте «Payeer.com», в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами, осуществляли перевод полученной криптовалюты в валюту Российской Федерации – рубли, с последующим переводом на банковскую карту ПАО «…» Сбербанк принадлежащую и находящуюся в пользовании с последующим переводом на банковские карты «…», обналичивая которые получали денежные средства в свое распоряжение. В указанный период времени «…» в ходе осуществления преступной деятельности, связанной с незаконным оборотом наркотических средств, вышеуказанным способом легализовали денежные средства на общую сумму не менее 2100 000 рублей».

Авторы отмечают, что в постановлении о назначении судебно-экономической экспертизы, перед экспертом по данному уголовному делу были сформулированы следующие вопросы:

1. Какая сумма криптовалюты «LTC», согласно программе «Jaxx» была зачислена и переведена на сотовые телефоны «», «», «», в период времени с 1.10.2017 по 26.07.2018, в период времени с 01.01.2018 по 26.07.2018, согласно протоколу осмотра предметов от 04.12.2018.

2. Какая сумма денежных средств поступила на счета банковских карт ПАО «Сбербанк России» в дни перевода криптовалюты «LTC» либо на следующий день согласно программе «Jaxx» : на номер карты «», номер счета «» в период времени с 1.10.2017 по 26.07.2018, 01.01.2018 по 26.07.2018, исключая поступления от следующих лиц : «» согласно материалам уголовного дела.

3. Какая сумма криптовалюты «LTC», согласно информации, предоставленной из компании «Payeer» была зачислена на счет в период времени с с 1.10.2017 по 26.07.2018, согласно материалам уголовного дела.

4. Какая сумма денежных средств поступила на счета банковских карт ПАО «Сбербанк России» в дни перевода криптовалюты, либо на следующий день по программе «Payeer», номер карты «», номер счета «» в период с «».

Соответственно, в рамках подобного роды экспертизах излагаются все операции с денежными средствами, которые имеют признаки легализации преступных доходов с указанием реквизитов счетов, точных сумм и, при наличии возможности, назначение платежа. При этом вывод о том, что операции представляют собой действия, направленные на легализации преступных доходов, то есть вывод правового характера, в данном случае делает следователь, излагая вывод в постановление о привлечении в качестве обвиняемого и обвинительном заключении с перечнем доказательств. Даже вероятностный характер ответов экспертов на вопрос относительно правовой природы операций не допустим.

Наряду с производством судебной экономической экспертизы хорошим подспорьем для доказательственной базы, подтверждающей «легализацию» являются финансовые расследования, проводимые силами Росфинмониторинга на основании запросов правоохранительных органов. В своих расследования, сотрудники Росфинмониторинга проводят анализ юридических лица, взаимосвязей между ними, промежуточных звеньях на основе движения денежных средств. По итогу такого расследования делается вывод о «сомнительном характере операций», а также предоставляются сведения о «возможных путях расходования денежных средств».

Рассматривая вопросы совершенствования практики раскрытия и расследования преступлений, связанных с незаконным оборотом наркотических средств с использованием сведений о криптовалюте мы пришли к выводу о том, что для ее совершенствования необходимо ряд изменений в первую очередь связанных с особенностями работы

следственных и оперативных подразделений. В частности, считаем важным проводить периодическое обучение сотрудников следственных и оперативных подразделений с целью повышения их знаний в сфере расследования преступлений, связанных с незаконным оборотом наркотических средств, с использованием данных о криптовалюте. Кроме того, важно издавать методические рекомендации, направленные на работу со следами доказательственной информации для сотрудников следственных и оперативных подразделений. Отдельным направлением совершенствования практики раскрытия и расследования преступлений в данной сфере представляется совершенствование технической базы органов предварительного следствия и оперативных подразделений.

Подводя итоги настоящего вопроса хотелось бы отметить, что по категории уголовных дел, связанны с незаконным оборотом наркотиков одним из условий судебной перспективы дела является качественно и детально проведенный осмотр электронных носителей информации. В рамках настоящего параграфа нами были сформулирован и представлен исчерпывающий перечень рекомендаций относительно данного следственного действия. Роль специалиста в данном следственном действии является если не главенствующей, то точно немаловажной. Роль специалиста сводится в направлении следователя к тем деталями технического характера, сведениями и метаданным, которые могут иметь значение для уголовного дела. При этом относимость таких сведений к предмету доказывания определяется непосредственно следователем (дознавателем). Кроме того, хотелось бы отметить, что такая форма использования специальных знаний как производство судебной экспертизы и допрос эксперта является одной из неотъемлемых составляющих материалов уголовного дела, связанного с незаконным оборотом наркотических средств. Вместе с тем, эффективность данных уголовно-процессуальных средств напрямую зависит от того, насколько качественно следователь подошел к их подготовке: правильно установил обстоятельства, изъял образцы, принял меры к сохранению следов

и т.д. В рамка данной категории дел, как мы можем наблюдать, перечень судебных экспертиз является достаточно разнообразным ввиду того, что данные преступления имеют отношения как к предметам материального мира (наркотикам, прекурсорам) и психике и физическому состоянию человека (в данном случае мы говорим о лицах, которые употребляют наркотические средства), так и к идеальным следам, которые содержатся в электронного носителя информации и на мощностях информационно-коммуникационной сети «Интернет».

Рассматривая вопросы совершенствования практики раскрытия и расследования преступлений, связанных с незаконным оборотом наркотических средств с использованием сведений о криптовалюте мы пришли к выводу о том, что для ее совершенствования необходимо произвести ряд изменений в первую очередь связанных с особенностями работы следственных и оперативных подразделений. В частности, считаем важным проводить периодическое обучение сотрудников следственных и оперативных подразделений с целью повышения их знаний в сфере расследования преступлений, связанных с незаконным оборотом наркотических средств, с использованием данных о криптовалюте. Кроме того, важно издавать методические рекомендации, направленные на работу со следами доказательственной информации для сотрудников следственных и оперативных подразделений. Отдельным направлением совершенствования практики раскрытия и расследования преступлений в данной сфере представляется совершенствование технической базы органов предварительного следствия и оперативных подразделений.

Заключение

Подводя итоги данного вопроса отметим, что у криптовалют есть перспектива стать основой для фундаментального скачка в развитии цифровой экономики как в России, так и во всем мире, однако для этого необходимо разработать адекватный механизм правового регулирования данного явления. Вместе с тем в настоящее время ни в отечественной, ни в зарубежной доктрине не сложилось единой позиции относительно того, что представляет собой криптовалюта. Действующее на настоящий момент законодательство не учитывает всей специфики этого явления и многогранности понятия. На наш взгляд, в целях удовлетворения постоянно изменяющихся потребностей роста новой цифровой экономики надо обеспечить гибкость при внесении изменений в нормативно-правовую базу в части правового регулирования криптовалют. При этом, определяя правовой режим криптовалют, следует прежде всего учитывать экономическую сущность данного явления. Отсутствие должного правового подхода к регулированию криптовалюты приводит к негативным последствиям, в первую очередь связанным с увеличением уровня преступности. В этой связи считаем важным рассмотреть вопросы связанные с особенностями использования криптовалютпри совершении преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ, в том числе и как средство конспирации преступной деятельности.

Криптовалюта выступает характерным примером инновации экономики нракобизнеса. Именно использование криптовалют позволяет наркодилерам посредством задействования новых финансовых механизмов обеспечивать независимость экономики террора от легальных экономических структур в процессе производства и потребления необходимых им товаров и услуг. Использование криптовалюты в качестве средства легализации преступных доходов позволяет осуществлять сделки по купле-продаже наркотических средств без оставления значительных следов в

информационной среде.

В целях минимизации использования криптовалюты в преступных целяхнеобходимо выполнение следующих мероприятий: - идентификация клиентов сервисов, связанных с криптовалютными операциями на основании Федерального закона от 7 августа 2001 г. N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»; - передача указанных выше сведений о клиентах и их операциях Федеральной службе по финансовому мониторингу, Федеральной налоговой службе и иным уполномоченным органам власти. Данные положения наиболее полным образом соответствуют относительно недавно обновленным рекомендациям ФАТФ; -в менение обязанности получения сервисами по операциям с криптовалютой лицензии на осуществление деятельности, а также обязанности взаимодействия аккредитованными провайдерами. Указанное способствует минимизации риска трансграничного характера криптовалют; - вменение обязанности страхования рисков утраты средств клиентов и выплаты компенсаций клиентам в случае утраты их средств. Данное положение должно способствовать повышения информационной безопасности сервисов при оказании ими услуг.

Широкое распространение криптовалюты в сфере наркобизнеса обусловлено теми преимуществами, которыми её наделяют принципы работы самой технологии блокчейн. К таким чертам мы отнесли следующее: анонимностью, трансграничностью, доступность, скорость транзакций и т.д. Современные тенденции таковы, что роль криптовалюты «Биткойн» в настоящее время в преступной среде уменьшается по причины разработки и совершенствования сервисов, направленных на деанонимизацию сделок данной криптовалютой. В связи с этим набирают популярность иные виды криптовалют, которые обладают более высокими конспиративными характеристиками;Имеется высокая потребность в рассмотрении и принятии комплекса нормативных положений, изложенных в проекте федерального

закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях (в части установления ответственности для владельцев интернет-ресурсов, а также хостинг провайдеров за размещение (распространение) запрещенной информации о наркотических средствах и психотропных веществах)», разработанного МВД России совместно с Минкомсвязью России, ФСБ России и Минюстом России.

Рассматривая вопросы особенностей выявления и документирования преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, совершенных с использованием криптовалют стоит отметить, наша страна является правовым государством. Согласно Конституции РФ, высшей ценностью является права и свободы гражданина и человека, в связи с чем такие права и свободы человека могут быть ограничены только лишь судом путем вынесения соответствующего решения. Указанное является конституционной гарантией каждого от незаконного преследования и нарушения его прав. В сети Интернет могут проводится следующие мероприятия, требующие судебного санкционирования: 1. Контроль почтовых отправлений, телеграфных или иных сообщений; 2. «Наведение справок». 3. Получение компьютерной информации. 4. Обследование помещений, зданий, сооружений, участков местности и транспортных средств. Это те основные мероприятия, которые чаще всего применяются на практике, при выявлении и раскрытии преступлений, совершенных в сети Интернет, в том числе с использованием криптовалюты. Особенность данных мероприятий заключается в том, что посягают на права и законные интересы граждан в связи с чем их проведение ограничено судебным санкционированием.

По категории уголовных дел, связанны с незаконным оборотом наркотиков одним из условий судебной перспективы дела является качественно и детально проведенный осмотр электронных носителей информации. В рамках настоящего параграфа нами были сформулирован и представлен исчерпывающий перечень рекомендаций относительно данного

следственного действия. Роль специалиста в данном следственном действии является если не главенствующей, то точно немаловажной. Роль специалиста сводится в направлении следователя к тем деталями технического характера, сведениями и метаданным, которые могут иметь значение для уголовного дела. При этом относимость таких сведений к предмету доказывания определяется непосредственно следователем (дознавателем). Кроме того, хотелось бы отметить, что такая форма использования специальных знаний как производство судебной экспертизы и допрос эксперта является одной из неотъемлемых составляющих материалов уголовного дела, связанного с незаконным оборотом наркотических средств. Вместе с тем, эффективность данных уголовно-процессуальных средств напрямую зависит от того, насколько качественно следователь подошел к их подготовке: правильно установил обстоятельства, изъял образцы, принял меры к сохранению следов и т.д. В рамка данной категории дел, как мы можем наблюдать, перечень судебных экспертиз является достаточно разнообразным ввиду того, что данные преступления имеют отношения как к предметам материального мира (наркотикам, прекурсорам) и психике и физическому состоянию человека (в данном случае мы говорим о лицах, которые употребляют наркотические средства), так и к идеальным следам, которые содержатся в электронного носителя информации и на мощностях информационно-коммуникационной сети «Интернет».

Рассматривая вопросы совершенствования практики раскрытия и расследования преступлений, связанных с незаконным оборотом наркотических средств с использованием сведений о криптовалюте мы пришли к выводу о том, что для ее совершенствования необходимо ряд изменений в первую очередь связанных с особенностями работы следственных и оперативных подразделений. В частности, считаем важным проводить периодическое обучение сотрудников следственных и оперативных подразделений с целью повышения их знаний в сфере расследования преступлений, связанных с незаконным оборотом

наркотических средств, с использованием данных о криптовалюте. Кроме того, важно издавать методические рекомендации, направленные на работу со следами доказательственной информации для сотрудников следственных и оперативных подразделений. Отдельным направлением совершенствования практики раскрытия и расследования преступлений в данной сфере представляется совершенствование технической базы органов предварительного следствия и оперативных подразделений.

Список использованных источников

Нормативно-правовые акты

1. «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ // СПС «Гарант».

2. Модельный закон об оперативно-розыскной деятельности (в редакции Постановления Межпарламентской Ассамблеи государств — участников СНГ от 16 ноября 2016 г. № 27-6). URL: docs.cntd.ru/document/902050857 (дата обращения: 16.05.2022).

3. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : федеральный закон от 6 июля 2016 г. № 374-ФЗ // СПС «КонсультантПлюс».

4. Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Доступ из справ.-прав. системы «КонсультантПлюс».

5. Приказ Министерства труда и социальной защиты РФ от 1 ноября 2016 г. № 598н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» // СПС «Гарант».

6. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2021 года [Электронный ресурс] https://xn--b1aew.xn--p1ai/reports/item/19897618/ (дата обращения: 22.03.2022).

7. Приговор от 3 июля 2017 г. по делу № 1-125/2017 // Судебные и нормативные акты РФ (СудАкт) [сайт] (дата обращения: 20.11.2021).

8. Приговор Свердловского районного суда г. Костромы от 11 мая 2017 г. по делу № 1-136/2017 в отношении А.В. Новицкого // Судебные и нормативные акты РФ (СудАкт) [Электронный ресурс] URL: https://sudact.ru/ (дата обращения: 15.11.2021)

Научная и учебная литература

1. Агарков А.В. Содержание оперативно-розыскного мероприятия наведение справок» в современные условия // Вестник Кузбасского института. 2018. № 2 (35). С.123.
2. 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. 9.
3. Ализаде В.А., Волеводз А.Г. Неприменение ст. 174.1 Уголовного кодекса РФ по делам о наркопреступениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. 2018. № 1 (50). С. 5-13.
4. Баженов С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России № 2 (65), 2017. С. 32.
5. Бегичев А.В. Использование протоколов осмотров Интернет-сайтов в судебной практике // Вестник московского университета МВД России. 2014. № 11. С. 208.
6. Безопасность электронного банкинга / А.М. Сычев, П.В. Ревенков, А.Б. Дудка. М., 2017. 293.
7. Беломытцева О.С. О понятии криптовалюты «биткоин» в рамках мнений финансовых регуляторов и контексте частных электронных денег // Проблемы учета и финансов. 2014. № 2. С. 26 - 28.
8. Бульбачева А.А., Котяжов А.В. — Коллизии и противоречия правового регулирования в сфере противодействия незаконному обороту наркотических средств, психотропных веществ и их прекурсоров:пути совершенствования антинаркотического законодательства// Полицейская деятельность. 2020. № 3. С. 32.

9. Васюков В. Ф., Булыжкин А. В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения. Российский следователь. 2016. № 6. С. 7.

10. Воскресенская Е.В. О необходимости правового регулирования виртуальных валют // Вестник Омской юридической академии. 2018. Том 15. №2. С. 149.

11. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве. Труды Академии управления МВД России. 2017. № 4. С. 47.

12. Дворянкин О. А, Клочкова Е. Н. Криптовалюта — новый инструмент наркобизнеса // Наркоконтроль. 2018. № 4. С. 19—22.

13. Денисов Е.А. Скриншоты в системе уголовно-процессуальных доказательств: вопросы теории и практики // Вопросы студенческой науки. 2017. № 15. 180.

14. Долгиева М. М. Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы рос. права. — 2019. № 4. С. 128—139.

15. Дремлюга Р.И. Незаконный оборот наркотиков и крипторынки: угрозы и вызовы правоохранителю // Международное сотрудничество и зарубежный опыт. 2018. № 2. С. 33.

16. Дубоносов, Е. С. Оперативно-розыскная деятельность: учебник и практикум для прикладного бакалавриата. 5 изд., перераб. и доп. М., 2016. С.81.

17. Еськов В.Д., Чеботарев С.А. Особенности осмотра страниц в сети Интернет // Материалы VI Международной научной конференции студентов и магистрантов. 2017. С. 39.

18. Ефимова Л.Г. Некоторые аспекты правовой природы криптовалют //Юрист. 2019. № 3. С. 12.

19. Земцова С.И. Криптовалюта в незаконном обороте наркотических средств: вопросы деаномизации и ответственности // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 55.

20. Кейси М., Винья П., Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. Перевод на русский язык, издание на русском языке, оформление. М., 2017. С. 149.

21. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М., 2012. С. 182.

22. Козулепенко А.Р. К вопросу о роли специалиста при осмотре мобильного устройства по уголовным делам, связанным с незаконным оборотом наркотиков // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 4. С. 53.

23. Кучеров И. И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. 2018. № 12. С. 18.

24. Мамлеев Р. Р. Средства и методы осуществления оперативно-разыскного мероприятия получение компьютерной информации // Полицейская и следственная деятельность. 2016. № 4. С. 37—45.

25. Оперативно-розыскная деятельность: учебник для студентов вызов, обучающихся по специальности «Юриспруденция» / под ред. И.А. Климова. М., 2014. С.311.

26. Оперативно-розыскная энциклопедия / Авт. – сост. проф. А.Ю. Шумилов. М.: Изд-ль Шумилова И.И., 2004. С.159-160.

27. Ривман Д. В. Комментарий к Федеральному закону «Об оперативно-розыскной деятельности». СПб., 2003. С.98.

28. Родивилин И. П., Родивилина В. А. Криптовалюта как объект преступления // Деятельность правоохранительных органов в современных условиях: сб. мат-лов XXIII междунар. научно-практ. конф. В 2-х тт. — Иркутск: Восточно-Сибирский институт МВД России, 2018. С. 262—265.

29. Романенко М.А. Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения // Вестник Омского университета. 2008. № 1. С. 172.

30. Савельев А.И. Криптовалюты в системе объектов гражданских прав // Закон. 2019. № 8. С. 138.

31. Сальников Е.В. Сальникова И.Н. Криптовалюта как иновация экономики терророра // Науковедение. 2016. № 3. С. 33.

32. Санчат Ч.А. К вопросу о допустимости в качестве доказательств компьютерной информации, размещенной в сети интернет // Новая наука: от идеи к результату. 2017. № 3. С. 189.

33. Серов А.В., Дубинин А.С. Получение компьютерной информации как самостоятельное оперативно-розыскное мероприятие // Вестник Воронежского института МВД России. 2018 № 3. С. 170.

34. Сидоренко Э.Л. Наркотики и криптовалюта: новые криминологические тренды // Наркоконтроль. 2018. № 2. С. 8-13.

35. Сидорова К.С. Способы установления ip-адреса и сведений о нем при расследовании уголовных дел // Вестник Сибирского института бизнеса и информационных технологий. 2018. № 2. С. 88.

36. Судницын А. Б., Молоков В. В. Отдельные возможности получения и использования сведений об операциях с криптовалютой при раскрытии и расследовании преступлений // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 213—221.

37. Теория оперативно-розыскной деятельности / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. М., 2006. С.182

38. Трибушный И.Ю., Трибушная М.И., Трибушная В.Х. Ключевые аспекты российской цифровой экономики и ее нормативного регулирования // Инновационная экономика: перспективы развития и совершенствования, № 8 (34), 2020. С. 43.

39. Трунцевский Ю. В. Цифровая (виртуальная) валюта и противодействие отмыванию денег: правовое регулирование // Банковское право. 2018. № 2. С. 18—28.

40. Тумаков А.В., Петраков Н.А. Правовой режим криптовалюты // Государственная служба и кадры. 2021. № 5. С. 174.

41. Федеральный закон «Об оперативно-розыскной деятельности»: научно-практический комментарий / под ред. д-ра юрид. наук, проф А.С. Бахты. Хабаровск, 2013. С.54.

42. Хажиахметова Е.Ш. Криптовалюта – деньги XXI век // новая наука: от идеи к результату. Агентство международных исследований, 2016. № 11.

Интернет-ресурсы

1. FATF/GAFI. Regulation of virtual assets. Paris, 19 October 2018. [Электронный ресурс] URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html (дата обращения: 20.11.2021).

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронныйресурс] URL: https://bitcoin.org/bitcoin.pdf (датаобращения: 07.11.2021).

3. Russo, Camila. Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now. Bloomberg. [Электронный ресурс] URL: https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now?srnd=cryptocurriences (дата обращения: 12.11.2021 г.).

4. World Drug Report 2017, Presentation, UNDOC. [Электронныйресурс] URL:

http://www.unodc.org/wdr2017/field/WDR_2017_presentation_lauch_version.pdf (датаобращения: 22.11.2021)

5. В компании Bitfury появилась технология по отслеживанию ненадежных транзакций URL:https://crypt-mining.net/news/v-kompanii-bitfury-poyavilas-texnologiya (дата обращения 18.05.2022).

6. Все криптовалюты [Электронный ресурс] URL: https://investing.com (дата обращения: 19.11.2021).

7. Криптовалюты [Электронный ресурс] URL: https://www.mercatus.org/ (дата обращения: 03.11.2021).

8. МВД России обнародовало проект антинаркотической стратегии до 2030 года [Электронный ресурс] URL: http://политикапрезидента.рф/mvd-obnarodovalo-proekt-antinarkoticheskoy-strategii-do-2030-goda (дата обращения: 22.03.2022).

9. Рускоин. [Электронный ресурс] URL: https://ruscoin.io/ (дата обращения: 19.11.2021).

10. Суд в России разрешил арестовать Ethereum на миллиард рублей URL:https://www.rbc.ru/crypto/news/624c17599a7947515eb896fa (дата обращения 22.04.2022).