Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2021. – Т. 7 (73). № 3. – С. 155-162.

УДК 343.9
DOI 10.37279/2413-1733-2021-7-3(2)- 155-162

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ ПРИ ПОЛУЧЕНИИ ИНФОРМАЦИИ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ И ДРУГИХ ВИРТУАЛЬНЫХ АКТИВОВ

Лагуточкин А. В., Ильинский И. И.

В статье раскрывается вопрос проведения оперативно – розыскных мероприятий при получении информации о преступлениях, совершенных с использованием криптовалют и других виртуальных активов. Как известно к числу главных задач теории оперативно-розыскной деятельности (далее – ОРД) необходимо отнести процесс совершенствования этой деятельности на основе оптимального сочетания организационно-управленческих и оперативно-тактических мероприятий, изучение передовой оперативно-розыскной практики и разработка на этой основе действенных способов организации и практического осуществления оперативно-розыскных мероприятий (далее – ОРМ) в различных условиях оперативной обстановки. Любые современные исследования в данной области представляются попыткой по-иному представить сложившиеся практикой процессы, сформировать новые идеи вокруг реализации поставленных перед субъектами ОРД задач. И, достаточно редко, формируются направления инновационного развития ОРД, формирования совершенно новых подходов и тактик в условиях противодействия преступлениям, совершенным с использованием криптовалют и других виртуальных активов. Представленная статья является одной из тех, которые для исследователей формируют идею, путь, методическое направление по которому в ближайшем будущем необходимо пройти. Представленные направления и способы борьбы с преступлениями, совершенные с использованием криптовалют и других виртуальных активов, уже предопределены существующими событиями в стране и в мире, а также возможны в соответствии с перспективным технологическим прогрессом человечества.

В деятельности органов внутренних дел произошли значительные изменения. Следует принять во внимание отдельные изменения законодательной и ведомственной нормативной базы, регламентирующей оперативно-розыскную деятельность, организационно-структурные перестроения в органах внутренних дел, корректировку функционирования социальных институтов в условиях постоянного развития и т.п. Указанные обстоятельства диктуют необходимость осмысления современных реалий в сфере противодействия преступлениям, совершенным с использованием криптовалют и других виртуальных активов, поиска результативных форм и методов борьбы, выработки эффективных мер по оптимизации деятельности уполномоченных субъектов и других подразделений полиции.

Ключевые слова: программное обеспечение, информация, технологии, правоохранительная деятельность, искусственный интеллект, криптовалюта, виртуальные активы.

Важно отметить, что на сегодняшний день владельцев криптовалют в России немало. По приведенным данным, наша страна входит в тройку государств – лидеров по использованию цифровых валют, а количество криптокошельков граждан РФ превышает 8 млн, – еще какое-то время придется ждать принятия такого законодательства [1]. Рассматривая спектр преступлений, совершенных с использованием криптовалют и других виртуальных активов, необходимо сделать вывод, что их число достаточно велико, а их количество и качество имеет прогрессивное состояние по отношению к общей преступности. Ограничением могут быть лишь те преступления, которые априори, не могут быть совершены с использованием сетевого цифрового пространства или спонсированы с использованием указанных финансовых активов. Например, ст. 245 УК РФ «Жестокое обращение с животными» сама

по себе не может быть связана с использованием криптовалют и других виртуальных активов кроме случаев финансовой подпитки преступников со стороны иных лиц через виртуальные активы. Так, преступление будет иметь большую общественную опасность, если осуществлялось издевательство над животными с использованием онлайн трансляции через Интернет, а финансовая сторона преступления была спровоцированы ради наживы извне, со стороны.

Сфера объектов, имеющих особое внимание оперативных подразделений, в части использования криптовалют и других виртуальных активов весьма разнообразна, что говорит о необходимости применения всех оперативно-розыскных инструментов для выявления, предупреждения, пресечения и раскрытия преступных намерения или совершившихся фактов. Сами по себе криптокошельки иные виртуальных активы являются второстепенными по отношению к самому преступлению, так как, немалая часть преступных деяний имеют нематериальный состав и получение или использование материальных ресурсов становится не важным, но имеющим доказательственное значение, например, для установления мотива преступления.

ОРД в своем понимании представляет собой систему действий и противодействий, которая осуществляется специальным субъектом, для осуществления защиты жизни и здоровья, обеспечения прав и свобод человека и гражданина, права собственности, обеспечение безопасности общества и государства от преступных посягательств [4].

Существуют ряд оперативно-розыскных мероприятий, которые напрямую участвуют в процессе документирования действий, проверяемых и разрабатываемых, использующих криптовалюту и другие виртуальные активы в своей преступной деятельности.

Алгоритм действий оперативного сотрудника можно представить в следующей последовательности решаемых оперативно-тактических задач: 1. Выявление и досмотр электронных устройств, с помощью которых фигурант осуществляет контроль над своими виртуальными активами. 2. Получение информации об активности использования фигурантом виртуальных активов в преступной деятельности и ее документирование. 3. Реализация полученной информации, легализация ее в уголовном процессе.

Выявление устройств осуществляется: Контактным (личным) способом. 2) Бесконтактным способом. Контактный способ может быть гласным (официальным) или с применением оперативных комбинаций. Бесконтактный способ осуществляется по подготавливаемым оперативным сотрудником заданиям на проведение специальных технических мероприятий в ПСТМ. Контактный способ наиболее часто используем в силу того, что фигурант может быть задержан за совершение административного правонарушения или в иных законных случаях. В естественно складывающихся условиях оперативником избирается способ досмотра электронного устройства, в том числе, исходя из оперативно-розыскной тактики. Перед досмотром определяется устройство, частники и используемая техника. Чаще всего, этими устройствами выступают: смартфоны, планшеты, ноутбуки, компьютеры и роутеры (как средство выхода в сеть). Иногда встречаются случаи использование компьютеров в Интернет-кафе или иных общественных местах.

Процесс выявления устройств, используемых преступником в последнее время осложняется тем, что у фигуранта в пользовании могут быть до десятка смартфо-

нов, компьютеров, ноутбуков. Так, Российский рынок смартфонов по итогам первого квартала 2021 г. увеличился по сравнению с аналогичным периодом прошлого года на 27% в денежном выражении и составил 153 млрд. руб. По многим информационным данным, россияне стали больше внимания уделять выбору смартфона, среднее время интернет-сессий пользователей в онлайн-магазинах и на сайтах с отзывами про гаджеты за последний год увеличилось на 40%.

В частности, после получения доступа к техническому устройству, оперативный сотрудник самостоятельно определяет какое ОРМ необходимо для решения стоящих задач. Важным является то: 1) какая информация необходима для процесса документирования и доказывания преступных деяний; 2) необходимы ли дополнительные знания для осуществления осмотра технического устройства (привлечение специалиста).

Осуществляя оперативный осмотр, сотрудник вправе внешне определить необходимые данные. После включения устройства изучает электронные последовательности открытий и иной активности фигуранта. В случае необходимости осуществляет документирование процесса осмотра посредством использования фотовидео, результаты которого могут быть приобщены к протоколу осмотра устройства в виде фототаблицы.

Каждый оперативник с базовыми знаниями технических устройств должен знать и выявлять следующие обязательные данные: 1) для смартфонов – «абонентский номер» это – номер, идентифицирующий оконечный элемент сотовой связи. Он состоит из 11 последовательных цифр, 1-ая из которых определяет код страны, 2,3,4-ая определяют принадлежность абонентского номера к региону или оператору сотовой связи, остальные – определяющий номер клиента; 2) IMEI (International Mobile Equipment Identity – международный идентификатор мобильного оборудования) – уникальный номер сотового аппарата. Данный номер состоит из 15 последовательных чисел, из которых первые 14 определяют происхождение, модель и серийные номер сотового устройства, а 15-ая – контрольная цифра. В предоставляемых сотовыми операторами детализациях последняя контрольная цифра всегда обозначается как «0». Она не имеет целевого значения, поэтому идентификация сотового аппарата при его изъятии всегда происходит по первым 14 цифрам. Зная IMEI, посредством множества онлайн-сервисов мы можем определить марку и модель сотового телефона. Одним из самых удобных сервисов является www.imei.info. 3) IP-адрес (Internet Protokol address) – это уникальный идентификационный номер, который присваивается каждому компьютеру при выходе в сеть интернет. Он представляет собой последовательность из 4 цифр в диапазоне от 0 до 255, чередующихся через точку. Например, 178.218.36.0. IP-адрес выдается компьютеру его интернет провайдером в момент начала интернет сессии – открытия первой интернетстраницы, и заканчивается закрытием интернет-сессии – закрытием последней интернетстраницы. IP-адрес выдается компьютеру его интернет провайдером в момент начала интернет сессии – открытия первой интернетстраницы, и заканчивается закрытием интернет-сессии – закрытием последней интернет-страницы.

Таким образом, на каждом сайте («Вконтакте», «Авито», «Юла» и др.) хранится история соединений с его пользователями, а, следовательно, и их IP-адреса. При каждом выходе в интернет преступник оставляет свой «след», по которому его можно вычислить. Также как и абонентский номер, IP-адрес имеет свой ресурс ну-

мерации, то есть каждому интернет провайдеру выделено определенное количество IP-адресов в конкретном диапазоне. При помощи интернет ресурса www.2ip.ru (прямая ссылка: www.2ip.ru/whois/), зная IP-адрес, можно определить провайдера.

1. MAC-адрес (Media Access Control – надзор за доступом к среде, также Hardware Address, также физический адрес) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), «прошитый» в ней при изготовлении. Этот номер используется для идентификации отправителя и получателя фрейма; и предполагается, что при появлении в сети нового компьютера (или другого устройства, способного работать в сети) сетевому администратору не придётся настраивать этому компьютеру MAC-адрес вручную.

Уникальность MAC-адресов достигается тем, что каждый производитель получает в координирующем комитете IEEE Registration Authority диапазон из 16 777 216 адресов и, по мере исчерпания выделенных адресов, может запросить новый диапазон. Поэтому по трём старшим байтам MAC-адреса можно определить производителя. Существуют таблицы, позволяющие определить производителя по MAC-адресу; в частности, они включены в программы типа arpalert.

В широковещательных сетях (таких, как сети на основе Ethernet) MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне модели OSI, которую используют протоколы более высокого (сетевого) уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, ARP и RARP в сетях IPv4, и NDP в сетях на основе IPv6).

В случае проведения ОРМ исследования предметов (смартфоны, ноутбуки, компьютеры и роутеры) значительным является образовательный уровень оперативного сотрудника и технические возможности. Не каждое техническое устройство оснащено одинаковыми процессами и программным обеспечением. Базовые специальные знания позволяют на начальном уровне определить направления поиска и устанавливать местонахождение электронных следов проводимых фигурантом операций. Однако уровень подготовки оперативных сотрудников для работы в рассматриваемом сегменте крайне полярен и неодинаков, чаще, готовность ограничивается знаниями, приобретенными в процессе пользования информационных сетей в условиях самообучения и не имеет своей специализации. Потому обязательным на этапе исследования является привлечение специалиста. Специалист привлекается из числа: обладающих специальными знаниями, в тех направлениях, которые необходимы оперативному сотруднику (IT – сфера, программисты, обслуживающие сети, сотрудники информационных компаний и т.д.); сотрудники ЭКЦ; сотрудники ПСТМ.

Последние, на наш взгляд, являются более привлекательными субъектами. Во-первых, являются сотрудниками МВД, во –вторых, являются оперативными сотрудниками, обладающими и осуществляющими ОРД в полном объеме полномочий, в третьих, помимо знаний обладают возможностями использовать состоящую на вооружении специальную технику, которая по своим свойствам уникальна и из-

готовлена под решение оперативно-розыскных задач. Для организации участия специалиста ПСТМ необходимо подготовить в соответствии с нормативными и правовыми актами МВД задания и сопутствующих документов, определить и согласовать по времени, месту и тактики организации исследования.

В идеале, оперативный сотрудник должен представить информацию специалисту об исследуемом техническом устройстве, а именно: наименование, модель устройства; установленное программное обеспечений (в том числе, информация о фаерволах устройства); имеющиеся элементы блокировки; сформулировать вопросы необходимые для специалиста об устройстве.

Чаще информация специалисту поступает не в полном объеме и восполняет специалист информацию на месте исследования самостоятельно.

Специалист, исследуя устройства, определяет наиболее важные элементы: 1) Наличие установленного программного обеспечения связанного с использованием криптовалют и других виртуальных активов. 2) Устанавливает признаки использования криптовалют и других виртуальных активов при которых требуется для выявления следов дополнительного применения специального оборудования.

Важно отметить, что проведение исследования может предшествовать судебной компьютерно-технической экспертизе при расследовании преступлений, связанных с использованием криптовалюты и иных виртуальных активов.

Помимо названного выше, особый интерес вызывает зарегистрированная на фигуранта электронная почта. Достаточно часто, многие сервисы для идентификации и верификации, а также для определения «логина» используют электронную почту. Таким образом, перлюстрация представленных электронных ресурсов расширяет сферу поиска криптовалют и других виртуальных активов.

В случае выявления информации о цифровых финансовых активах действия сотрудника оперативного подразделения связано с проведением ОРМ «Наведение справок». Наведение справок – это способ собирания информации, необходимой для решения задач ОРД, путем изучения документов (в том числе архивных), а также направления запросов в любые органы физическим и юридическим лицам, имеющим информационные системы. Наведение справок предполагает сбор сведений о биографии проверяемых, их родственных связях, образовании, роде занятий, имущественном положении, месте проживания, фактах допущенных в прошлом правонарушений и других данных, необходимых для конкретных задач ОРД.

Современная концепция осуществления государственного управления, характерна для информационного общества, которое способно удаленно посредством сетей реализовывать необходимые задачи. Сегодня большинство организаций осуществляют работу в условиях использования глобальных и иных информационных сетей, представляя широкий спектр услуг. Поэтому один из способов наведения справок вытекает из сказанного – путем направления запросов (электронных) в государственные и иные организации, объединения, общества.

Так, выявленные электронные кошельки, наиболее популярными представителями которых являются «Киви банк», «Яндекс.Деньги», «ВэбМани» и «Тинькофф – мобильный кошелек», излюбленные ресурсы преступников, так как для их создания необходим только абонентский номер. Эти организации не имеют представительств, поэтому все операции производят онлайн. Обычный не идентифицированный кошелек имеет мало возможностей – хранение не более 15 000 руб., оборот не более

40 000 руб. в месяц, запрет на вывод денежных средств в иные платежные сервисы, способен совершать только интернет покупки и онлайн платежи. Полностью же идентифицированный кошелек имеет все возможности банковских карт. Что важно знать, на один электронный кошелек можно открыть бесконечное множество виртуальных платежных карт, то есть сервис электронных кошельков номинально выдает пользователю контрольные данные по платежной карте без ее пластикового носителя. Основная информация, которую возможно получить по электронному кошельку (помимо установочных данных владельца и движения денежных средств) – это привязанные к нему абонентские номера и использованные IP-адреса.

Многие фигуранты принимают денежные средства на счет абонентских номеров. У каждого сотового оператора есть свои особенности по указанному направлению: 1) расчетные операции по абонентским номерам «Билайн» проводит ЗАО «Национальная сервисная компания». Поэтому данные о движении денежных средств можно запросить как у самого оператора «Билайн», так и у ЗАО «НСК»; 2) расчетные операции по абонентским номерам «МТС» ПАО «Мобильные ТелеСистемы» проводят самостоятельно, поэтому данные о движении денежных средств можно запросить только у самого сотового оператора; 3) расчетные операции по абонентскому номеру «Мегафон» проводит ООО «банк Раунд». Данные о движении денежных средств можно запросить только у данной организации; 4) у оператора сотовой связи «теле2» нет устоявшегося корреспондента и для проведения расчетных операций он может использовать много сторонних организаций. Информацию о движении денег нужно запрашивать у самого оператора, а после – у корреспондента.

Отдельно необходимо отметить о банковских возможностях. Банковские и кредитные организации способны отслеживать транзакции клиентов, в том числе переводы на виртуальные активы или криптокошельки. Запросы в банки о наличии и движении денежных средств по счетам в определенный период времени в отношении подозреваемых, совершающих или совершивших преступления – обязательны.

Кроме электронной почты, любопытным по отношению к разработке фигуранта являются и социальные сети. Так, на начало 2020 г. в России безусловное 1 место по ежемесячному охвату аудитории занимает сеть «В Контакте» – 40,1 млн. активных пользователей. По мнению экспертов, главное преимущество соцсети – это ее техническая продвинутость. На втором месте находятся «Одноклассники» с аудиторией в 29,8 млн. аккаунтов.

Крупнейшая в мире социальная сеть Facebook, насчитывающая на сегодняшний день свыше 900 млн активных участников, в Рунете пока занимает лишь третье место – 9,8 млн. человек. Однако с сентября 2013 г., сеть демонстрирует впечатляющие темпы роста. За год ее российская аудитория выросла на 56%, также у «В Контакте» на 24%, а у «Одноклассники» на 32%. Но скорее всего, такой активный рост связан с тем, что изначально число пользователей Facebook в России было незначительным. Посмотрим, удастся ли в этом году соцсети сохранить такой темп роста.

Количество пользователей сервиса микроблогов Twitter превышает 250 мил. человек, при этом количество российских пользователей, по статистике компании «Яндекс», составляет более 2,64 млн. человек.

Запустившаяся в конце июня новая соцсеть Google+ продолжает набирать популярность. К концу 2014 г. Google+ уже насчитывала 83 млн. пользователей. Данных по количеству пользователей Google+ в Рунете нет. Представленные сайты – это

огромный банк данных, перлюстрируя которые оперативный сотрудник может получать необходимые искомые данные необходимые для решения стоящих задач.

Что очень важно в проведении ОРМ «Наведенис справок» это то, что необязательно обращаться в правоприменительные органы иностранных государств с просьбой, о наведении справок на территории данного государства, ибо эти действия можно равноудалено провести с включенного в сеть ПК. Основное отличие наведения справок как оперативно-разыскного мероприятия от следственного действия, направленного на сбор информации, состоит в том, что истинные цели оперативно-разыскного мероприятия могут легендироваться, скрываться.

Считаем важным отметить ныне действующий Федеральный закон от 31.07.2020 N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», использование криптовалюты законодательно ограничено: прямо установлен полный запрет на оплату цифровой валютой товаров, работ и услуг – он распространяется на действующие на территории России юридические лица, в том числе филиалы и представительства иностранных и международных компаний, и на граждан, находящихся в РФ не менее 183 дней в течение 12 следующих подряд месяцев [2].

В ФЗ об ОРД отсутствуют какие-либо ограничения на получение в процессе наведения справок информации конфиденциального характера, однако следует учитывать, что действующим российским законодательством установлены специальные режимы ограничения доступа к достаточно большому объему сведений, относящихся к частной жизни граждан, а также составляющих профессиональную тайну: государственную (см. ст. 29 Конституции РФ, Закон о государственной тайне, ст. ст. 283 и 284 УК РФ), коммерческую, служебную (см. ст. 139 ГК РФ; ст. 183 УК РФ), личную и семейную, тайну предварительного следствия (см. ст. 310 УК РФ) и др. [3]. В заключении хотелось бы отметить, что раскрытие преступлений связанным с криптовалютой и иными виртуальными активами без использования специальных знаний, является затруднительным, а нередко и вовсе невозможным.

Список литературы

1. Шувалова М. Криптовалюта в России: законодательное недорегулирование. 1 марта 2021. [Электронный ресурс] https://www.garant.ru/news/1448450/ (10.07.2021).
2. Федеральный закон от 31 июля 2020 г. N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»
3. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации от 14 августа 1995 г. № 33 ст. 3349.
4. Титов М.В., Иванов С.И. Получение компьютерной информации – как новый вид оперативно-розыскного мероприятия // Молодая наука. Сборник научных трудов научно-практической конференции для студентов и молодых ученых. Научный редактор Н.Г. Гончарова. 2017. С. 395-396.

A.V. Lagutochkin, I.I. Ilyinskiy. Features of conducting operational investigative measures when obtaining information about crimes committed using cryptocurrencies and other virtual assets // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2021. – T. 7 (73). № 3. – P. 155-162.

The article reveals the issue of conducting operational investigative measures when obtaining information about crimes committed using cryptocurrencies and other virtual assets. As is known, the main tasks of the theory of operational search activities (hereinafter referred to as ORD) should include the process of improving this activity on the basis of an optimal combination of organizational, managerial and operational tactical measures, the study of advanced operational search practices and the development on this basis of effective ways of organizing and practical implementation of operational search activities (hereinafter referred to as ORM) in various operational conditions. Any modern research in this area seems to be an attempt to present the processes that have developed in practice in a different way, to form new ideas around the implementation of the tasks assigned to the subjects of the ORD. And, quite rarely, directions of innovative development of

the HORDES are formed, the formation of completely new approaches and tactics in the context of countering crimes committed using cryptocurrencies and other virtual assets. The presented article is one of those that for researchers form an idea, a path, a methodological direction along which it is necessary to go in the near future. The presented directions and methods of combating crimes committed using cryptocurrencies and other virtual assets are already predetermined by existing events in the country and in the world, and are also possible in accordance with the promising technological progress of mankind. At present, significant changes have taken place in the activities of the internal affairs bodies. It is necessary to take into account certain changes in the legislative and departmental regulatory framework regulating operational and investigative activities, organizational and structural changes in the internal affairs bodies, adjustment of the functioning of social institutions in conditions of constant development, etc. These circumstances dictate the need to understand modern realities in the field of countering crimes committed using cryptocurrencies and other virtual assets, to search for effective forms and methods of fighting, to develop effective measures to optimize the activities of authorized entities and other police units.

Key words: software, information, technologies, law enforcement, artificial intelligence, cryptocurrency, virtual assets.

Spisok literatury

1.Shuvalova M. Kriptovalyuta v Rossii: zakonodatel'noe nedoregulirovanie. 1 marta 2021. [Elektronnyj resurs] https://www.garant.ru/news/1448450/ (10.07.2021).

2.Federal'nyj zakon ot 31 iyulya 2020 g. N 259-FZ «O cifrovyh finansovyh aktivah, cifrovoj valyute i o vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federacii»

3.Federal'nyj zakon ot 12 avgusta 1995 g. № 144-FZ «Ob operativno-rozysknoj deyatel'nosti» // Sobranie zakonodatel'stva Rossijskoj Federacii ot 14 avgusta 1995 g. № 33 st. 3349.

4.Titov M.V., Ivanov S.I. Poluchenie komp'yuternoj informacii – kak novyj vid operativno-rozysknogo meropriyatiya // Molodaya nauka. Sbornik nauchnyh trudov nauchno-prakticheskoj konferencii dlya studentov i molodyh uchenyh. Nauchnyj redaktor N.G. Goncharova. 2017. S. 395-396.

.