КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

Э. С. Маркарян*

Специфика проведения следственного осмотра при расследовании преступлений, совершенных с использованием криптовалют

Аннотация. *В статье проведен анализ особенностей производства следственного осмотра при расследовании преступлений, совершенных с использованием криптовалют. Определяются объекты, подлежащие осмотру, предлагаются криминалистические рекомендации для повышения эффективности результатов его проведения и меры по обеспечению сохранности полученных данных. Отмечено, что по делам о преступлениях, совершенных с использованием криптовалют, в качестве места происшествия могут выступать адрес местонахождения физического лица или организации и место нахождения используемых аппаратно-программных средств. Специфика осмотра предметов и документов по делам о преступлениях, совершенных с использованием криптовалют, заключается в том, что осмотру подлежат, как правило, служебные журналы системных и прикладных программ, программ-кошельков, применяемых для осуществления транзакций, а также файлы wallet.dat или иные, содержащие сведения о кошельках. В ходе проведения осмотра необходимо обратить внимание на то, что персональный компьютер будет являться наиболее важным источником криминалистически значимой информации ввиду специфики совершаемых преступлений.*

Ключевые слова: *преступления, совершенные с использованием криптовалют; следственный осмотр; объекты осмотра; тактические приемы.*

DOI: 10.17803/1994-1471.2018.91.6.146-152

Для обеспечения правильности выбора тактики производства следственных действий необходимо проведение совместной следственной и оперативной оценки собранной информации. Некачественное документирование собранной информации, а также неквалифицированное проведение отдельных следственных действий, часто приводят к тому, что собранные и задокументированные данные не позволяют своевременно начать расследование, ибо не обеспечивают следственную перспективу уголовных дел.

Предпосылками к успешному расследованию преступления с использованием криптовалют в большинстве случаев будут быстрота и решительность действий следователя и опе-

* *Маркарян Эльвира Сергеевна,* соискатель кафедры криминалистики Воронежского государственного университета
seledkva@mail.ru
394018, Россия, г. Воронеж, Университетская пл., д. 1

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

Перечень неотложных следственных действий и оперативно-розыскных мероприятий, очередность их проведения будут определяться конкретной следственной ситуацией, в которой начинается расследование[1].

Осмотр, обыск и выемка являются важнейшими инструментами установления обстоятельств расследуемого события и главными процессуальными способами изъятия вещественных доказательств по делам данной категории. При осмотрах, обысках, выемках, сопряженных с изъятием электронных носителей информации, возникает ряд общих проблем, связанных со спецификой изымаемых технических средств[2].

Рассмотрим более подробно особенности производства следственного осмотра (места происшествия, предметов и документов) в процессе расследования преступлений, совершенных с использованием криптовалют.

Одним из самых важных следственных действий на первоначальном этапе расследования преступлений, совершенных с помощью криптовалют, является осмотр места происшествия. Сущность осмотра заключается в непосредственном исследовании следователем, дознавателем, а также другими участниками следственного действия обстановки места происшествия; выявлении, изучении, фиксации и изъятии в установленном законом порядке материальных объектов и следов на них с целью получения сведений и доказательств, имеющих значение для раскрытия и расследования преступлений, а также событий, содержащих признаки преступления[3].

Проведение осмотра предполагаемого или действительного места происшествия в ряде случаев имеет решающее значение для установления факта наличия или отсутствия оснований для возбуждения уголовного дела[4]. В этой связи закон допускает производство данного следственного действия на основании ч. 2 ст. 176 УПК РФ до возбуждения уголовного дела. Основания для проведения осмотра и процессуальный порядок установлены в ст. 176—178 УПК РФ.

Осмотр по делам о преступлениях, совершенных с использованием криптовалют, позволяет установить ряд *важных* обстоятельств, а именно:

— наличие следов события, подлежащего расследованию;
— если факт наличия следов установлен, то необходимо установить, содержатся ли признаки состава преступления;
— кто непосредственно принимал участие в совершении преступления и какую функцию выполнял;
— наличие свидетелей совершения преступления;
— наличие на месте происшествия носителей информации, содержащих следы события, подлежащего расследованию;
— наличие технических средств, которые использовались для доступа к информации;
— имеются ли на месте происшествия следы подготовки к преступлению;
— были ли предприняты попытки сокрытия следов преступления, если да, то какие именно.

По делам о преступлениях, совершенных с использованием криптовалют, в качестве места происшествия могут выступать адрес местонахождения физического лица или организации и место нахождения используемых аппаратно-программных средств.

Основными объектами, подлежащими осмотру, являются помещения, где расположена компьютерная техника, переферийные устройства, оптические и магнитные носители, рас-

---

1 *Зеленский В. Д.* Криминалистическая методика расследования отдельных видов и групп преступлений : учебное пособие. Краснодар : КубГАУ, 2013. С. 146.

2 Криминалистика / под ред. Н. П. Яблокова. М., 2005. С. 689.

3 Криминалистика : учебник для вузов / под ред. Р. С. Белкина. М., 1998. С. 550.

4 Руководство по расследованию преступлений : учебное пособие / рук. авт. колл. А. В. Гриненко. М., 2002. С. 172.

печатки, мобильные телефоны. При осмотре помещения необходимо обращать внимание на небольшие листки (клочки, обрывки) бумаги, которые нередко прикрепляются к компьютеру или находятся в непосредственной близости от него (на них могут быть записаны коды и другие важные для следствия пометки).

Носители информации, имеющей отношение к расследуемому событию, могут быть с соблюдением установленного УПК РФ порядка изъяты и приобщены к уголовному делу в качестве вещественного доказательства.

Сразу по прибытии на место происшествия необходимо принять меры к обеспечению сохранности информации в подлежащих осмотру объектах, для чего необходимо соблюдать следующие правила:

— не разрешать кому бы то ни было из лиц, находящихся в это время в помещении, прикасаться к объектам осмотра;
— не разрешать кому бы то ни было выключать электроснабжение объекта;
— не разрешать никому и не производить самому никаких манипуляций с техникой, если их результат заранее не известен;
— необходимо учитывать вероятность принятия лицами, заинтересованными в сокрытии преступления, мер по уничтожению информации и других ценных данных, а также вероятность установки в осматриваемую компьютерную технику специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специального сигнала или кода, автоматически уничтожают всю хранящуюся там информацию либо интересующую следствие наиболее важную ее часть и вероятность установки иных средств защиты информации от несанкционированного доступа.

На месте происшествия, как правило, могут находиться электронные носители информации: внешние накопители на жестких магнитных дисках, оптические диски, flash-накопители. Соответственно, в протоколе осмотра места происшествия необходимо указать на факт их наличия и отметить данные о месте нахождения носителя информации, его типе, названии, а также информацию, индивидуализирующую и идентифицирующую объект (маркировочные обозначения, серийные номера, характерные надписи и метки и т.п.).

Также не исключается наличие на месте происшествия различной цифровой техники (ноутбуков, мобильных телефонов, планшетных компьютеров, электронных книг и т.п.), на носителях которых могут остаться следы события преступления. Наличие такого рода техники описывается в протоколе с указанием сведений, аналогичных сведениям, проводимым при обнаружении носителей информации, однако дополнительно указывается комплектация оборудования.

Необходимо учитывать, что преступление, совершенное с использованием криптовалют, может быть совершено и с рабочего места, где все данные хранятся на сервере. Соответственно, необходимым условием для надлежащего проведения расследования будет проведение осмотра помещения с сервером, на котором предположительно будет иметься информация, относящаяся к событию преступления. В данном случае в протоколе осмотра необходимо будет указать на факт наличия технических средств, к которым нет логического доступа непосредственно из осматриваемого помещения, поскольку рабочее место по управлению сервером будет находиться, как правило, в другом помещении. Целесообразно будет указать на место доступа к серверу с правами администратора, и данное место также должно подлежать осмотру в качестве места происшествия.

При осмотре места преступления необходимо дополнительно обратить внимание на:

— обнаружение, осмотр и изъятие средств подготовки, совершения и сокрытия преступления;
— наличие электронных средств связи;
— наличие специальных технических средств для негласного получения информации;
— наличие специальной литературы, методических рекомендаций и цифровых видеофильмов, раскрывающих способ преступления;
— наличие электронных записей, находящихся в памяти цифрового устройства и содержащих криминалистически значимые сведения — bitcoin-адреса, имена, номера теле-

фонов, сетевые псевдонимы, сетевые адреса и другую информацию.

Важно отметить, что по результатам осмотра следователь или дознаватель может установить, совершено ли преступление с использованием криптовалют либо происшедшее событие является следствием негативных факторов или правонарушением иного рода.

Осмотр предметов по делам о преступлениях, совершенных с использованием криптовалют, на первый взгляд не содержит особой специфики по сравнению с аналогичным осмотром, проводимым по делам о преступлениях в сфере информационно-коммуникационных технологий, порядок и содержание которого детально описаны А. Н. Яковлевым, В. Б. Веховым В. Ю. Агибаловым, П. В. Костиным, Т. Э. Кукарниковой и другими учеными[5]. Вместе с тем это не совсем верное утверждение. Специфика осмотра предметов и документов по делам о преступлениях, совершенных с использованием криптовалют, заключается в том, что осмотру подлежат, как правило, служебные журналы системных и прикладных программ, программ-кошельков, применяемых для осуществления транзакций, а также файлы wallet.dat или иные, содержащие сведения о кошельках. Это предполагает использование в ходе осмотра современного программного обеспечения, позволяющего быстро находить требуемые файлы и интерпретировать их содержимое. Использование в этих целях компьютера, специально не подготовленного для проведения осмотра, например рабочего компьютера следователя, нецелесообразно.

В ходе проведения осмотра необходимо обратить внимание на то, что персональный компьютер (ПК) будет являться наиболее важным источником криминалистически значимой информации ввиду специфики совершаемых преступлений. Повышенное внимание сто́ит обратить на аппаратное содержимое ПК, в первую очередь на жесткий диск (внутренний или внешний) и сетевую карту. Обусловлено это тем, что именно на жестком диске, как правило, хранится информация об используемом специализированном программном обеспечении (ПО) для работы с криптовалютами, а именно программы-кошельки и программы для майнинга. Сетевые карты, в свою очередь, обладают уникальным номером (MAC-адресом), который используется интернет-провайдерами для идентификации своих клиентов, что в последующем может стать важным для деанонимизации пользователя криптовалют. В процессе проведения осмотра необходимо установить IP- и MAC-адрес ПК. IP-адрес присваивается интернет-провайдером и используется для идентификации компьютера в сети Интернет при передаче и приеме информации. MAC-адрес задается каждому устройству, предназначенному для работы в компьютерных сетях, на заводе-изготовителе. Однако следует помнить, что MAC-адрес может быть подменен средствами операционной системы. Установление IP- и MAC-адресов и сопоставление их с данными, полученными от провайдеров интернет-услуг и платежных систем, позволяет установить причастность пользователя к совершению преступления.

Также немаловажно изучить данные всех браузеров, установленных на ПК. Ввиду того, что многие пользователи криптовалют используют их для просмотра специализированных сайтов о криптовалютах, для регистрации онлайн-кошельков криптовалют, посещения сайтов бирж и обменников. Особо пристальное внимание следует уделять Tor-браузеру, в случае его на-

[5] См., например: *Агибалов В. Ю.* Виртуальные следы в криминалистике и уголовном процессе М., 2012. С. 91 ; *Вехов В. Б.* Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники : учеб. -метод. пособие. М., 2000. С. 25 ; *Костин Г. В.* Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики : автореф. дис. ... канд. юрид. наук. Н. Новгород, 2007. С. 26 ; *Кукарникова Т. Э.* Электронный документ в уголовном процессе и криминалистике : дис. ... канд. юрид. наук. Воронеж, 2003. С. 96 ; *Яковлев А. Н.* Теоретические и методические основы экспертного исследования документов на машинных носителях информации : автореф. дис. ... канд. юрид. наук. Саратов, 2000. С. 20.

личия. Tor необходим для сокрытия личных данных и следов пребывания пользователя при работе в сети Интернет. Использование данного программного обеспечения свидетельствует об опытности пользователя и (или) его желании скрыть следы своей противоправной деятельности. С пользовательской точки зрения Tor представляет собой специальный браузер (на основе Mozilla Firefox).

При осмотре любого браузера необходимо проявлять осторожность: не закрывать открытые вкладки (это может привести к прекращению сеанса работы с сервисом, требующим ввода пароля), переход по гиперссылкам осуществлять в режиме «открыть на новой вкладке». Существенное значение может иметь информация, полученная при изучении истории просмотра веб-страниц и закладок в браузере. При этом особого внимания заслуживают:

1) социальные сети («ВКонтакте», «Facebook», «Одноклассники» и т.д.). Изучение переписки может указать на факт передачи или получения закрытых ключей кошелька криптовалюты с целью его дальнейшего распоряжения или же адреса криптовалюты для получения или отправки переводов. Также необходимо проверить, состоит ли подозреваемый (обвиняемый) в группах, посвященных криптовалютам;
2) информация с различных сайтов, которые посещал подозреваемый (обвиняемый), содержащая сведения о криптовалютах, способах деанонимизации (миксерах), использовании сети Tor;
3) иные электронные платежные системы. Изучая данные браузера, можно установить и электронные платежные системы, которыми пользовался подозреваемый (обвиняемый), помимо криптовалютных. Это могут быть платежные системы Qiwi, WebMoney, «Яндекс-деньги» и др. Они могут использоваться как посредники для обмена криптовалют на фиатные деньги и обратно.

Изучение электронной почты также может дать немало информации. Посредством нее возможно установить:

1) историю переписки, которая может содержать сведения о противоправной деятельности и преступных связях подозреваемого, а также контакты других лиц;
2) доступ к другим сетевым службам. Это позволит восстановить неизвестные правоохранительным органам пароли доступа к форумам, онлайн-кошелькам криптовалют, биржам, интернет-казино и иным сайтам, связанным с работой криптовалют. Работа с электронной почтой осуществляется либо через веб-страницу, либо через специальное приложение (Microsoft Outlook, TheBat!, Mozilla Thunderbird и т.д.).

В ходе осмотра необходимо исследовать и средства синхронизации данных или облачные хранилища. Помимо локального хранения файлов, все большее распространение получают средства синхронизации файлов на нескольких компьютерах и в сети (например, Dropbox, OneDrive, «Яндекс.Диск»), в которых могут быть сохранены файлы кошелька криптовалюты wallet.dat, удаленные из памяти компьютера, контакты и т.п. Эту возможность не следует недооценивать, так как синхронизация может производиться без команды пользователя, например, при синхронизации с ПК или при выходе в Интернет с мобильного телефона. Так, для осмотра облака Dropbox нужно убедиться, что соответствующая программа запущена (рядом с часами в правом нижнем углу экрана компьютера должен отображаться значок в виде открытой коробки), а на «ЯндексДиск» можно попасть, если введен пароль от электронной почты на сайте yandex.ru. Криминалистическое значение исследования средств синхронизации состоит в том, что могут быть получены данные, сохраненные с других устройств подозреваемого (смартфон, ноутбук, планшет) или удаленные им, но сохранившиеся в таком хранилище.

Используя в ходе осмотра программное обеспечение для восстановления недавно удаленной информации, можно получить значимую для расследования информацию. Существует специальное программное обеспечение, позволяющее восстановить удаленную информацию, например, R.saver, Recuva, RecoverMyFiles. В то же время существует программное обеспечение для необратимого удаления информации (CCleaner, DataShredder). Наличие на ПК такого

ПО следует рассматривать как характеризующую информацию (владелец ПК является опытным пользователем и возможно ему есть что скрывать).

При осмотре нужно минимизировать влияние на носители информации: не копировать на них новые файлы (особенно крупные), не запускать требовательные к объему памяти программы или программы для обслуживания носителей информации для исключения утраты возможности восстановления недавно удаленных файлов.

На заключительном этапе следственного осмотра при принятии решения об изъятии компьютера его целесообразно не выключать, а перевести в спящий режим, в этом случае сохраняется состояние всех запущенных приложений, а не только информация на жестком диске.

БИБЛИОГРАФИЯ

1. *Агибалов В. Ю.* Виртуальные следы в криминалистике и уголовном процессе. — М., 2012. — 152 с.
2. *Вехов В. Б.* Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники : учеб. -метод. пособие. — М., 2000. — 64 с.
3. *Зеленский В. Д.* Криминалистическая методика расследования отдельных видов и групп преступлений : учебное пособие. — Краснодар : КубГАУ, 2013. — 335 с.
4. *Костин Г. В.* Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики : автореф. дис. ... канд. юрид. наук. — Н. Новгород, 2007. — 30 с.
5. Криминалистика / под ред. Н. П. Яблокова. — М., 2005. — 781 с.
6. Криминалистика : учебник для вузов / под ред. Р. С. Белкина. — М., 1998. —990 с.
7. *Кукарникова Т. Э.* Электронный документ в уголовном процессе и криминалистике : дис. ... канд. юрид. наук. — Воронеж, 2003. — 204 с.
8. Руководство по расследованию преступлений : учебное пособие / рук. авт. колл. А. В. Гриненко. — М., 2002. — 768 с.
9. *Яковлев А. Н.* Теоретические и методические основы экспертного исследования документов на машинных носителях информации : автореф. дис. ... канд. юрид. наук. — Саратов, 2000. — 24 с.

Материал поступил в редакцию 8 сентября 2018 г.

SPECIFIC CHARACTER OF INVESTIGATORY EXAMINATION IN THE INVESTIGATION OF CRIMES COMMITTED INVOLVING CRYPTO CURRENCY

MARKARYAN Elvira Sergeevna — PhD candidate of the Department of Criminalistics of the Voronezh State University
seledkva@mail.ru
394018, Russia, Voronezh, Universitetskaya pl., d. 1

Abstract. *The article analyzes the features of the examination in the investigation of crimes committed using crypto currency. Objects of examination are identified, criminalistic recommendations are offered to improve the effectiveness of its results and measures to ensure the safety of the data obtained. It is noted that in cases of crimes committed using crypto currencies, the address of the individual or organization and the location of the used hardware and software can be considered the scene of the crime. Specificity of examination of objects and documents on crimes committed with the use of crypto currencies is that, as a rule, service logs of system and application programs, wallets used to carry out transactions, as well as wallet.dat or other files containing information about e-wallets are subject to examination. During the inspection, it is necessary to pay attention to*

the fact that the personal computer will be the most important source of forensic information due to the specific nature of the crimes committed.

Keywords: *crimes committed using crypto currency, investigatory examination, objects of examination, tactical techniques.*

REFERENCES (TRANSLITERATION)

1. *Agibalov V. Yu.* Virtual'nye sledy v kriminalistike i ugolovnom protsesse. — M., 2012. — 152 c.
2. *Vekhov V. B.* Osobennosti rassledovaniya prestupleniy, sovershaemykh s ispol'zovaniem sredstv elektronno-vychislitel'noy tekhniki : ucheb. -metod. posobie. — M., 2000. — 64 c.
3. *Zelenskiy V. D.* Kriminalisticheskaya metodika rassledovaniya otdel'nykh vidov i grupp prestupleniy : uchebnoe posobie. — Krasnodar : KubGAU, 2013. — 335 c.
4. *Kostin G. V.* Issledovanie mashinnykh nositeley informatsii, ispol'zuemykh pri sovershenii prestupleniy v sfere ekonomiki : avtoref. dis. ... kand. yurid. nauk. — N. Novgorod, 2007. — 30 c.
5. Kriminalistika / pod red. N. P. Yablokova. — M., 2005. — 781 c.
6. Kriminalistika : uchebnik dlya vuzov / pod red. R. S. Belkina. — M., 1998. —990 c.
7. *Kukarnikova T. E.* Elektronniy dokument v ugolovnom protsesse i kriminalistike : dis. ... kand. yurid. nauk. — Voronezh, 2003. — 204 c.
8. Rukovodstvo po rassledovaniyu prestupleniy : uchebnoe posobie / ruk. avt. koll. A. V. Grinenko. — M., 2002. — 768 c.
9. *Yakovlev A. N.* Teoreticheskie i metodicheskie osnovy ekspertnogo issledovaniya dokumentov na mashinnykh nositelyakh informatsii : avtoref. dis. ... kand. yurid. nauk. — Saratov, 2000. — 24 c.