2) некоторые следы уничтожаются при транспортировке;

3) обращается большое внимание на следы пальцев рук, гораздо меньше на следы обуви, наложения волокон на одежде подозреваемого.

Важно отметить, что каждое следственное действие преследует свои собственные цели и решает специфические для него задачи, которые, несомненно, связаны с общими задачами расследования.

Следует отметить, что в проведении осмотра места происшествия участвуют члены следственно-оперативной группы (СОГ), которые являются представителями соответствующих государственных правоохранительных структур, однако в части определения их статуса при проведении этого действия, по нашему мнению, есть проблема. Так, эксперт-криминалист при проведении осмотра места происшествия по сути исследований не проводит, а занимается поиском, фиксацией улик. Сотрудники органа дознания (оперуполномоченный уголовного розыска или участковый инспектор) также могут являться участниками и выполняют свои обязанности под руководством следователя, но в рамках своих полномочий.

В настоящее время в процессе осмотра места происшествия следователям приходится иметь дело с описаниями различных предметов, названия и назначение которых неочевидны, поэтому большинство исследователей избегают использования таких терминов, как «кровь» и «золото», поскольку невозможно делать выводы до проведения исследования и считать найденный объект таковым. По нашему мнению, при составлении протокола допустимо употреблять описание предметов: «пятна жидкости, похожие на кровь», «изделия из желтого металла, похожее на золото» и т. п.

Таким образом проблемы организационного, правового и тактического характера являются актуальными и требующими научной разработки.

Шандарович И. О., Кислицкая Н. А.

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОБЫСКА ПО ДЕЛАМ, СВЯЗАННЫМ С КРИПТОВАЛЮТАМИ

Шандарович Игорь Олегович, Кислицкая Надежда Александровна, студенты 4 курса Белорусского государственного университета, г. Минск, Беларусь, igor.shandarovich@yandex.by

Научный руководитель: канд. юрид. наук, доцент Хлус А. М.

В настоящее время цифровизация глубоко вошла в повседневную жизнь. Это отразилось и на общей картине преступности. Информационные технологии широко используются при совершении преступлений, создавая такие алгоритмы преступного поведения, которые не существовали еще 10 лет назад. Особым вниманием среди преступников пользуются криптовалюты в связи с их анонимностью. В ходе совершения преступлений, связанных с

криптовалютами, они могут являться как предметом преступления, так и средством его совершения.

Одним из основных моментов расследования преступлений, связанных с криптовалютами, является осмотр места происшествия и обыск жилища подозреваемого. Здесь можно найти и изъять носители данных, которые позволят выявить электронном-цифровые следы, логины и пароли от сайтов и приложений, позволяющих установить потенциальных свидетелей, потерпевших и соучастников.

Перед проведением обыска следует перевести все телефоны лиц, участвующих в следственном действии, в режим полета, а после входа в квартиру – всех лиц, находящихся в помещении. После этого следует изъять мобильные телефоны последних и запретить им доступ к компьютерной технике.

Как указывает следователь по особо важным делам главного следственного управления Следственного комитета Республики Беларусь Л. Л. Мельник, при проведении обыска по делу, связанному с криптовалютой, следует проверить рабочее состояние компьютерной техники. Если компьютерная техника выключена, ее включать не надо, так как ее запуск приведет к изменению данных на ней и может уничтожить доказательства. В случае, если компьютерная техника выключена, необходимо извлечь из нее кабель питания, при этом не следует его извлекать первоначально из розетки и подготовить таким образом ее к изъятию. Что касается действий следователя при обнаружении ноутбука, то необходимо достать из него батарею. В некоторых устройствах есть дополнительные батареи, которые находятся в многофункциональном отсеке на месте оптического дисковода, их также следует извлекать. Операционные системы WindowsServer, Unix, Linux, macOS, по возможности необходимо выключить с помощью специальной команды «shutdown»;

При обнаружении мобильного телефона необходимо зафиксировать IMEI-номера устройства (его можно найти на коробке из-под телефона), не следует включать его, если он выключен. Если обнаружены мобильные телефоны, которыми лица, у которых проводится обыск, не пользуются непосредственно, то их также следует перевести в режим полета и переписать IMEI-номера. Не исключено, что такие «холодные» телефоны использовались злоумышленниками для принятия-отправки СМС с кодами подтверждения при проведении транзакций или для переписки в мессенджерах со сторонних аккаунтов. При обнаружении извлеченных SIM-карт следует переписать их серийный номер. Аналогичные действия необходимо провести с картами памяти (если таковые имеются).

Далее следует изъять всю компьютерную технику, находящуюся в помещении: мобильные телефоны, планшеты, ноутбуки, стационарные компьютеры и т. д. В случае изъятия стационарного компьютера следует изымать весь системный блок, а не только жесткий диск, так как некоторые программы и приложения могут быть привязаны непосредственно к «железу» и

со сторонней системы не получится войти в аккаунты подозреваемого даже имея логины и пароли.

Таким образом, проведение обыска по делам, связанным с криптовалютами, имеет свои особенности. Указанные выше действия, способствуют сохранению электронно-цифровых следов и доказательств, которые могут быть уничтожены, способствуют выявлению преступлений и привлечению виновных к уголовной ответственности.

Шнейдерова Д. И.

СЕРВИСЫ-АНОНИМАЙЗЕРЫ КАК СРЕДСТВА СОКРЫТИЯ ЛИЧНОСТИ ПРЕСТУПНИКА ПО ДЕЛАМ О ХИЩЕНИЯХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

Шнейдерова Дарья Игоревна, аспирант Белорусского государственного университета, г. Минск, Беларусь, galuzodi@mail.ru

Научный руководитель: канд. юрид. наук, доцент Асаёнок Б. В.

Практическая невозможность установления личности преступника по уголовным делам о хищениях в сфере оборота криптовалют – ключевая проблема, образующая низкий процент раскрываемости указанной категории преступлений, которая вызвана использованием киберпреступниками специализированных сервисов, позволяющих осуществлять противоправную деятельность через сеть Интернет анонимно для сторонних пользователей и правоохранительных органов, т. е. с сокрытием реального IP-адреса используемого в этих целях устройства. Среди таких сервисов можно выделить механизмы маршрутизации NAT и DHCP, VPN-сервер, прокси-сервер SOCKS и TOR-маршрутизатор.

Технологии NAT и DHCP, применяемые крупными интернет-провайдерами, позволяют скрывать фактическое количество IP-адресов устройств, выходящих в сеть, тем самым образуя диссонанс между реальным количеством пользователей и адресами тех устройств, которые доступны для анализа трафика сети. Так, технология NAT присваивает один и тот же внешний IP-адрес нескольким устройствам, выходящим в интернет, при этом сохраняя внутренние IP-адреса в специальной переводной таблице с целью последующего обеспечения правильной маршрутизации ответного входящего пакета данных. Технология DHCP действует в противоположном порядке – присваивает одному внутреннему IP-адресу несколько краткосрочных внешних адресов, что позволяет считать активность одного лица в сети как деятельность разных пользователей.

VPN выступает разновидностью частной виртуальной сети, позволяющей своим клиентам выходить в интернет не под адресом своего устройства, а под IP сервера VPN, шифруя при этом трафик подключения пользователя к VPN-сервису и лишая провайдера возможности анализа активности пользователя в