ково-познавательной деятельности следователя и эксперта позволит наделить субъектов доказывания возможностью реального оперирования научно-практическим аппаратом и методологическим ресурсом судебной экспертологии в целях повышения эффективности расследования преступлений.

ИННОВАЦИОННЫЕ АСПЕКТЫ ОБНАРУЖЕНИЯ СЛЕДОВ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

С. В. Рыбак, Д. А. Романюк

УО ФПБ «Международный университет “МИТСО”»,
ул. Казинца, 21, к. 3, 220099, г. Минск, Беларусь, *di.rom@mail.ru*

Рассматриваются особенности обнаружения следов преступлений, совершаемых использованием криптовалюты. Определяется важность познавательной деятельности на первоначальном этапе, которая позволяет повысить эффективность работы по обнаружению и фиксации специфических следов.

Ключевые слова: криминалистическая наука; цифровая криминалистика; виртуальный след; криптовалюта; биткоин.

В связи с проникновением во все сферы жизнедеятельности информационных технологий в последние годы активно развиваются новые способы совершения преступлений. Такие слова, как «кардинг», «кардшаринг», «скимминг», «фишинг», «кэш-треппинг» прочно вошли в сферу профессиональной лексики правоохранительных органов. Модернизируются способы совершения «традиционных» преступлений, при которых преступники применяют различные технические новинки. Одно из направлений преобразования технических достижений в преступный инструмент связано с появлением технологии «блокчейн», а также «криптовалют».

В соответствии с п. 4 Декрета Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики» криптовалюта – это «биткоин, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена».

Представляется возможным выделить следующие направления использования криптовалют при совершении преступлений:

– как средство платежа за запрещенные или ограниченные в гражданском обороте вещества и предметы, а также инфраструктуру и услуги, которые используются в преступной деятельности;

– при легализации преступных доходов;

– как инструмент совершения мошенничеств в сети Интернет;

– как финансовый инструмент для получения платежа при использовании вредоносного программного обеспечения от жертвы или без использования такового;

– как объект хищения с использованием вредоносного программного обеспечения или без него у физических и юридических лиц;

– в майнинговых бот-сетях на чужих вычислительных мощностях.

Последовательность действий следователя на первоначальном этапе расследования по обнаружению и фиксации следов преступлений, совершенных с использованием криптовалют, зависит от складывающейся следственной ситуации, определяемой конкретным из вышеупомянутых направлений преступной деятельности и специфическим способом использования криптовалюты при совершении преступления.

Остановимся на отдельных специфических аспектах деятельности по обнаружению и фиксации следов и успешного расследования рассматриваемой категории преступлений.

– изучение первоначально поступившей информации о преступлении, совершенном с использованием криптовалют, от НЦБ «Интерпол», уполномоченных учреждений юстиции иностранных государств, юридических и физических лиц. На данном этапе особое внимание необходимо уделить установлению сведений, идентифицирующих предполагаемого преступника, его потенциальных сообщников, в том числе идентификатора криптокошельков, логинов учетных записей на криптобиржах, USER-агентов (пользователей) использованных Интернет-браузеров, IP-адресов, электронных почтовых ящиков и иной значимой информации;

– в случае предоставления использованного при совершении преступления программного обеспечения (далее – ПО), необходимо назначить компьютерно-техническую экспертизу для установления механизма совершенного преступления и возможного факта использования вредоносного ПО при его совершении. Выводы эксперта позволят правильно квалифицировать преступление при принятии решения о возбуждении уголовного дела;

– истребование и осмотр у Интернет-провайдера информации, связанной с посещаемыми подозреваемым Интернет-ресурсами. В ходе осмотра полученных сведений следует зафиксировать IP-адреса и располагающиеся на них Интернет-ресурсы, которые использовались в предполагаемой преступной деятельности. При использовании анонимных IP-адресов, скрывающих реальный IP-адрес злоумышленника, целесообразно направить требование Интернет-провайдеру на установление абонентов (лиц) с реальными IP-адресами, посещающих Интернет-ресурсы анонимайзеров для сокрытия действительного IP-адреса;

– направление поручений в орган дознания на проведение оперативно-розыскных мероприятий (далее – ОРМ), с целью фиксации противоправной деятельности лица, предположительно причастного к совершению преступления с использованием криптовалют. При установлении абонентских номеров телефонов данного лица следует провести ОРМ, направленные на фиксацию его телефонных переговоров и используемого Интернет-трафика. Проведение данных ОРМ позволяет установить факт использования криптовалют в первую очередь посредством осмотра СМС-уведомлений о фактах входа в интересуемые криптокошельки при двух-трех факторной аутентификации. Данная информация в последующем используется при осмотре и сопоставлении с иными имеющимися по уголовному делу данными использования криптовалют, с целью привязки использования криптокошельков к конкретному лицу в определенное время. Также указанные ОРМ предоставляют возможность установить посещаемые злоумышленником Интернет-ресурсы, в том числе используемые в преступной деятельности учетные записи на криптобиржах, а также получить реквизиты доступа к данным учетным записям, что позволяет в дальнейшем осуществить их осмотр;

– при использовании IP-адресов, скрывающих реальный IP-адрес злоумышленника, необходимо направить требование Интернет-провайдеру об установлении абонентов (лиц), использующих реальные IP-адреса для посещения Интернет-ресурсов анонимайзеров с целью использования IP-адресов, скрывающих реальный IP-адрес;

– проведение осмотров в сети Интернет с использованием различных Интернет-браузеров, в том числе по используемым злоумышленником биткоин-кошелькам, логинам учетных записей, например, на таких Интернет-ресурсах как bitcointalk.org (крупнейший форум, посвященный использованию криптовалюты «Bitcoin»), blockchain.com (блокейн-обозреватель), walletexplorer.com (позволяет идентифицировать принадлежность биткоин-кошельков конкретным компаниям);

– обыск целесообразно проводить одновременно с ОРМ, направленным на фиксацию активности интересуемого лица в сети Интернет. При этом фиксируется факт включения компьютера злоумышленника и подключения к сети Интернет в момент начала производства обыска. Сопряжение обыска и ОРМ необходимо для последующего получения доступа к учетным записям лица, у которого производится обыск, в том числе на ресурсах сети Интернет, а также к сведениям, хранящимся в компьютере и подключенных к нему удаленных устройствах (виртуальные машины, удаленные сервера). В противном случае, при выключенном компьютере и использовании криптования (шифрования) храня-

щихся в нем данных высока вероятность неполучения необходимых сведений для дальнейшего расследования.

Таким образом, при расследовании преступлений, совершенных с использованием криптовалют, последовательность и конкретный перечень следственных и процессуальных действий, ОРМ, зависят от конкретной следственной ситуации. Знание и использование изложенных особенностей познавательной деятельности на первоначальном этапе позволяет повысить эффективность работы по обнаружению и фиксации специфических следов, что определяет перспективы всего процесса расследования.

НЕКОТОРЫЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ

К. А. Сайед

ИДН Новополоцкого ГОВД, ул. Дзержинского, 2, 211440, г. Новополоцк, Беларусь, *kristy_0515@mail.ru*

Рассматриваются некоторые особенности расследования мошенничества с учетом теоретико-правовых взглядов на проблему борьбы с мошенничеством в сети Интернет и современной правоприменительной практики.

Ключевые слова: криминалистика; криминалистическая методика; расследование мошенничества; цифровая криминалистика.

Общество – динамически развивающаяся социальная структура, постоянно претерпевающая изменения в связи с рядом факторов, в том числе таких, как рост или падение экономики, наличие кредитно-банковских или страховых отношений, развитие и внедрение компьютерных технологий в повседневную жизнь. Однако, наряду с развитием общества, развивается и преступность, как неотъемлемая его часть. В настоящее время преступления в виде мошенничества получили большое распространение. Данное преступление превратилось для некоторых граждан из несущественного дополнительного в основной источник дохода [1, с. 15].

Для сравнения можно привести данные о том, что в Российской империи за 20 лет дореформенного периода (1827–1846) было осуждено и сослано в Сибирь за воровство и мошенничество 40 660 человек. В 1918 г. процент осужденных за мошенничество составил 5,0 %, в 1925 г. уже 5,7 % [2, с. 98]. В 2011 г. зарегистрировано мошенничеств 3106 (раскрыто 83,3 %); 2012 г. – 2131 (раскрыто 87,6 %); 2013 г. – 2789 (раскрыто 87,5 %); 2014 г. – 3224 (раскрыто 84,7 %); 2015 г. – 2831 (раскрыто 86,2 %); 2016 г. – 3748 (раскрыто 88,3 %); 2017 г. – 3204 (раскры-