Вопросами обнаружения, фиксации, изъятия, исследования и использования компьютерной информации (цифровых следов) при расследовании преступлений занимались такие ученые-криминалисты, как В.А. Мещеряков, А.Г. Волеводз, В.Е. Козлов, А.Ю. Семенов, Л.Б. Краснова, В.П. Леонтьев, А.Б. Смушкин, В.Б. Вехов, А.Н. Колычева.

При производстве дознания по уголовным делам против пограничной безопасности, где фигурируют цифровые следы, сложность объясняется специфичностью и новизной рассматриваемых доказательств, многообразием способов криминальных посягательств, сложностью сбора и закрепления доказательной базы, мощным противодействием со стороны преступников, что создает для сотрудников органов пограничной службы Республики Беларусь существенные преграды в защите прав граждан, интересов общества и государства от противоправных действий.

Актуальность исследования обусловлена тем, что в научной литературе отсутствует формулировка понятия «цифровые следы», методологические основы их изучения и использования в науке криминалистике и следственной практике, а также классификация. За последнее время было защищено несколько докторских и кандидатских диссертаций, в которых основное внимание было уделено проблемам расследования и предупреждения преступлений в сфере компьютерной информации. В науке существует множество подходов к классификации цифровых следов, которые предложены учеными-криминалистами, а также формировались параллельно с исследованием теоретических основ и сущности цифровых следов. Исходя из проведенного анализа понятийного аппарата и с учетом мнения авторов, исследовавших следовые картины в сфере компьютерной информации, считаем допустимым предложить следующее понятие цифрового следа.

Цифровой след – это данные о совершении действий в информационном пространстве технических устройств, их сетей и систем, такие как создание, включение, удаление, внесение изменений, активация, открывание.

С цифровыми следами с помощью технических средств производится такое преобразование информации, находящейся на материальном носителе, при котором человек сможет ее воспринять визуально, аудиально или иным способом. Поэтому, несмотря на то, что компьютерная информация не имеет физических параметров, присущих материальным объектам, она обладает определенными фиксированными характеристиками, существенно отличающими ее от идеальных следов, таких как объем (размер), формат (вид информации), сведения о местонахождении (реквизиты размещения на носителе), время (создания, модификации, использования, уничтожения) и т. п., а также рядом иных свойств, таких как объективность, достоверность, полнота, точность, актуальность, полезность и т. д. Исходя из вышеперечисленного, можно сделать вывод о том, что цифровые следы не относятся к материальным и идеальным следам, а представляют из себя совершенно новый вид следов преступления в криминалистике.

Изложенное позволяет сделать следующие выводы.

1. Научное сообщество не пришло к единому пониманию следов, образующихся в результате взаимодействия информационно-телекоммуникационных объектов компьютерной техники посредством электромагнитных сигналов, и придерживается полярных мнений как на понятие следа, его природы, так и на их классификации.

2. Самым лаконичным и емким обозначением рассмотренного вида следов является понятие «цифровой след», который: несет в себе криминалистически значимую информацию; фиксируется посредством электромагнитных взаимодействий или сигналов; имеет форму, пригодную для обработки с использованием компьютерной техники; содержится на материальном носителе в результате создания определенного набора двоичного машинного кода либо его преобразования и не может существовать без материального носителя; выражается в модификации, копировании, удалении или блокировании.

3. Цифровые следы имеют материальную природу, поскольку по своей сути сходны с многими невидимыми материальными следами, возникают в результате взаимодействия электромагнитных и цифровых сигналов, обладающих физическими параметрами, с материальными свойствами объектов (время, частота, направленность, напряжение) и отражаются в преобразованной (воспринимаемой) форме на материальном носителе.

4. Таким образом, цифровыми следами преступления являются файлы системного и прикладного программного обеспечения, конфигурационные файлы, файлы-журналы, файлы, источники информации, образующиеся в ходе деятельности пользователя; файлы, обеспечивающие аутентификацию и конфиденциальность пользователей, информация, полученная с помощью соответствующих радиоэлектронных или специальных технических средств.

УДК 343.985.8

А.М. Шинкевич

ПРЕСТУПНОСТЬ В СФЕРЕ КРИПТОВАЛЮТЫ: АНАЛИЗ И ПЕРСПЕКТИВЫ

В последние годы цифровые деньги (криптовалюты) стали важной частью мировой экономики. С ростом их популярности появились новые способы совершения и сокрытия преступлений. За фиатные денежные средства, добытые преступным путем, как правило, приобретается криптовалюта. Это повышает уровень сохранности преступных активов и снижает возможность их «замораживания» правоохранительными органами.

Изучение научных трудов показало, что все преступления, сопряженные с использованием криптовалюты, условно можно разделить на три группы: преступления, в которых криптовалюта выступает предметом преступного посягательства; преступления, в которых криптовалюта является средством совершения преступлений; преступления, совершаемые в целях майнинга криптовалюты.

Преступления, в которых криптовалюта выступала предметом преступного посягательства, как правило, сопряжены с обманом, введением в заблуждение ее владельцев либо с неправомерным доступом к охраняемой компьютерной информа-

ции – криптокошелькам, личным кабинетам криптобирж и криптообменников. Мошенники, действуя анонимно в сети Интернет, создают поддельные страницы сайтов криптобирж и криптообменников для торговли или обмена криптовалюты, фальшивые версии официальных криптокошельков, размещая их в Google Play и Apple App Store, распространяют вредоносное программное обеспечение, которое шифрует файлы пользователя и требует выкуп в криптовалюте за их восстановление. Мошенники выдают себя за брокеров, обещая высокую доходность от торговли криптовалютой, забирают деньги своих клиентов. Все эти действия осуществляются анонимно с использованием специального программного обеспечения, позволяющего скрывать местонахождение мошенника. Однако преступные посягательства на цифровые активы могут осуществляться и открыто. Например, путем совершения грабежа, разбоя или вымогательства.

Преступления, в которых криптовалюта являлась средством совершения преступлений, как правило, связаны с торговлей запрещенными товарами, работами или услугами, взяточничеством, мошенничеством в сети Интернет. Прежде всего это преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ, порнографических материалов, оружия и боеприпасов. Через сеть Интернет в обмен на криптовалюту преступники оказывают услуги по изготовлению поддельных денежных знаков, документов (паспорта, водительские удостоверения), продают программное обеспечение для «взлома» устройств, имеющих доступ в сеть Интернет, персональные данные физических и юридических лиц, банковские платежные карточки и электронные кошельки, оформленные на подставных лиц – дропов. Такие сделки, как правило, осуществляются в криптовалюте с использованием тайников – закладок. В Республике Беларусь появились факты взяточничества, финансирования экстремизма и терроризма с использованием криптовалюты. Незаконные сделки в криптовалюте позволяют уклоняться от уплаты налогов, легализовывать денежные средства, полученные преступным путем.

Особого внимания заслуживают схемы мошенничества в сети Интернет через криптовалютное финансирование ICO (Initial Coin Offering). Мошенники рекламируют фальшивые проекты по выпуску и продаже новых токенов и в обмен на них анонимно собирают средства (фиатные или криптовалюту) от инвесторов, обещая в ближайшем будущем высокую доходность. Фальшивые проекты представляют собой информацию, размещенную на специально созданных сайтах, в мессенджерах и социальных сетях о возможности стать инвестором высокодоходного проекта, выпускающего новые токены, стоимость которых будет расти. По статистике, менее половины всех ICO продолжают существовать через четыре месяца после самого размещения монет. Распознать мошеннические проекты рядовому пользователю сети Интернет весьма проблематично. Южная Корея и Китай на законодательном уровне запретила ICO. В Республике Беларусь ICO разрешены для резидентов Парка высоких технологий.

Аналогичные «пирамиды» реализуются мошенниками через специально созданные сайты, предлагающие услуги облачного майнинга, участия в инвестиционных фондах, вымышленных аукционах и лотереях. Активно рекламируются боты для автоматической торговли криптовалютой, которые на самом деле похищают средства и (или) личную информацию пользователей.

Отдельного внимания заслуживают преступления, совершаемые в целях майнинга криптовалюты. В основном они связаны с распространением и скрытой установкой специальных программ, предназначенных для майнинга криптовалюты за счет аппаратных мощностей устройств пользователей сети Интернет. Ввиду того что майнинг является весьма энергозатратным, имеют место факты хищения электрической энергии майнерами.

Таким образом, преступность в сфере криптовалюты – сложная и многоаспектная проблема для большинства стран мира. По мере развития криптоиндустрии в Республике Беларусь эта проблема будет возрастать. Необходимо проводить дальнейшие исследования и разрабатывать новые методы борьбы с преступностью в этой сфере. Ключевым фактором успеха является сотрудничество и взаимодействие между правительствами, правоохранительными органами, банковскими финансовыми организациями внутри страны и за рубежом.

УДК 351.74 + 004

А.А. Шульченко

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ OSINT В СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ

Цифровизация становится неотъемлемым элементом деятельности любого человека. Повсеместно социальные и политические процессы, а также деятельность государственных органов перемещаются в цифровую среду и для того, чтобы успешно адаптироваться в обществе, люди создают различные цифровые профили на различных порталах, ведут страницы в социальных сетях, выкладывая при этом фотографии и иную информацию о себе. В современном информационном обществе, где совершение преступлений в виртуальном пространстве становится все более распространенным, органам внутренних дел (ОВД) необходимо активно использовать разные методы по установлению правонарушителей, в том числе эффективно могут применяться методы открытого исследования информации (OSINT).

Справочно: OSINT, или открытое исследование информации. Этот метод предоставляет возможность собирать и анализировать данные из различных открытых источников, таких как интернет, социальные сети, новостные статьи, форумы и другие общедоступные ресурсы.

Значительный рост киберпреступности подчеркивает важность эффективного мониторинга и анализа данных, доступных в сети Интернет. OSINT предоставляет сотрудникам возможность получать ценную информацию из открытых источников, таких как социальные медиа, форумы и другие онлайн-ресурсы. Это способствует не только выявлению и раскрытию преступлений, совершенных в сети Интернет, но и преступлений, совершенных по линии иных подразделений ОВД. Качественный OSINT также обеспечивает возможность оперативного реагирования на угрозы, связанные с виртуальной безопасностью.