К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

При нарушении организационных средств защиты информации преступники чаще всего, используя служебное положение и имеющиеся у них идентификаторы доступа, осуществляют доступ к конфиденциальной компьютерной информации, либо к машинным носителям информации, после чего копируют, изменяют, либо похищают конфиденциальные сведения целиком, либо идентификационные данные для доступа к таким сведениям.

К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации. Анализ сведений ИЦ МВД Республики Беларусь[1] показывает, что большинство НДКИ преступники совершают, нарушая технические средства защиты информации. Таким образом, классифицируем способы совершения НДКИ как организационные и технические.

НДКИ, сопряженный с нарушением технических мер по защите компьютерной информации, чаще всего преступниками реализовывается посредством социальной инженерии, когда необходимые идентификаторы для доступа в закрытые сети передачи информации, либо к персональным страницам в социальных сетях, они получают непосредственно у потерпевших, путем применения психологических приемов воздействия.

Вторым, не менее распространенным способом совершения НДКИ является использование специально созданного программного обеспечения по подбору паролей для несанкционированного доступа к информационному ресурсу. Программный продукт для подбора паролей имеет определенный алгоритм действия, не сложен в изготовлении при наличии соответствующих навыков. Это программы, способные из заданного пользователем диапазона символов подобрать в максимально короткие сроки пароль доступа к сведениям ограниченного доступа, или сети, где такие сведения циркулируют. Такая технология взлома системы защиты получила название «Брутфорс» (от англ. brute force – грубая сила), когда преступник получает доступ к информации ограниченного доступа или закрытую сеть, путем подбора идентификаторов. При этом установленные программные средства защиты информации не фиксируют НДКИ, так как доступ осуществляется с использованием зарегистрированных в системе идентификаторов.

Встречаются и менее распространенные способы совершения НДКИ, носящие «бытовой» характер. Эти способы представляют собой несанкционированный доступ к личному кабинету пользователя услуги, например, интернет-банкинга, когда его владельцы пренебрегают правилами хранения и использования сеансовых ключей доступа (идентификаторов учетной записи), передавая их третьим лицам.

Таким образом, следует, что НДКИ преимущественно совершается тремя, наиболее распространенными способами: путем использования специального программного средства по подбору идентификаторов по технологии «Брутфорс»; посредством применения приемов социальной инженерии; злоупотреблением доверием владельцев идентификаторов доступа в личные кабинеты информационных систем. Их общей особенностью выступает стремление преступника завладеть идентификационными данными для несанкционированного доступа к компьютерной информации с целью получения материальной и иной выгоды.

УДК 343.9

А.И. Чурносов

ЦИФРОВЫЕ СЛЕДЫ КАК ИСТОЧНИК ПОЛУЧЕНИЯ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ И ОПЕРАТИВНО-РОЗЫСКНОЙ ИНФОРМАЦИИ НА ПРИМЕРЕ ОРГАНОВ ПОГРАНИЧНОЙ СЛУЖБЫ РЕСПУБЛИКИ БЕЛАРУСЬ

В XXI в. произошло преобразование общественной жизни, и в первую очередь это связано с научно-техническим прогрессом. Были созданы объективные условия для роста количества преступлений против информационной безопасности, что является негативной тенденцией, присущей любому современному обществу. Бурное развитие компьютерных технологий и повышение их роли в современной жизни человечества закономерно повлекло к внедрению компьютерных систем практически во все сферы деятельности человека. Такие тенденции, как появление компьютерной техники с огромными производительными возможностями, широкая функциональность ее применения, предопределяют компьютеризацию управленческой и экономической сфер жизни общества и необходимость более тщательного подхода к обеспечению безопасного функционирования компьютерных систем.

На современном этапе для лиц, производящих дознание в органах пограничной службы Республики Беларусь, все более актуальным становится исследование и изъятие цифровых следов при расследовании преступлений, создающих угрозу пограничной безопасности, в первую очередь по уголовным делам, возбуждаемым по признакам преступлений, связанным с организацией незаконной миграции, ст. 371[1] (в 2021 г. органами дознания возбуждено 16 уголовных дел в отношении 17 лиц, а в 2022 г. – 35 уголовных дел в отношении 66 лиц); незаконным перемещением через таможенную границу Евразийского экономического союза и (или) Государственную границу Республики Беларусь наркотических средств, психотропных веществ либо их прекурсоров или аналогов – ст. 328[1] (в 2021 г. органами дознания возбуждено 9 уголовных дел в отношении 7 лиц, а в 2022 г. – 11 уголовных дел в отношении 11 лиц) Уголовного кодекса Республики Беларусь.

[1] Здесь и далее сведения информационного центра Министерства внутренних дел Республики Беларусь за 2017–2022 гг. о зарегистрированных на территории республики преступлениях, предусмотренных ст. 349 Уголовного кодекса Республики Беларусь.

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-