ЮРИДИЧЕСКИЕ НАУКИ

УДК 343.8 **DOI 10.52928/2070-1632-2021-59-14-91-97**

ПРЕСТУПЛЕНИЯ, СОПРЯЖЕННЫЕ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ: СПОСОБЫ СОВЕРШЕНИЯ И СЛЕДОВАЯ ИНФОРМАЦИЯ

канд. юрид. наук, доц. П.Л. БОРОВИК
(Академия Министерства внутренних дел Республики Беларусь, Минск)

Представлены результаты криминалистического анализа типичных способов совершения преступлений, сопряженных с использованием средств электронных платежей. Показано, что в основе этой преступной деятельности лежат методы социальной инженерии, основанные на применении достижений современных информационно-коммуникационных технологий, а также на действиях и подходах, посредством которых правонарушители получают неправомерный доступ к персональным данным потерпевшего. С учетом изучения этапов механизма рассматриваемых уголовно-наказуемых деяний сформулированы источники следовой информации, отражающие процессы взаимодействия участников криминального события между собой и с окружающей средой.

Ключевые слова: *мошенничество, средства электронного платежа, противодействие преступности, обман, способ преступления, следовая информация.*

Введение. Современное состояние товарно-денежных отношений характеризуется существенным увеличением доли безналичного денежного оборота в общем объеме финансовых транзакций. Это связано с активным использованием средств электронных платежей[1] (далее – СЭП), к которым относится широкий перечень инструментов оплаты товаров и услуг, а также денежных переводов: платежные карты, мобильные устройства и персональные компьютеры с доступом к банковским счетам и аккаунтам, электронные платежные системы, системы дистанционного банковского обслуживания «Клиент-банк» (далее – ДБО).

По мере роста количества и сумм безналичных операций возросло и количество противоправных деяний в отношении владельцев денежных средств. Так, за 12 месяцев 2020 г. в сравнении с аналогичным периодом прошлого года в Республике Беларусь отмечен значительный рост количества преступлений, связанных с получением неправомерного доступа к чужим денежным средствам. Особую общественную опасность представляют мошеннические действия, отличающиеся от других имущественных преступлений (например, кражи) тем, что потерпевший добровольно либо неосознанно отдает свое имущество преступнику вследствие обмана или злоупотребления доверием, которые вводят жертву в заблуждение. Используя методы социальной инженерии, основанные на достижениях современных информационных технологий, мошенники выманивают у пользователей необходимые для осуществления незаконных платежей или переводов реквизиты (например, пароли защищенного протокола авторизации «3-D Secure»), либо осуществляют несанкционированный доступ к пользовательской информации, позволяющие выполнить авторизацию и последующее хищение денежных средств со счетов пользователей.

Результаты исследования научной литературы, посвященной вопросам совершенствования деятельности органов уголовного преследования, а также изучения соответствующих уголовных дел по данному направлению позволили выявить ряд нерешенных проблем, в основе которых лежит несоответствие устоявшихся теоретико-прикладных подходов к криминалистическому обеспечению противодействия данным криминальным деяниям современным потребностям правоприменительной практики.

Отдельные вопросы рассматриваемой проблематики затрагивались в работах Р.Н. Боровского, Г.Н. Доронина, Л.М. Прозументова, А.В. Шеслера, А.И. Долгова, В.Н. Кудрявцева, Л.В. Лямина, В.Е. Эминова, С.Л. Алексеева, Я.И. Гилинского, Б.Э. Шавалеева (2013 – 2020 гг.) и др. Представляя собой «срез» текущего положения дел в части, касающейся отдельных криминалистических аспектов противодействия преступности данного вида, исследования указанных авторов не претендуют на окончательность и однозначность содержащихся в них теоретических положений, выводов и практических рекомендаций. Несмотря на их высокую научную и прикладную значимость, современные подходы к противодействию указанным преступлениям остались за рамками проведенных научных дискуссий.

Разнообразие современных способов мошенничества с использованием СЭП диктует необходимость их комплексного изучения с целью выработки научно-обоснованных рекомендаций по противодействию им. При этом, в контексте растущей общественной опасности данных уголовно-наказуемых деяний особую важность приобретает необходимость научного осмысления типичных способов совершения таких преступлений, а также соответствую-

[1] Здесь и далее под электронным средством платежа понимается средство и/или способ, которые позволяют клиенту оператора по переводу денежных средств составлять/удостоверять/передавать распоряжения для перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации (в том числе платежных карт), а также других технических устройств.

щей следовой информации. Представляется, что их знание позволит практическому сотруднику более качественно оценить информацию об обстоятельствах деяния в конкретных следственных ситуациях и принять верное тактическое и уголовно-процессуальное решение в условиях недостаточной информационной определенности.

Все это обосновывает актуальность обозначенной темы и предопределяют задачи исследования.

Основная часть. Одним из ключевых источников информации о преступном поведении лица, совершившего общественно опасное деяние, является способ преступления – совокупность используемых при его совершении приёмов и методов, последовательность совершаемых преступных действий, применения средств воздействия на предмет посягательства. Способ указывает, какие именно действия произведены, выражает субъективные компоненты личности преступника, форму его вины, мотив и цели, характер применяемых орудий и средств [1, с. 10]. Таким образом, криминалистическая сущность способов преступления и практическая значимость их изучения заключается в выявлении закономерностей будущих доказательств, необходимых для качественного расследования противоправных деяний.

Среди наиболее распространенных способов совершения преступлений указанного вида особой популярностью у правонарушителей пользуется *фишинг* (69,41% от общего числа изученных уголовных дел). Термин образован от английского словосочетания «password fishing» («выуживание паролей») и в классической интерпретации означает введение пользователя в заблуждение при помощи поддельного сайта, визуально имитирующего сайт банка или иной интернет-системы, предполагающей идентификацию пользователя[2]. Главная задача мошенника – заманить пользователя на этот сайт и убедить его сообщить идентификационные либо иные персональные данные. Для этого злоумышленники используют следующие приемы и методы:

1) *рассылка спама* (недобросовестная реклама товаров, которые можно приобрести в интернет-магазине, причем в рекламе обязательно приводится ссылка на сайт магазина-однодневки либо поддельный сайт, визуально неотличимый от настоящего). Осуществляется с помощью СМС-сообщений, электронной почты, рекламных баннеров на веб-сайтах, новостных лент, популярных интернет-мессенджеров (WhatsApp, Viber, Telegram, Facebook), коммуникативно-развлекательных мобильных приложений (Snapchat, TikTok) и социальных сетей (Instagram, «ВКонтакте», Twitter, Tinder и др.).

Особую значимость рассматриваемый метод приобрел с распространением онлайн-сервиса «Bit.ly» (https://bitly.com), предназначенного для создания сокращенных URL. Данный сервис сокращает ссылку, превращая её фактически в семь символов, следующих за приставкой-названием самого сервиса, например: *bit.ly/2ByeRZX*. Суть такого сокращения – сделать ссылку более компактной для рассылки, а следовательно – более кликабельной.

2) *использование вредоносных программ класса «Троян»* (например, Trojan.Win32.DNSChanger), проникающих в компьютер пользователя под видом легитимного программного обеспечения (в данную категорию обычно входят программы, выполняющие различные неподтверждённые пользователем действия: сбор информации о банковских картах и передача этой информации злоумышленнику, использование ресурсов компьютера в целях майнинга, нелегальной торговли и др.).

Упрощенной формой реализации данного метода является несанкционированная модификация файла Hosts (текстовый файл, содержащий базу данных доменных имен и используемый при их трансляции в сетевые адреса узлов; запрос к этому файлу имеет приоритет перед обращением к DNS-серверам). Более сложные методы основаны на применении вредоносных программ класса «Руткит» (от англ. rootkit, то есть «набор root-а»), обеспечивающих маскировку объектов (процессов, файлов, каталогов, драйверов), управление событиями, происходящими в системе и сбор данных – параметров системы.

Специфика указанных методов заключается в том, что вредоносный код может использовать авторизацию пользователя в системе для получения к ней расширенного доступа или получения его авторизационных данных. Кроме того, вредоносный код может быть внедрен в страницу как через уязвимость на веб-сервере, так и на компьютере пользователя[3].

Разновидностью фишинга является преднамеренное введение пользователя в заблуждение посредством использования *программного обеспечения класса Hoax*[4] (в переводе с англ. означает «обман») с целью получения финансовой выгоды (2,08% от общего количества преступлений типа «фишинг»). Такие программы значительно преувеличивают эффект имеющихся проблем либо вовсе выдают на экран информацию о несуществующих ошибках в работе компьютера, вынуждая пользователя заплатить деньги за подобный функционал, чтобы избавить компьютер от якобы обнаруженных ими угроз. При этом, подобные программы чаще всего именно вынуждают, а не предлагают себя приобрести, объявляя пользователю, что без оплаты проблему не решить.

Следующим, не менее актуальным способом совершения преступления, сопряженного с использованием СЭП, является *фарминг* (от англ. pharming – скрытное перенаправление на ложный IP-адрес) (18,24% от общего ко-

---

[2] Зайцев, О. Мошенничество в Интернете и защита от него [Электронный ресурс] / О. Зайцев // КомпьютерПресс. URL: https://compress.ru/ article.aspx?id=18184.

[3] Дудников, Е.А. Анализ существующих целей сетевых атак и способов атак на web-сервисы [Электронный ресурс] / Е.А. Дудников. URL: https://cyberleninka.ru/article/n/analiz-suschestvuyuschih-tseley-setevyh-atak-i- sposobov-atak-na-web-servisy.

[4] Антивирусное программное обеспечение «Лаборатории Касперского» к подобным программам относит следующие: HEUR:Hoax.Win32.Uniblue.gen, Hoax.Win32.PCFixer.gen, Hoax.Win32.DeceptPCClean.*, Hoax. Win32.PCRepair.*, HEUR:Hoax.Win32.PCRepair.gen, HEUR:Hoax.MSIL.Optimizer.gen, Hoax.Win32.SpeedUp-MyPC.gen и др.

личества). Его особенностью является подмена оригинального сетевого ресурса на мошеннический и скрытое перенаправление пользователя на поддельный сайт с целью завладения личными данными пользователя. Осуществляется посредством использования вредоносных программ класса XSS (от англ. Cross-Site Scripting – «межсайтовый скриптинг»), осуществляющих внедрение в выдаваемую веб-системой страницу вредоносного кода, либо подмены кэша DNS на конечном устройстве пользователя или на сетевом оборудовании провайдера услуг связи. Возможна также модификация системных настроек (например, перенастройка браузера на работу через троянский прокси-сервер или подмена DNS-сервера провайдера в настройках TCP/IP на троянский DNS-сервер).

Еще одним современным видом мошенничества, направленного на несанкционированное получение доступа к СЭП, является *взлом сети, составляющей «интернет вещей»* пользователя (1,04% от общего количества). Используя специальное программное обеспечение (например, поисковые системы Shodan и Censys), злоумышленники осуществляют поиск незащищенных роутеров, IP-камер, элементов системы «умный дом», носимых смарт-гаджетов и других устройств, использующих установленные по умолчанию логины и пароли либо имеющих иные уязвимости. Затем, подключаясь к этим устройствам, правонарушители приобретают доступ к персональной информации владельца (сведения об аккаунте, цифровом окружении, домашней Wi-Fi-сети и пр.), позволяющей выполнить скрытое перенаправление пользователя на мошеннический сайт. Принимая сообщения от доверенных устройств в своей домашней сети, пользователь обычно не сомневается в их достоверности и переходит по вредоносным ссылкам либо выполняет иные действия, посредством которых мошенники получают неправомерный доступ к СЭП потерпевшего.

В контексте растущей общественной опасности преступлений рассматриваемой категории особое значение приобретает *мошенничество в системах ДБО* (11,31% от общего количества).

Различные методы мошенничества указанного вида нередко могут быть классифицированы как одна из форм фишинга. Вместе с тем, с точки зрения практической реализации мошенничество в системах ДБО основано на получении несанкционированного доступа к пользовательской информации, необходимой для авторизации и последующего хищения денежных средств со счетов пользователей. Злонамеренные действия правонарушителей обычно основываются на различных способах использования вредоносных программ. К наиболее распространенным из них относятся:

1) *«заражение» вредоносным программным обеспечением компьютера с системой ДБО пользователя посредством целевой рассылки электронных писем*. В их тексте обычно приводятся и обосновываются причины для открытия файла с вирусом, прилагаемого к письму (например, с просьбой проверки документов финансового характера, статистической отчетности и пр.). После открытия вложенного файла компьютерный вирус внедряется в систему пользователя и сообщает на удаленный сервер злоумышленника свой статус об успешной установке. Данный метод актуален для проведения целевых атак, когда у мошенника имеются адреса электронной почты лиц, работающих с системой ДБО;

2) *эксплуатация уязвимостей на тематических сайтах* (например, «Клерк.ру», «Audit – it.ru», «Бухгалтерия онлайн», «В помощь бухгалтеру» и др.). Данный метод является одним из наиболее эффективных, поскольку дает возможность выполнять массовое распространение вредоносного программного обеспечения с учетом конкретной целевой аудитории. Схема атаки обычно состоит из следующих действий:

– осуществляется компрометация соответствующего тематического сайта;

– в сайт встраивается вредоносный программный код, который вместе с содержимым сайта загружает вредоносные компоненты;

– при посещении пользователями такого сайта правонарушителем осуществляется анализ их программно-аппаратного окружения (операционная система, установленные компоненты, браузер и его плагины и др.). В случае обнаружения осуществляется загрузка и запуск заданной вредоносной программы;

– после запуска вредоносной программы на удаленный сервер злоумышленника сообщается статус об успешной установке;

– злоумышленник проверяет на сервере появление новых событий от распространяемых им программ.

Последующие действия мошенников обычно направлены на закрепление в системе, дальнейшее хищение ключевой информации, а также получение удаленного управления компьютером[5].

С развитием информационно-коммуникационных технологий одной из распространенных разновидностей рассмотренного способа мошенничества стало *создание поддельных платежных систем и форм экспресс-оплаты*. Осуществляя взлом систем защиты популярных онлайн-сервисов (интернет-магазины, электронные сервисы объявлений, торговые площадки, банки и пр.), мошенники создают ложные формы оплаты, посредством которых получают доступ к денежным средствам пользователей, оплачивающих различные услуги.

Для маскировки всех вышеприведенных мошеннических действий, а также сокрытия соответствующих следов злоумышленники обычно используют приемы и методы, основанные на применении браузера сети Tor, виртуальных частных сетей и прокси-серверов, позволяющих скрывать реальный IP-адрес, а также сетевых атак класса *DoS* (от англ. Denial of Service – отказ в обслуживании), с помощью которых блокируется доступ легитимных пользователей к системным ресурсам.

[5] Мошенничество в платежной сфере: Бизнес-энциклопедия / Л. Лямин [и др.]. – М. : ЦИПСиР, 2016. – С. 6.

Таким образом, структурное строение способов мошенничества с использованием СЭП характеризуется тем, что они, как правило, относятся к разновидности полноструктурных, включающих в себя подготовку, совершение и маскировку (сокрытие) преступлений.

Важным структурным элементом механизма преступления являются сведения об особенностях следовой информации и объектах-носителях, ее отражающих. Знание таких особенностей позволяет органу уголовного преследования, с одной стороны, установить в первоначальных следственных ситуациях характерный способ совершения расследуемого уголовно-наказуемого деяния (даже по отдельным признакам), а с другой – при обнаружении следов определенного вида выдвинуть типовую версию о расследуемом событии. Следовая информация по делам о преступлениях, совершаемых с использованием информационных технологий, характеризуется наличием идеальных, материальных и виртуальных (образующихся в электронной среде) следов преступления. Источником идеальных следов являются свидетели, обвиняемые (подозреваемые) по делам рассматриваемой категории, а также лица, пострадавшие от смежных либо сопутствующих деяний.

Материальные следы преступления являются традиционным объектом криминалистического исследования и включают в себя следы-отображения, следы-предметы и следы-вещества: различные договоры, записи, распечатки; следы пальцев рук на клавиатуре аппаратных компонентов компьютера; следы красителей, тонеров, чернил; микрочастицы (например, волокна одежды на мебели, волосы, перхоть, попавшие на клавиатуру); следы обуви; следы орудий взлома и инструментов в помещениях, где происходил непосредственный физический контакт с компьютерной техникой.

В ходе раскрытия и расследования преступлений, совершаемых с использованием информационных технологий, наибольшей спецификой, а, следовательно, и значимостью, обладают виртуальные следы. Под ними обычно понимают любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов [2, с. 94]. Их специфика обусловлена в первую очередь особенностями способов подготовки, совершения и сокрытия таких преступлений, в основе которых лежат технологии создания или преобразования компьютерной информации в форме уничтожения, копирования, блокирования или модификации (в т.ч. с использованием территориально-распределенной передачи информации в сетях электросвязи), а также соответствующие им изменения физических характеристик ее носителя, имеющие причинно-следственные связи с событием правонарушения.

Указанное обстоятельство закономерно обусловливает специфические особенности орудий и средств совершения рассматриваемых преступлений, в качестве которых обычно выступают программное обеспечение, компьютерная техника (в т.ч. электронные носители информации), а также сети электросвязи (локальные сети, глобальная сеть «Интернет», проводные и беспроводные каналы связи). Так, компьютерная информация в механизме уголовно-наказуемых деяний, сопряженных с использованием СЭП, выступает не только как предмет преступного посягательства (при ее неправомерном уничтожении, копировании, блокировании или модификации), но и является средством совершения преступления.

Существенное значение для установления виртуальных следов, свидетельствующих об обстоятельствах совершенного преступления, имеет *механизм следообразования* в различных программно-аппаратных средах. Так, при установлении следовой картины противоправного деяния может представлять интерес информация, содержащаяся в реестре операционной системы, системных журналах и лог-файлах (протоколах автоматической регистрации событий в хронологическом порядке, происходящих в ходе работы операционной системы и иного программного обеспечения), регистрационных сведениях о сетевых ресурсах, доменах и их владельцах. Указанные объекты могут нести определенную криминалистически значимую информацию, представляющую оперативный интерес и свидетельствующую об использовании программных и сетевых ресурсов в преступных целях. Данная информация может быть выявлена и зафиксирована следующими способами: в ходе мониторинга сетевых ресурсов, на которых пользователями неоднократно размещалась данная информация; в ходе проведенных оперативно-розыскных мероприятий; в заявлении потерпевшего о преступлении; в рамках расследования другого уголовного дела; при получении информации от граждан [3, л. 21].

Определяющим для формулирования системы следов по делам о преступлениях, сопряженных с использованием СЭП, представляется закономерная связь этапов механизма преступления: *рассылка информации (спам, поддельные e-mail, вредоносное программное обеспечение) – взаимодействие с пользователем СЭП (прием «заказов», переписка, скрытая переадресация на поддельный интернет-ресурс) – вывод денежных средств (перевод и обналичивание)*. Указанные этапы являются взаимосвязанными звеньями единой цепи, развертывание которой подчинено общему преступному замыслу. При этом каждый из них может рассматриваться как самостоятельный и целостный источник виртуальных следов, отражающей определенные процессы взаимодействия участников криминального события между собой и с окружающей средой.

Так, при *рассылке спама либо поддельных e-mail* на компьютере у потерпевшего можно обнаружить следующие виртуальные следы:

– фотоизображения товаров, «приобретенных» либо предлагаемых для «приобретения» в ходе мошеннической сделки, а также их метаданные – структурированные данные (признаки), уникальным образом описывающие компьютерную информацию: имя, размер (объем), формат (вид информации), время и дата (создания, модификации, использования, уничтожения), атрибуты (скрытый, системный, архивный, только для чтения),

месторасположение источника, параметры безопасности (права доступа, владелец, свойства аудита и пр.), наличие предыдущих версий и т.д.;

– номера мобильных телефонов и иные контактные данные (e-mail, логины Skype, учетные данные мессенджеров и пр.), указанных в объявлении;

– техническая информация о компьютере отправителя, содержащаяся в служебных заголовках e-mail (название и номер версии почтового клиента, тип операционной системы, наименование и номер версии почтового сервера, внутренние IP-адреса, тип используемого брандмауэра, результаты проверки антивирусом);

– содержание переписки с использованием СМС, e-mail, различных мессенджеров (Skype, Viber, Telegram, WhatsApp и др.);

– номера счетов, электронных кошельков и банковских карт, на которые и с которых потерпевшим были переведены денежные средства.

Виртуальные следы, свидетельствующие о рассылке спама либо поддельных e-mail, следует искать и на компьютере у злоумышленника. Если правонарушитель самостоятельно осуществлял вредоносную рассылку, то у него может быть найдено специализированное программное обеспечение (как платное, так и бесплатное), предназначенное для рассылки спама по электронной почте, массового постинга в веб-форумы и доски объявлений. Если обращался к услугам профессионалов («спамеров»), то при поиске указывающих на это следов необходимо обратить внимание на его контакты с таковыми: просмотр объявлений о предлагаемых услугах спамеров, содержание возможной переписки с ними, следы подготовки размещаемого текста, перевода денежных средств и пр.

На *использование вредоносных программ в компьютере* потерпевшего могут указывать: информация, находящаяся в оперативной памяти или файле подкачки либо гибернации; лог-файлы, содержащие протоколы результатов работы антивирусных и тестовых программ; модифицированные файлы, входящие в состав системного и прикладного программного обеспечения, контрольная сумма (CRC) которых отличается от заявленной производителем (например, изменение основной загрузочной записи MBR, файловой таблицы MFT, подмена исполняемых файлов операционной системы и т.д.); записи в системном реестре или каталогах профилей пользователей; файлы конфигурации безопасности и настроек сетевого окружения (IP-адрес, маска подсети, шлюзы, DNS, монтируемые сетевые диски, таблица маршрутизации и т.п.); журнал событий операционной системы (протоколы загрузки, безопасности, аудита, ошибок и т. п).

При *изготовлении вредоносных программ* на компьютере злоумышленника могут быть обнаружены следующие виртуальные следы:

– исходные коды вредоносных программ, в том числе программ двойного назначения;

– файлы программного обеспечения, не имеющие электронной цифровой подписи, либо не имеющие информации о разработчиках, либо входящие в состав «потенциально опасных программ» (программы-кейлоггеры, программы тестирования уязвимостей, средства для дизассемблирования и отладки программного кода, драйверы виртуальных устройств, эмуляторы и т.п.);

– программное обеспечение для управления вредоносными программами (большинство из них работает по схеме «клиент-сервер», предусматривающей скрытую установку одной из частей (клиентское приложение) на компьютер жертвы; другая же часть (сервер) устанавливается на компьютер злоумышленника для дистанционного контроля и управления «зараженным» устройством).

– иные файлы, образующиеся в ходе криминальной деятельности правонарушителя, в том числе их резервные копии и удаленные файлы, подлежащие восстановлению.

О *целевом применении (распространении) вредоносного программного обеспечения* могут свидетельствовать различные информационные объекты, выявленные на компьютере правонарушителя и содержащие деструктивный код, например: файлы исполняемых программ; командные файлы, скрипты (CMD, BAT, INF, SH и пр.), файлы офисных документов; файлы интерпретируемых программ; загрузочные секторы жестких дисков и электронных носителей; сообщения электронной почты; пиринговые (файлообменные) сети; системные драйверы.

При *создании в сети «Интернет» поддельного интернет-ресурса*, выдающего себя за популярный онлайн-сервис, можно рассчитывать на обнаружение следующих виртуальных следов на компьютере злоумышленника:

– регистрационные данные на доменное имя;

– лог-файлы, в которых отражены сведения о взаимодействии с регистратором доменных имен (запросы на оказание услуг хостинга, перечисление денежных средств, авторизация на веб-сервере, работа с конструктором сайта, залив контента и пр.);

– лог-файлы, в которых отражена информация об истории настроек DNS-сервера, поддерживающего домен мошенников;

– сведения о SEO-раскрутке мошеннического сайта (переписка с рекламными студиями, площадками обмена баннерами и ссылками, рассылка спама и пр.);

– лог-файлы с записями о фактах отслеживания активности посетителей мошеннического сайта.

При *взаимодействии злоумышленника с пользователем СЭП – потенциальной жертвой криминального деяния* могут быть обнаружены следы от переписки (e-mail, мессенджеры, СМС, веб-формы), раскрывающей детали различных аспектов мошеннических действий (прием «заказов», уточняющие вопросы, «техническая» поддержка и пр.). О скрытой переадресации на поддельный интернет-ресурс могут свидетельствовать история посещенных веб-ресурсов в браузере на компьютере потерпевшего и сравнение ее с историей ввода поисковых запросов. Если переадресация осуществлялась в ходе перехода по ссылкам, то эффективным способом ее обна-

ружения является исследование файлов *.htaccess* и *<head>* документов. Получить информацию о «незаконных» скрытых переадресациях, возникших в результате несанкционированного доступа к компьютеру пользователей СЭП, помогут предупреждения из Google Search Console (веб-сервис, позволяющий проверять статус индексации и оптимизировать видимость сайтов), а также аналитика поведения пользователей в Google Analytics и «Яндекс.Метрике» (сервисы для создания детальной статистики посетителей веб-сайтов). Возможно также использование специального программного обеспечения, позволяющего выявлять правила скрытой переадресации (например, Netpeak Spider (https://netpeaksoftware.com/ru/spider), Rookee (https://www.rookee.ru) и др.).

При *получении и выводе (обналичивании) денежных средств* правонарушители обычно оставляют следующие виртуальные следы:

– лог-файлы со сведениями о вводе и выводе денег из СЭП (банковские реквизиты, дата и время транзакции, наименование валюты и сумма денежных средств);

– лог-файлы в системах дистанционного управления счетами в СЭП (дата и время входа и выхода, идентификаторы транзакций);

– сведения о взаимодействии с посредниками по безопасному выводу, обналичиванию денежных средств (переписка по e-mail, СМС, мессенджеры).

Для обнаружения виртуальных следов *подготовки и проведения сетевых атак класса DoS* на компьютере потерпевшего рекомендуется исследовать лог-файлы программных средств защиты – антивирусных программ, межсетевых экранов, детекторов атак и аномалий трафика, систем обнаружения неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими.

На компьютере правонарушителя могут быть обнаружены следующие виртуальные следы, указывающие на факт подготовки и проведении сетевых атак данного класса:

– наличие установленных программ, предназначенных для осуществления вредоносных атак, например: «Hoic» (высокоскоростной многопоточный генератор пакетов типа http-flood), «Hping» (генератор пакетов и анализатор протокола TCP/IP), «Pyloris» (программное средство для тестирования серверов, может быть использован для реализации DoS-атак); «Thcssl» (программа для «бесконечной» перезагрузки, а следовательно – и деактивации удаленного сервера); «Torshammer» (программный инструмент, позволяющий выполнять анонимные атаки через сети Tor и др.), а также лог-файлы, образующиеся в ходе их работы;

– лог-файлы со сведениями, указывающими на контрольные обращения правонарушителя к атакуемому веб-ресурсу в ходе проведения атаки, чтобы удостовериться в ее действенности.

В случае осуществления атак с использованием бот-сетей (от англ. botnet – компьютерная сеть, в которой каждое устройство с доступом в интернет заражено вредоносной программой и управляется бот-мастером), на компьютере у правонарушителя могут быть найдены следы соответствующего программного обеспечения.

Существенное значение для раскрытия и расследования инцидента могут иметь лог-файлы, содержащие статистические сведения операторов связи о сетевом трафике, через сети которых осуществлялась вредоносная атака.

Обобщение особенностей представленных характерных объектов-носителей виртуальных следов преступной деятельности в сфере использования СЭП поможет создать необходимую основу для разработки, внедрения и эффективного применения средств и методов собирания, и исследования следовой информации.

Следует добавить, что представленные в настоящей работе типичные способы совершения преступлений, сопряженных с использованием СЭП, и соответствующая им система виртуальных следов не исключают и не ограничивают дополнительное исследование механизма совершения рассматриваемых криминальных деяний, и могут быть детализированы и дополнены.

Заключение. Суммируя вышеизложенное, представляется возможным сформулировать следующие выводы.

1. Активное внедрение различных систем расчетов с использованием СЭП привело к появлению разнообразных специфических форм мошенничества. В их основе лежат методы социальной инженерии, основанные на применении достижений современных информационно-коммуникационных технологий, а также на действиях и подходах, посредством которых мошенники получают неправомерный доступ к СЭП потерпевшего.

2. Типичными способами совершения преступлений, сопряженных с использованием СЭП, являются:

– *фишинг* – введение пользователя СЭП в заблуждение при помощи поддельного сайта, предполагающего авторизацию пользователя и последующий несанкционированный доступ правонарушителя к его персональным данным, реализуемое с помощью рассылки спама и (или) внедрения вредоносных программ;

– *фарминг* – скрытое перенаправление пользователя на мошеннический сайт с целью завладения личными данными пользователя, осуществляемое посредством внедрения в выдаваемую веб-системой страницу вредоносного кода, либо подмены кэша DNS на конечном устройстве пользователя или на сетевом оборудовании провайдера услуг связи;

– *взлом сети, составляющей «интернет вещей» пользователя*, основанный на эксплуатации недокументированных уязвимостей элементов сети, позволяющей выполнить скрытую переадресацию пользователя на мошеннический сайт;

– *мошенничество в системах ДБО*, основанное на получении несанкционированного доступа к пользовательской информации, необходимой для авторизации и последующего хищения денежных средств со счетов пользователей. Реализуется с помощью внедрения вредоносных программ на компьютер с системой ДБО пользователя посредством целевой рассылки электронных писем, либо эксплуатации уязвимостей на тематических сайтах.

3. Специфика виртуальных следов, обращающихся в ходе совершения преступлений, сопряженных с использованием СЭП, обусловлена в первую очередь особенностями способов их подготовки, совершения и маскировки (сокрытия).

4. Определяющим критерием для формирования системы следов по делам о преступлениях, сопряженных с использованием СЭП, является закономерная связь этапов механизма преступления (рассылка информации – взаимодействие с пользователем СЭП – вывод денежных средств), каждый из которых может рассматриваться как самостоятельный и целостный источник виртуальных следов, отражающей определенные процессы взаимодействия участников криминального события между собой и с окружающей средой.

ЛИТЕРАТУРА

1. Зуйков, Г.Г. Криминалистическое учение о способе совершения преступления : автореф. дис. ... д-ра юрид. наук / Г.Г. Зуйков ; Высш. шк. МВД СССР. – М., 1970. – 31 с.
2. Вехов, В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации средств ее обработки / В.Б. Вехов. – Волгоград : ВА МВД России, 2008. – 401 с.
3. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети интернет : дис. ... канд. юрид. наук / А.Н. Колычева. – М., 2018. – 200 л.

REFERENCES

1. Zuikov, G.G. (1970). *Kriminalisticheskoe uchenie o sposobe sovershenіya prestupleniya*. Moscow. (In Russ.).
2. Vekhov, V.B. (2008). *Osnovy kriminalisticheskogo ucheniya ob issledovanii i ispol'zovanii komp'yuternoi informatsii sredstv ee obrabotki*. Volgograd: VA MVD Rossii. (In Russ.).
3. Kolycheva, A.N. (2018). *Fiksatsiya dokazatel'stvennoi informatsii, khranyashcheisya na resursakh seti internet*. Moscow. (In Russ.).

Поступила 16.10.2021

CRIMES ASSOCIATED WITH THE USE OF ELECTRONIC PAYMENT MEANS: METHODS AND TRACE INFORMATION

P. BOROVIK

The results of a forensic analysis of typical methods of committing crimes involving the use of electronic payment methods are presented. It is shown that the basis of this criminal activity are the methods of social engineering based on the application of the achievements of modern information and communication technologies, as well as on actions and approaches through which offenders gain unauthorized access to the personal data of the victim. Taking into account the study of the stages of the mechanism of the considered criminal acts, the sources of trace information are formulated, reflecting the processes of interaction of participants in a criminal event with each other and with the environment.

Keywords: *fraud, means of electronic payment, crime prevention, fraud, method of crime, trace information.*