осмотра) организационных методов защиты информации (порядок осуществления пропускного режима в осматриваемом месте, типичные места хранения электронных носителей информации, возможность проникновения посторонних лиц к осматриваемому месту и др.); технических методов защиты информации (фильтры, экраны на аппаратуру, ключ для блокировки клавиатуры, устройства аутентификации, электронные ключи на микросхемах и др.); программных методов защиты информации (блокировка экрана и клавиатуры, использование средств парольной защиты BIOS и др.).

В случае наличия сведений о лице, предположительно совершившем преступление, нужно сконцентрировать внимание на программно-технических устройствах и предметах, в ходе предварительного осмотра которых можно выявить следы преступной деятельности установленных лиц. В случае отсутствия сведений о лице, совершившем преступление, принять меры по его установлению и розыску с учетом выявленных сведений на месте происшествия.

Таким образом, рассмотренный алгоритм действий в ходе осмотра места происшествия по уголовным делам о хищениях имущества путем модификации компьютерной информации позволяет повысить результативность следственного действия, избежать утери доказательственной информации, с помощью которой возможно установление различных обстоятельств совершенного преступления.

УДК 343.8

П.Л. Боровик

СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ, СОПРЯЖЕННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Разнообразие современных способов мошенничества с использованием средств электронных платежей диктует необходимость их комплексного изучения с целью выработки научно обоснованных рекомендаций по противодействию им. В контексте растущей общественной опасности данных уголовно наказуемых деяний особую важность приобретает необходимость научного осмысления типичных способов их совершения. Полагаем, что знание таких способов позволит практическому сотруднику более качественно оценить информацию об обстоятельствах уголовно наказуемого деяния в конкретной следственной ситуации и принять верное тактическое и уголовно-процессуальное решение в условиях недостаточной информационной определенности.

Одним из наиболее распространенных способов совершения преступлений указанного вида является фишинг (англ. phishing, от password fishing – выуживание паролей). В классической интерпретации термин означает введение пользователя в заблуждение при помощи поддельного сайта, визуально имитирующего сайт банка или иной интернет-системы, предполагающей идентификацию пользователя. Главная задача мошенника – завлечь пользователя на этот сайт и убедить его сообщить идентификационные данные. Для этого злоумышленники используют следующие приемы и методы:

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.);

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 неподтвержденные пользователем действия – сбор информации о банковских платежных карточках и передача этой информации злоумышленнику, использование ресурсов компьютера в целях майнинга, нелегальной торговли и др.).

Разновидностью фишинга является преднамеренное введение пользователя в заблуждение посредством использования программного обеспечения класса Hoax (англ. – обман) с целью получения финансовой выгоды. Такие программы обычно выдают на экран информацию о несуществующих ошибках в работе компьютера, вынуждая пользователя заплатить деньги, чтобы избавить компьютер от якобы обнаруженных ими угроз. При этом подобные программы чаще всего именно вынуждают, а не предлагают себя приобрести, объявляя пользователю, что иным способом проблему не решить.

Следующим не менее актуальным способом совершения преступления, сопряженного с использованием средств электронных платежей, является фарминг (англ. pharming – скрытное перенаправление на ложный IP-адрес). При его реализации происходит подмена оригинального сетевого ресурса на мошеннический и скрытое перенаправление пользователя на поддельный сайт с целью завладения личными данными пользователя. Посредством использования вредоносных программ класса XSS (англ. Cross-Site Scripting – межсайтовый скриптинг) осуществляется внедрение в выдаваемую веб-системой страницу вредоносного кода либо подмена 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 средствам электронных платежей, является взлом сети, составляющей интернет вещей пользователя. 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. После чего, подключаясь к этим устройствам, правонарушители получают доступ к персональной информации владельца (сведения об аккаунте, цифровом окруже-

нии, домашней Wi-Fi-сети и т. д.), 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 средствам электронных платежей пользователя.

В контексте растущей общественной опасности преступлений рассматриваемого вида особое значение приобретает мошенничество в системах дистанционного банковского обслуживания «Клиент – Банк». Различные методы мошенничества указанного вида нередко могут быть классифицированы как одна из форм фишинга. Вместе с тем с точки зрения практической реализации мошенничество в таких системах дистанционного банковского обслуживания 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 методах использования вредоносных программ. К наиболее распространенным из них относятся:

заражение вредоносным программным обеспечением компьютера с системой дистанционного банковского обслуживания пользователя посредством целевой рассылки электронных писем (после открытия вложенного файла компьютерный вирус внедряется в систему пользователя, после чего сообщает об успешной установке злоумышленнику);

эксплуатация уязвимостей на тематических сайтах (например, «Бухгалтерия онлайн», «В помощь бухгалтеру» и др.) – один из наиболее эффективных методов, поскольку дает возможность выполнять массовое распространение вредоносного программного обеспечения с учетом конкретной целевой аудитории.

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 т. д.), мошенники создают ложные формы оплаты, посредством которых получают доступ к денежным средствам пользователей, оплачивающих различные услуги.

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

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

Представленные способы совершения преступлений, сопряженных с использованием средств электронных платежей, не ограничивают дополнительное исследование механизма совершения рассматриваемых уголовно наказуемых деяний и могут быть детализированы и дополнены.

УДК 343.985.2

Д.Г. Вильмак

ТАКТИКА ПОЛУЧЕНИЯ ВЕРБАЛЬНОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ

Следственные действия, которые основываются на устном общении, называются вербальными (допрос, очная ставка, предъявление для опознания и др.). В настоящее время ученые выделяют три вида вербальной информации: речь, письменное и внутреннее общение.

Относительно речи применительно к рассматриваемому вопросу можно сказать, что с помощью речи следователь общается, проводя допрос подозреваемого, обвиняемого, свидетеля, специалиста, эксперта и др., получает какую-либо информацию.

Как справедливо отмечает В.И. Комиссаров, общими признаками вербальных следственных действий являются психологические и логические приемы получения, анализа и использования информации от человека при проведении допроса, очной ставки, проверки показаний на месте.

От проведения мероприятий по получению вербальной информации, а именно качественного опроса виновных лиц, свидетелей и очевидцев, зависит успех и ход дальнейшего расследования уголовного дела.

При изучении уголовных дел нами установлено, что опрос проводился в 100 % случаев по делам любой категории, так как данное мероприятие позволяет в полной мере установить следовую картину происшествия, наличие причастности лица к тому или иному факту, определить, ориентируется ли задержанное лицо или явившееся с явкой с повинной в совершенном преступлении. Признание лицом факта совершения им преступления – это всего лишь информация, придающая определенную, в данном случае обвинительную, интерпретацию полученным в ходе проверки сообщения о преступлении сведениям и делающая их пригодными в качестве ориентира для производства дальнейших следственных действий в целях достижения положительного результата по тому или иному уголовному делу.

При изучении юридической литературы Российской Федерации не было найдено конкретного определения такого действия, как получение объяснения, что, в свою очередь, затрудняет понимание его смысла и природы. Следует указать, что в белорусском законодательстве закреплено определение понятия «получение объяснения» в следующей интерпретации.

Получение объяснений – процессуальный способ собирания сведений об обстоятельствах преступного деяния, который используется до возбуждения уголовного дела. Таким образом, получение объяснений является первоочередным способом