УДК 343.985.7:[343.7:004](470)

И. Ю. ГАЗИМУЛЛИН, *доцент кафедры оперативно-разыскной деятельности органов внутренних дел Уфимского юридического института МВД России (г. Уфа)*

I. Y. GAZIMULLIN, *associate professor of the department of investigative activities of the internal affairs bodies Ufa Law Institute of the Ministry of Internal Affairs of the Russian Federation (Ufa)*

НЕКОТОРЫЕ ОРГАНИЗАЦИОННО-ТАКТИЧЕКСКИЕ ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

THE SOME ORGANIZATIONAL AND TACTICAL FEATURES OF COUNTERING CRIMES COMMITTED WITH THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Аннотация. *В настоящей статье рассмотрены актуальные проблемы противодействия преступлениям, совершаемым с использованием современных информационно-телекоммуникационных технологий, основные способы их совершения, а также некоторые организационно-тактические аспекты их раскрытия органами внутренних дел.*

Ключевые слова и словосочетания: *информационные технологии, преступление, сайт, платформа, программное обеспечение, вирус, криптовалюта, платежная система.*

Annotation. *This article is devoted to the actual problems of countering crimes committed using modern information and telecommunication technologies, the main ways of committing them, as well as some organizational and tactical aspects of their disclosure by internal affairs bodies, are considered in detail.*

Keywords and phrases: *information technology, crime, website, platform, software, virus, cryptocurrency, payment system.*

Современная система коммуникации (сотовая связь, интернет) прочно вошла в жизнь современного человека и общества. Процесс цифровизации глобально охватил различные сферы жизни и производства. Современные информационные технологии не только предоставляют удобства в процессе коммуникации (прием и передача различной информации), но и облегчают доступ к данным пользователей (персональные данные, логины и пароли социальных сетей данные по открытым банковским счетам и т. д.), что создает благоприятные условия для действий преступников, направленных на хищение денежных средств путем обмана, злоупотребления доверием, вымогательства.

Уголовным законодательством Российской Федерации ответственность за хищение денежных средств с использованием информационно-телекоммуникационных технологий предусмотрена пунктом «г», части 3 статьи 158 (кража, совершенная с банковского счета, а равно в отношении электронных денежных средств), а также статьей 159.3 (мошенничество с использованием электронных средств платежа) Уголовного кодекса Российской Федерации (далее – УК РФ) [1].

Особенностью преступлений, совершаемых с использованием информационно-коммуникационных технологий, является сложный алгоритм действий, организованность, высокий уровень законспирированности преступников, транснациональный характер.

Стабильный рост совершаемых преступлений данной категории прослеживается

по всей территории государства, что в свою очередь не может не создавать соответствующий негативный общественный резонанс, требующий от органов правопорядка необходимой реакции для стабилизации оперативной обстановки.

Так, на территории Республики Башкортостан в 2020 году зарегистрировано 7141 преступление, предусмотренное статьей 159 УК РФ, в том числе с использованием сотового телефона – 2701, с использованием информационно-телекоммуникационной сети Интернет – 3569, с использованием банковских карт – 1002 преступления. За 10 месяцев 2021 года зарегистрировано 5480 преступлений: с использованием сотового телефона – 2184, с использованием информационно-телекоммуникационной сети Интернет – 2961, с использованием банковских карт – 444.

Приведенная статистика свидетельствует о стабильном росте преступлений, совершаемых с использованием информационных технологий, что в свою очередь вызывает острую необходимость в повышении качества противодействия указанным преступлениям.

К наиболее частым способам совершения преступлений с использованием средств коммуникации в сети Интернет можно отнести следующие:

1. Хищение денежных средств посредством получения предоплаты за товары и услуги с использованием интернет-сервисов для размещения объявлений, к примеру, «Авито», «Юла», «Циан» и других.

2. Хищение денежных средств с использованием неправомерного доступа (методом фишинга (от английского «fishing» – доступ к конфиденциальным данным (логинам и паролям) пользователей, который достигается путем массовых рассылок электронных писем с указанием прямых ссылок на сайты, внешне не отличающиеся от настоящих либо на сайты с редиректом); с использованием вредоносного программного обеспечения «MALWARE» (от английского «malicious software» – вредоносное программное обеспечение, имеющее своей целью в той или иной форме нанести ущерб пользователю либо компьютеру и его содержимому); с использованием методов социальной инженерии к аккаунтам социальных сетей.

3. Хищение денежных средств, совершаемое с использованием виртуальных SIP-номеров, указанных на подложных сайтах (например, на сайтах интернет-магазинов) при оплате различных товаров и услуг.

4. Хищение денежных средств, совершаемое под предлогом разблокировки банковских карт либо предотвращения транзакций, посредством рассылки SMS-сообщений с текстом о списании денежных средств или блокировке банковской карты.

5. Хищение денежных средств, совершаемое под предлогом оказания помощи, как правило, родственнику, попавшему в беду.

6. Хищение денежных средств, совершаемое с использованием вирусного программного обеспечения («Triada» и «Marcher») для операционной системы «Android».

Однако, наиболее сложными в организации раскрытия остаются преступления, совершаемые с использованием «фишинговых» сайтов, алгоритм совершения которых рассмотрим далее.

Преступления, совершаемые с использованием ссылок на фишинговые сайты (т. е. копии сайтов объявлений), представляют собой работу организованных преступных групп с детализированным распределением ролей и задач, возлагаемых на каждого из участников. Основной задачей преступной группы является получение от жертв информации о реквизитах банковской карты (номер, срок действия, данные держателя) и CVV/CVC-кода (от английского «Card Verification Value» – «значение верификации карты», которое является номером, зашифрованным в магнитной полосе карт международной платежной системы «Visa»), подтверждающим подлинность карты и совершение платежной операции держателем денежных средств.

В структуру организованной преступной группы входят следующие участники:

– организатор-администратор («topic starter» – от английского «topik», обозначающего тему, и «to start» – начинать; выраже-

ние компьютерного сленга, обозначающее человека, инициировавшего тему на форуме либо на другом сайте, где общаются пользователи);

– пособники («дропы» – подставные лица, предназначенные для промежуточного приема банковских переводов, товаров и посылок; «саппорты» – специалисты, решающие возникающеие технические проблемы работы сайта или платформы);

– исполнители («воркеры», или «спаммеры» – лица, в задачи которых входят: регистрация на сервисах бесплатных объявлений «аккаунтов-однодневок», создание объявлений-приманок по заготовленным шаблонам, коммуникации с жертвами посредством чатов на площадках объявлений или в мессенджерах, доставка фишинговых ссылок).

На организатора возлагаются следующие обязательства, заключающиеся в виде создания и предоставления:

– группы в кроссплатформенной системе мгновенного обмена сообщениями «Telegram» для общения на условиях анонимности, получения инструкций (мануалов) по совершению преступлений, получения выплат за совершение преступлений;

– автоматизированной системы для создания ссылок на фишинговые сайты (боты) с функцией копирования реального объявления, созданного на платформах размещения объявлений, например, «Avito», «Юла», «BlaBlaCar», «Booking»;

– фишингового сайта с платежной системой, обеспечивающего получение информации о реквизитах банковской карты потерпевшего;

– создание сети «дропов», которая является неким списком тех, на чьи банковские карты будут перечисляться денежные средства потерпевших.

Хищение денежных средств осуществляется следующими путями.

1. Путем прямого перевода со счета карты потерпевшего с использованием сведений о реквизитах банковской карты и простого ключа электронной подписи (SMS-кода подтверждения из банка) на первую «дроп»-карту. Перевод средств осуществляется автоматически специальной программой, предназначенной для формирования распоряжения на перевод денежных средств через сервисы некоторых банков, к примеру, CARD2CARD, P2P.

2. Путем ручного списания, т. е. хищения с использованием сведений о реквизитах банковской карты и простом ключе электронной подписи (SMS-кода подтверждения из банка), путем их ввода на сайтах различных магазинов либо путем входа в личный кабинет онлайн-банка потерпевшего, при этом организатор получает доступ через исполнителя в виде скриншота из SMS-оповещений из банка.

На исполнителя («воркера») возлагаются следующие обязательства:

– поиск потенциальных жертв на сайтах объявлений;

– связь с жертвой с последующим переводом её на фишинговый сайт;

– получение от жертвы простого ключа электронной подписи (SMS-кода подтверждения из банка).

Пособники («саппорты») выполняют функцию администраторов фишинговых сайтов и вступают в общение с потерпевшим в случае, когда необходимо дополнительное введение в заблуждение. Например, после списания денежных средств потерпевший сомневается, что товар будет доставлен, и «саппорт» убеждает оформить возврат денежных средств, после чего потерпевший снова вводит реквизиты банковской карты, простой ключ электронной подписи, вследствие чего денежные средства списываются повторно.

Другие пособники («дропы») обеспечивают движение денежного потока путем предоставления банковских карт, которые оформлены на их имена или подставное лицо либо без полного оформления, для первичного перевода либо последующего приема денежных средств, их последующего обналичивания либо конвертации в криптовалюту (электронное платежное средство без физического выражения формы, используемое как традиционные денежные средства, включая хранение, передачу третьим лицам, оплату товаров и услуг).

Таким образом, после первичного списания денежные средства потерпевшего поступают администратору на карту дропа, администратор переводит деньги в криптовалюту либо отправляет деньги на другую карту дропа во избежание блокирования банком, а затем покупает криптовалюту. По договоренности с исполнителями администратор пересылает около 80 % от похищенной суммы в виде криптовалюты, а исполнитель в свою очередь через криптовалютные обменники (сервисы, специализирующиеся на обменах цифровых активов) выводит деньги на свою карту.

Криптовалютные обменники, участвующие в транше денежных средств, являются частными лицами, не входящими в число членов преступной группы, а свою выгоду они получают от владения криптовалютой и её продажи.

В целях раскрытия и расследования данного вида преступления необходимо организовывать и проводить первоначальные оперативно-разыскные и иные мероприятия в следующем порядке:

– при получении информации (поступлении заявления) о совершенном преступлении необходимо выяснить у жертвы, на каком ресурсе и кем размещено объявление, произвести осмотр технического устройства с целью установления адреса размещенного объявления и ссылок на фишинговый сайт, установить способ связи с заявителем, где и каким способом происходило общение (переписка, голосовые сообщения, звонки в мессенджерах или по телефону);

– при обнаружении еще активной ссылки на фишинговый сайт произвести его осмотр, в том числе зафиксировать содержимое с помощью скриншотов / фотографирования и копирования путем сохранения web-страницы (составная часть веб-сайта, интернет-магазина, портала или блога);

– от заявителя необходимо получить информацию о денежном переводе, а именно, был это прямой перевод на банковскую карту или абонентский номер преступника либо перевод через платежную систему. В случае перевода через платежную систему выяснить, какой кредитно-финансовой организации она принадлежит, после чего направить запрос на получение номера карты и IP-адреса (уникальный идентификационный номер, который присваивается каждому компьютеру при выходе в сеть Интернет). Таким образом будет установлен хостинг (место для хранения на физическом носителе хостинг-арендодателе), с использованием которого были переведены денежные средства.

– направить запросы в организации, занимающиеся SMS-активацией.

После проведения неотложных первоначальных мероприятий необходимо направить усилия на установление всех участников группы.

Для установления исполнителей (воркеров) у компаний, предоставляющих услуги сотовой связи, необходимо получить сведения о принадлежности используемых абонентских номеров и IMEI-кодов (уникальный идентификационный номер сотового аппарата) устройств, используемых для общения с потерпевшим и регистрации на сайтах объявлений. При получении ответа необходимо изучить полученные сведения и установить лицо, которое использовало абонентский номер и устройство при совершении преступления.

Для установления организаторов (администраторов) следует запросить информацию у регистратора доменных имен и хостинга по фишинговому сайту. В дальнейшем необходимо изучить ответы и направить запросы на по IP-адресам входа в личный кабинет, адресу электронной почты, в банки (либо провести идентификацию по способу оплаты через агрегаторы платежей).

При получении ответа из банка по движению денежных средств потерпевшего следует направить запрос в банк получателя денежных средств на получение информации о владельце банковской карты, привязанных к ней абонентских номерах, входах в личный кабинет, месте и времени получения банковской карты, а также запрос о дальнейшем движении денежных средств.

При получении ответа из банка получателя важно изучить полученную информацию

о дроп-карте, привязанном абонентском номере и входах в личный кабинет. По абонентскому номеру следует установить IMEI-адрес используемого устройства и его местонахождение. В дальнейшем необходимо проводить работу по лицу, использовавшему номер и устройство, в целях документирования его противоправной деятельности.

Раскрытие и расследование хищений, совершаемых с использованием средств сотовой связи и сети Интернет, требует углубленного анализа поступающей информации, индивидуального и творческого подхода к каждому факту совершенного преступления, а также специфических познаний, расширение объема которых будет приходить с опытом.

Общеизвестно, что телефонные и интернет-преступления часто носят межрегиональный характер, поэтому для достижения положительных результатов необходимо качественное поддержание взаимодействия и осуществления обмена информацией представителями правоохранительных органов всех субъектов Российской Федерации.

ЛИТЕРАТУРА

1. Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1993 г. № 63-ФЗ: (ред. от 9 марта 2022 г.) (с изм. и доп., вступ. в силу с 17 марта 2022 г.) // СПС «КонсультантПлюс».

2. Генеральная прокуратура Российской Федерации: портал правовой статистики / http://crimestat.ru>regions_chart_total (дата обращения: 01.02.2022).

УДК 343.983.22:006.91(470)

А. А. ДАМИНОВ, *старший преподаватель кафедры огневой и тактико-специальной подготовки Уфимского юридического института МВД России (г. Уфа)*

A. A. DAMINOV, *senior lecturer of the departament of fire and tactical special training of the Ufa Law Institute of the Ministry of Internal Affairs of Russia (Ufa)*

МЕТРОЛОГИЧЕСКИЙ АСПЕКТ СУДЕБНО-БАЛЛИСТИЧЕСКИХ ИССЛЕДОВАНИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОВД. МЕТОДЫ ИЗМЕРЕНИЯ ЭКСПЕРИМЕНТАЛЬНОЙ БАЛЛИСТИКИ

METROLOGICAL ASPECT OF FORENSIC BALLISTICS RESEARCH IN LAW ENFORCEMENT ACTIVITIES OF POLICE OFFICERS. METHODS OF MEASURING EXPERIMENTAL BALLISTICS

Аннотация. *В статье особое внимание уделяется общим знаниям пиродинамических процессов и пиростатике, рассматриваются теоретические и практические результаты исследований судебной*