нием и привлечением их к уголовной ответственности в качестве соучастников в случае дачи ими изобличающих показаний о совершенном преступлении.

Представляется, что разработка комплексной методики расследования – это адекватный ответ криминалистической науки на наиболее общественно опасные проявления современной преступной деятельности.[3] В случае создания методики расследования незаконной банковской деятельности и ее внедрения в деятельность органов внутренних дел, она будет широко использоваться следователями, занимающимися расследованием экономических преступлений, что позволит им быстро и точно определять способ совершения преступления, выбирать необходимый комплекс следственных действий, направленных на сбор и закрепление доказательственной базы.

[1] Поляков Н.В. К вопросу о субъекте незаконной банковской деятельности // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : материалы XV международной научно-практ. конф. Барнаул: Барнаульский юридический институт МВД России, 2017. ч. 1. С. 140-141.

[2] Соловьев И.Н. О некоторых мерах противодействия обналичиванию денежных средств // Налоговая политика и практика. 2011. № 3 (99). С. 10-15.

[3] Гармаев Ю.П. Разработка комплексной методики расследования как перспективная тенденция развития криминалистических методических рекомендаций // Правоведение. 2003. № 4. (249). С. 154-160.

Степанов А.Е.

Экспертно-криминалистический центр
Управления МВД России
по Амурской области (г. Благовещенск)

ПРОБЛЕМЫ РАССЛЕДОВАНИЯ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ ФИЗИЧЕСКИХ ЛИЦ С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНЫХ ПРОГРАММ

Современное общество находится на этапе четвертой промышленной революции. Технологии все плотнее входят во все сферы жизнедеятельности людей. Автоматизация бизнес-процессов, роботизация производств, интеграция различных устройств посредством мобильных сетей связи (так называемый «Интернет вещей», IoT – Internet of Things) – все это глобальные проявления внедрения современных информационных технологий. Они могут быть заметны не каждому, но каждый рядовой житель нашей страны так или иначе является частью этой интеграции. Развитие мобильных сетей передачи данных сделало максимально доступными ресурсы сети Интернет и повысило мобильность рядовых пользователей. Вкупе с появлением доступных мобильных устройств значительная часть рутинных операций повседневной жизни переместилась в онлайн-пространство. Отслеживание почтовых отправлений, покупка товаров на специализированных сайтах, оплата коммунальных счетов, перечисление денежных средств – эти и другие действия теперь не требуют от пользователя траты времени для визита в специализированную организацию. Мобильный телефон позволяет осуществить все эти операции за считанные минуты из любого места, где есть покрытие сотовой сети. Подобное положение дел выгодно и организациям, оказывающим различные услуги, в особенности банковскому сектору. Возможность клиента осуществлять элементарные транзакции без привлечения работников банков позволяет повысить оборачиваемость средств, значительно оптимизировать штат работников и сэкономить на открытии новых отделений. Однако не все радужно в таком перемещении онлайн – переместилась в сетевое пространство и преступность. Одним из распространенных преступлений в сфере информационных технологий с использованием мобильных устройств стали кражи денежных средств с банковских счетов

пользователей с использованием комплекса услуг «мобильный банк».

Для реализации кражи на мобильное устройство (преимущественно под управлением операционной системы Android) устанавливается вредоносное программное обеспечение (ПО), посредством которого происходит либо непосредственно сама кража денежных средств (перевод на банковский счет, счет мобильного телефона, электронный кошелек и т.д. злоумышленника), либо кража учетных данных пользователя мобильного банкинга. По данным компании «Group-IB», с июля 2015 г. по июнь 2016 г. рост количества украденных средств со счетов пользователей мобильного банкинга на базе ОС Android составил 450% к аналогичному периоду прошлых лет. И нет никаких предпосылок к снижению количества данных преступлений в дальнейшем.

При расследовании данного вида преступлений правоохранительные органы сталкиваются со следующими сложностями:

1) обращение в полицию по факту кражи происходит, как правило, через некоторое время после совершения кражи (в некоторых случаях – спустя месяцы);

2) особенности российского законодательства не позволяют правоохранительным органам оперативно получать необходимую для расследования информацию от банков, сотовых операторов, платежных систем и т.д.;

3) низкий уровень технической грамотности сотрудников правоохранительных органов, расследующих преступление, не всегда позволяет четко понять механизм преступления и выстроить адекватную стратегию расследования;

4) «география» преступления, как правило, выходит далеко за пределы региона нахождения потерпевшего;

5) низкий уровень взаимодействия правоохранительных органов из различных регионов;

6) отсутствие в ряде экспертных подразделений специализированных технических средств, а также специалистов с необходимыми навыками для исследования мобильных устройств;

7) частое отсутствие возможности проведения быстрого исследования мобильного устройства в экспертно-криминалистическом подразделении;

8) отсутствие централизованного подхода к расследованию данного вида преступлений.

Остановимся более подробно на каждом из пунктов.

При расследовании преступлений в сфере информационных технологий критическую важность имеет время реагирования на инцидент. IT-системы банков позволяют осуществлять транзакции в течение нескольких часов, поэтому для успешного расследования кражи крайне важно как можно более раннее обращение пострадавшего в правоохранительные органы. В силу специфики работы вредоносного ПО, осуществляющего хищение денежных средств, факт кражи не всегда сразу заметен пользователю (SMS о балансе карты скрываются от пользователя либо подменяются). Чем дольше не происходит обращения в правоохранительные органы, тем больше времени у преступников на обналичивание украденных средств и сокрытие следов преступления.

Даже после обращения пострадавшего в правоохранительные органы и возбуждения уголовного дела в силу принятого порядка расследования преступлений продолжается «потеря времени» на оформление запросов в банк, компанию оператора сотовой связи и т.д.

Стоит отметить, что дела о краже средств с использованием вредоносного ПО возбуждаются и принимаются к расследованию по месту обращения пострадавшего. Учитывая специфику распространения вредоносного ПО, злоумышленникам безразлично, на каком именно устройстве оно было установлено и где географически находится пострадавший. Главное требование – наличие подключенного на устройстве мобильного банкинга и доступ к сети Интернет. Часто дела возбуждаются и принимаются к расследованию в районных подразделениях полиции. И на этом

этапе географическое расположение пострадавшего уже играет значительную роль – во многих ли районных отделах полиции присутствуют следователи или дознаватели с пониманием технической стороны расследуемого преступления? А между тем стратегия расследования не может быть четко сформирована без знания технической стороны преступления.

Говоря о «географии» преступления, необходимо также отметить, что киберпреступления трансграничны и транснациональны. Установка вредоносного ПО происходит случайным образом. При этом средства со счетов пострадавших выводятся, как правило, в другие регионы страны, а обналичиваться могут в третьих регионах. Такой путь движения средств создает значительные проблемы следствию с точки зрения документального оформления преступления и негативно влияет на оперативность реагирования на инцидент и его расследование.

Как следствие вышеописанной «трансграничности» – проблема взаимодействия между правоохранительными органами разных регионов. Российская Федерация – страна огромных размеров, и средства, украденные с банковского счета потерпевшего в Амурской области, могут быть переведены на счет отделения банка из Подмосковья, а обналичены − через банкомат в Ленинградской области. Не всегда целесообразно направлять сотрудников в командировку к месту обналичивания денежных средств, а направленные в другие регионы поручения часто выполняются не на должном уровне.

Для установления механизма кражи следствию требуется проведение компьютерной экспертизы, в результате которой будут даны ответы на вопросы о наличии/отсутствии вредоносного ПО в операционной системе телефона, функциях данного ПО и произведенных им действиях. Поскольку мобильный телефон является самостоятельным классом устройств, доступ к содержащейся в его памяти информации получить возможно лишь с использованием специализированных программно-аппаратных комплексов (UFED, XRY); часто вредоносное ПО после совершения перевода денежных средств уничтожает следы своей деятельности, в этом случае от проводящего экспертизу специалиста требуются специальные познания в широком круге областей – от знания устройства и принципов работы мобильной операционной системы до восстановления информации и знания методик карвинга системной области памяти устройства на предмет наличия характерных для вредоносного ПО фрагментов. Возвращаясь к имеющимся реалиям, не все подразделения укомплектованы соответствующими техническими средствами и специалистами с нужным уровнем знаний.

Но даже если специалист соответствующей квалификации и необходимые технические средства имеются в региональном ЭКЦ, не всегда возможно провести исследование мобильного устройства в кратчайшие сроки. В соответствии с внутренними приказами МВД России исследования принимаются и исполняются в порядке принятия материалов. Кроме того, эксперты, обладающие специальными познаниями в области компьютерных технологий, часто привлекаются к дежурствам в составе следственно-оперативной группы в городских отделах полиции, а также к мероприятиям по охране общественного порядка, что является спорным решением с точки зрения эффективности использования высококвалифицированных узконаправленных специалистов. Таким образом, следствие не всегда имеет возможность оперативно получить необходимые для расследования данные.

Выше упоминалась так называемая «трансграничность» рассматриваемых преступлений. При этом одни и те же злоумышленники могут совершать кражи из любого региона страны. Логичным ответом на указанные особенности могла бы стать централизация расследования данных преступлений в едином подразделении, которое могло бы координировать работу региональных подразделений МВД России, вести аналитический учет совершенных преступлений, оперативно устанавливать и эф-

фективно пресекать каналы обналичивания денежных средств (в тесном сотрудничестве с подразделениями служб безопасности банков). При таком подходе от сотрудников правоохранительных органов в регионах потребовался бы минимальный набор необходимых познаний из сферы информационных технологий и выполнение ограниченного набора четко регламентированных действий по сбору первичной информации. В реальности же каждый регион вынужден сам вести весь комплекс мероприятий по расследованию данного типа преступлений.

Вышеописанные проблемы в той или иной степени характерны для всех регионов нашей страны. Киберпреступления – это преступления XXI в., а расследуются они по законам, развивавшимся и отточенным в XX в . Правоохранительная система ранее не сталкивалась ни с чем подобным. Стандартные методы оперативно-розыскной работы, непрерывно совершенствовавшиеся с момента появления в России полиции, не всегда подходят для расследования киберпреступлений. Кроме того, если злоумышленники могут моментально перестроиться под существующие условия, правоохранительная и законодательная системы обладают значительной инертностью. Все вышесказанное говорит о необходимости совершенствования всех аспектов правоохранительной деятельности и необходимости выработки гибких стратегий, применяемых при расследовании киберпреступлений.

Бердникова О.П.,

кандидат юридических наук
Уральский юридический институт
МВД России (г. Екатеринбург)

СЛОЖНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ ПОСЛЕДУЮЩЕГО ЭТАПА РАССЛЕДОВАНИЯ РАЗБОЕВ, СОВЕРШЕННЫХ ОРГАНИЗОВАННЫМИ ГРУППАМИ

По результатам анализа и оценки следственной ситуации, возникшей по окончании первоначального этапа расследования, определяется программа дальнейшего расследования разбоев, совершенных организованной группой. Последующий этап расследования нередко принимает комплексную (смешанную) структурную форму. После завершения первоначальных следственных действий и появления процессуальной фигуры подозреваемого (подозреваемых) задачи первоначального этапа считаются выполненными, однако подобная ситуация возникает далеко не по всем уголовным делам. Хотя информация, находящаяся в распоряжении следователя на последующем этапе, отличается более значительным объемом, большей логической упорядоченностью и доказательственной надежностью, чем на первоначальном этапе расследования, тем не менее число установленных криминальных эпизодов может быть значительно меньше, чем в действительности совершено соответствующей преступной организованной группой. Кроме того, нередко остаются не выявленными виновные лица не только по «новым», еще неизвестным эпизодам разбоев и грабежей, но и по «старым», уже установленным и доказанным эпизодам. Указанный ранее фактор повышенной латентности и другие негативные обстоятельства нередко приводят к таким недоработкам следствия и органов дознания, как неустановление всех эпизодов преступной деятельности и невыявление всех членов организованной группы, что, в свою очередь, обуславливает возможность продолжения совершения разбойных нападений оставшимися на свободе преступниками.

Анализ следственной и судебной практики по исследуемой категории уголовных дел позволил выделить следующие простые и сложные ситуации последующего этапа расследования.