Министерство внутренних дел Российской Федерации
Нижегородская академия

Д.В. Климов

РАССЛЕДОВАНИЕ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Учебное пособие

Нижний Новгород
НА МВД России
2017

УДК 343.132
ББК 67.410.212.2
К49

Рецензенты:
С.А. Мельникова
(отдел по расследованию преступлений в сфере высоких технологий и компьютерной информации СЧ ГСУ ГУ МВД России по Нижегородской области);
С.А. Арефьев
(отдел по расследованию организованной преступной деятельности в сфере экономики СЧ ГСУ ГУ МВД России по Нижегородской области)

Климов Д.В.

К49 Расследование хищений, совершенных с использованием сети «Интернет»: учебное пособие / Д.В. Климов. – Н. Новгород: Нижегородская академия МВД России, 2017. – 25 с.

Учебное пособие подготовлено на основе действующего уголовно-процессуального законодательства с учетом современной следственной и судебной практики.

В пособии автором приводится краткая характеристика основных видов хищений, совершаемых с использованием сети «Интернет». Дано описание действий следователя при расследовании уголовных дел о хищениях, совершенных с использованием сети «Интернет», в том числе о хищениях, совершенных с использованием поддельных платежных карт.

Пособие предназначено для курсантов и слушателей образовательных организаций системы МВД России, практических сотрудников органов предварительного расследования.

Печатается по решению редакционно-издательского совета
Нижегородской академии МВД России

ОГЛАВЛЕНИЕ

Введение 4

1. Современные виды хищений, совершаемых с использованием сети «Интернет 6

2. Алгоритм расследования преступлений о хищениях, совершаемых с использованием сети «Интернет» 9

3. Алгоритм расследования преступлений о хищениях, совершаемых с использованием поддельных платежных карт 15

Рекомендуемая литература 23

ВВЕДЕНИЕ

Особенностью существующего в настоящее время финансового рынка России является значительное увеличение расчетов, проводимых в безналичной форме, с использованием денежных средств, содержащихся на расчетных картах или электронных счетах. Параллельно с развитием платежных систем и сети «Интернет» растет количество хищений электронных денежных средств. Способы совершения рассматриваемых преступлений постоянно видоизменяются и совершенствуются, что вызывает озабоченность у представителей правоохранительных органов и населения страны в целом.

Так, начальник Бюро специальных технических мероприятий (БСТМ) МВД России Алексей Мошков, выступая на VI Международном форуме «Борьба с мошенничеством в сфере высоких технологий. AntifraudRussia – 2015», указал, что сотрудниками Управления «К» МВД России предотвращены интернет-хищения на сумму более полутора миллиардов рублей, задержаны участники десятков организованных преступных групп[1].

Борьба с преступлениями, совершенными с использованием современных информационных технологий, является задачей не только органов внутренних дел, но и всей правоохранительной системы государства. На Координационном совещании руководителей правоохранительных органов РФ в 2016 году с участием представителей администрации Президента РФ, Генеральной прокуратуры РФ, МВД России, ФСБ России, СК России, ФССП России, Роскомнадзора, Центрального Банка, Росфинмониторинга Генеральный прокурор РФ Юрий Чайка сообщил, что количество киберпреступлений, зарегистрированных в 2015 году, составило 44 тыс., что в четыре раза превышает показатели 2014 года. При этом сумма доказанного ущерба от подобных преступлений составила почти 6 млрд рублей. Наибольшее число киберпреступлений составляют кражи и мошенничества (около 23 тыс.). Также Генеральный прокурор отметил, что деятельность правоохранительных органов не отвечает современным угрозам, которые несет в себе киберпреступность, неудовлетворительным остается уровень следственной работы по подобным уголовным делам[2].

---

[1] Алексей Мошков принял участие в открытии VI Международного форума «Борьба с мошенничеством в сфере высоких технологий. AntifraudRussia – 2015». URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/7126771/ (дата обращения: 02.10.2016).

[2] Ущерб от киберпреступлений в России составил почти шесть миллиардов рублей. URL: https:/ ria.ru/incidents/20160923/1477709423.html (дата обращения: 11.10.2016).

Не только правоохранительные органы и специальные службы государства, но и коммерческие организации отмечают огромный размер ущерба, причиняемого российской экономике киберпреступностью. По данным исследования, проведенного компанией Group-IB, Фондом развития интернет-инициатив (ФРИИ) и корпорацией Microsoft в 2015 году экономике России такими преступлениями нанесен ущерб в 203,3 млрд руб. или 0,25% объема ВВП. Причем киберпреступность наносит ущерб не только крупным банковским и кредитным учреждениям (рост на 300% в 2016 году до 2,5 млрд рублей), но и физическим лицам (только посредством использования вредоносного программного обеспечения для мобильных платформ Android около 350 млн рублей)[1].

Настоящее учебное пособие имеет своей целью раскрытие информации об основных видах и особенностях расследования хищений, совершенных с использованием сети «Интернет», что позволит курсантам и слушателям сформировать необходимую систему знаний для успешного изучения курса «Расследование преступлений в сфере компьютерной информации», а также осуществления правоприменительной деятельности.

[1] Киберпреступность и киберконфликты: Россия. URL: https://clck.ru/AGUsK (дата обращения: 10.10.2016).

1. Современные виды хищений, совершаемых с использованием сети «Интернет»

Первая группа преступлений – это мошенничества, при которых потерпевшее лицо добровольно передает принадлежащие ему денежные средства лицу, совершающему преступление, в счет приобретения какого-либо товара, оказания услуг или выполнения работ. Основными площадками для совершения такого рода хищений являются различные интернет-магазины, интернет-аукционы, интернет-казино, интернет-сайты по обмену электронных платежных средств и так далее. Как правило, такие деяния квалифицируются по ст. 159 УК РФ.

Подобный вид хищений ярко демонстрирует следующий пример из следственной практики: сотрудниками подразделения «К» БСТМ МВД России была задержана жительница г. Москвы по подозрению в совершении мошеннических действий. По результатам доследственной проверки принято решение о возбуждении уголовного дела по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ. В ходе расследования уголовного дела установлено следующее: виновная, вступая в электронную переписку с потерпевшими, под видом трудоустройства на высокопоставленные должности в федеральные органы власти без прохождения установленных процедур путем обмана осуществляла хищения принадлежащих им денежных средств. Суммы хищений составляли более 100 тыс. рублей, похищенные денежные средства перечислялись на банковские счета и электронные кошельки[1].

Приведем еще один пример из следственной практики, который можно смело отнеси к категории «классических» мошенничеств, совершаемых с использованием сети «Интернет». Сотрудниками отдела «К» УМВД России по Ярославской области задержан мужчина, который на сайтах бесплатных объявлений в сети «Интернет» размещал информацию о продаже компьютерной техники. В ходе переписки с потерпевшими, осуществляемой посредством социальных сетей, мужчина представлял о себе подложные сведения и предлагал для оплаты товаров перевести денежные средства на платежные карты, которые были оформлены на подставных лиц. После получения денежных средств в счет оплаты товаров преступник прерывал с потерпевшими общение, не исполняя свои обязанности по поставке товаров. От действий виновного пострадали жители нескольких регионов РФ[2].

---

[1] Сотрудники Управления «К» МВД России пресекли деятельность мошенницы, представлявшейся сотрудницей органов государственной власти. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/8780631/ (дата обращения: 21.10.2016).

[2] В Ярославской области вычислили подозреваемого в мошенничестве в сети «Интернет». URL: https://xn--b1aew.xn-p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/8144230/ (дата обращения: 01.10.2016).

Вторая группа – это хищения электронных денежных средств, находящихся в принадлежащих потерпевшему электронных кошельках или на виртуальных расчетных счетах, совершенные путем их взлома, осуществляемого посредством использования вирусного программного обеспечения, взломщиков электронных кошельков, фишинговых сайтов, сайтов-клонов и др. Такие деяния, в зависимости от конкретного способа их совершения, квалифицируются по ст. 158 УК РФ либо по ст. 159^6 УК РФ.

Так, например, в производстве следственных подразделений органов внутренних дел по г. Сочи находится уголовное дело в отношении 23-летнего гражданина РФ по обвинению в совершении преступления, предусмотренного ст. 159^6 УК РФ. В ходе расследования уголовного дела установлено, что виновный внедрил в систему дистанционного банковского обслуживания одной из кредитных организаций вирусную программу, предоставившую ему возможность доступа к удаленному управлению расчетными счетами клиентов организации. Используя вредоносную программу, виновный похитил с одного из расчетных счетов денежные средства на сумму более 1,5 млн рублей[1].

Часто для совершения подобных преступлений используется создание так называемых «бот-сетей» посредством заражения вредоносным программным обеспечением большого количества компьютерной техники ничего не подозревающих граждан. Например, в 2016 году сотрудниками МВД России совместно с ФСБ России задержаны около 50 членов преступного сообщества, которые совершили хищения денежных средств с расчетных счетов юридических лиц, используя вредоносное программное обеспечение на сумму около 2,5 млрд рублей.

В ходе расследования уголовного дела, находящегося в производстве Следственного департамента МВД России, было произведено более 80 обысков на территории 15 субъектов РФ, огромное количество иных следственных действий. В ходе обысков изъято большое количество компьютерной и иной специализированной техники, электронных носителей информации, по которым проводятся компьютерно-технические судебные экспертизы. Кроме того, в период с 2015 года по настоящее время подобными преступлениями причинен ущерб на сумму около 3 млрд рублей[2].

Третья группа преступлений – это хищения, совершаемые под угрозой распространения информации, которая компрометирует потерпевших.

---

[1] В Сочи расследовано дело в отношении компьютерного мошенника. Информация официального сайта МВД России. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Departamenti/Sledstvennij_departament/NovostiSD/item/7917634/ (дата обращения: 10.09.2016).

[2] Сотрудники МВД России и ФСБ России задержали интернет-хакеров. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/7883879/ (дата обращения: 15.09.2016).

Для иллюстрации приведем пример из практики УМВД России по Смоленской области.

Как было установлено в ходе расследования, виновные лица создавали на сайтах знакомств «фейковые» страницы от имени молодых девушек, после чего вступали в переписку с мужчинами. В ходе общения они узнавали контактные данные потерпевших, в том числе номера мобильных телефонов. После этого потерпевшему поступали звонки от имени следователя органов внутренних дел, который сообщал им о том, что девушка, с которой велась переписка, является несовершеннолетней (14 или 15 лет) и ее родители обратились с заявлением в полицию. «Следователь» разъяснял потерпевшим возможность привлечения к уголовной ответственности за развратные действия в отношении несовершеннолетних по ст. 135 УК РФ, но выражал понимание и предлагал мирно урегулировать проблему, предоставляя номер якобы родителей девушки. В ходе общения с преступниками, представлявшимися родителями несовершеннолетней девушки, потерпевшим предлагалось выплатить около 50 тыс. рублей или более для прекращения уголовного дела. После перечисления денежных средств связь с потерпевшими прерывалась.

Жертвами злоумышленников, причастных к совершению шести эпизодов преступной деятельности, становились взрослые женатые мужчины, которые опасались распространения информации, порочащей их честь и достоинство. Это обстоятельство позволило виновным на протяжении длительного периода времени избегать привлечения к ответственности за совершение преступлений[1].

Указанный перечень хищений не является исчерпывающим, появляются все новые и более изощренные их способы, в частности:

– совершенные в сфере интернет-знакомств, так называемые «брачные аферы»;

– использование сайтов, созданных с ложной благотворительной целью, например под видом необходимости содержания приюта для животных или лечения детей;

– рассылки электронных писем с сообщениями о несуществующих выигрышах в лотереи, для получения которых необходимо произвести затраты денежных средств;

– рассылки электронных писем с сообщениями о несуществующих правах наследства, например так называемые «нигерийские письма счастья», для вступления в которые необходимо затратить определенную сумму денежных средств;

[1] Сотрудники отдела «К» в Смоленске задержали подозреваемых в мошенничестве. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/8138716/ (дата обращения: 20.09.2016).

– клонирование платежных карт;

– клонирование сим-карт и т. д.

Таковы основные виды хищений, совершаемых с использованием сети «Интернет».

2. Алгоритм расследования преступлений о хищениях, совершаемых с использованием сети «Интернет»

Анализ сложившейся следственно-судебной практики показывает, что организация эффективного расследования рассматриваемых категорий хищений возможна при выполнении определенного алгоритма действий, который будет изложен ниже.

1. Выполнить комплекс процессуальных действий с заявителем:

– незамедлительно после принятия решения о возбуждении уголовного дела вынести постановление о признании потерпевшим;

– допросить потерпевшего об обстоятельствах хищения принадлежащих ему денежных средств с указанием того, какие именно действия были выполнены им лично, с какой целью, с использованием какой техники и программного обеспечения, предоставлялись ли им кому-либо сведения о себе, по каким адресам в сети «Интернет» он обращался, на какие именно электронные кошельки, расчетные счета производил перечисления денежных средств, с использованием каких сервисов осуществлялась коммуникация с лицом, совершившим преступление;

– получить исковое заявление, вынести постановление о признании гражданским истцом;

– в случаях наличия у потерпевшего документов, подтверждающих факт совершения хищения (платежных поручений, приходных кассовых ордеров, скриншотов, фиксирующих перевод денежных средств в платежных системах), и/или документов, отражающих переписку потерпевшего с лицом, совершившим преступление (чаще всего скриншоты экрана с перепиской в социальных сетях или посредством электронной почты), вынести постановление о производстве их выемки, изъять в установленном порядке;

– провести осмотр компьютерной техники потерпевшего, в ходе которого фиксировать сведения, имеющие доказательственное значение (переписка с лицом, совершившим преступление, сведения о переводе средств в электронных платежных системах). Целесообразно оформлять приложения к протоколу следственного действия в виде скриншотов экрана компьютера (с целью обеспечения наглядности);

– принять решение о признании и приобщении к материалам уголовного дела в качестве вещественных доказательств изъятых предметов и документов.

2. Установить местонахождение электронно-вычислительной техники, которая использовалась в качестве орудия преступления. Это является самым главным элементом в доказывании по уголовным делам о хищениях, совершаемых с использованием интернет-технологий. Посредством такой техники лица, совершающие преступления, осуществляют управление электронными виртуальными счетами различных платежных систем или ведут переписку с потерпевшими.

С этой целью необходимо получить сведения о движении денежных средств в кредитной организации или у оператора платежной системы на основании запроса следователя, согласованного с руководителем следственного органа (в соответствии с требованиями ст. 26 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»[1] и ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»[2]).

Кроме того, на основании запросов в обозначенные организации необходимо получить сведения, указанные владельцем счета при его регистрации, и сведения об IP-адресах регистрации и доступа к счету.

В случаях перемещения похищенных денежных средств с использованием платежных систем, операторами которых являются юридические лица, зарегистрированные за пределами России, следует в установленном порядке направить запрос об оказании международно-правовой помощи;

– направить запросы в организации, которым принадлежат сайты социальных сетей, почтовых сервисов, с целью установления сведений о лице, которому принадлежит определенный идентификатор, логин, никнейм, почтовый ящик. В таком запросе нужно указать на необходимость предоставления не только сведений, указанных лицом при регистрации, но и сведений об IP-адресах регистрации и доступа к определенному ресурсу;

– полученную на основании вышеуказанных запросов информацию об IP-адресах проверить посредством открытого интернет-сервиса, расположенного по адресу: https://www.ripe.net/, или любого другого схожего с ними по функциональности сервиса, позволяющих установить принадлежность IP-адреса конкретному провайдеру;

– на основании судебного решения в соответствии с положениями ст. 53 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[3] произвести выемку сведений об абонентах в организации-провайдере, которой принадлежат интересующие следствие IP-адреса. Изъятию подлежат следующие сведения об абоненте: фамилия, имя, отчество; номер договора о

[1] Российская газета. 2011. 30 июня.
[2] Собрание законодательства РФ. 1996. № 6, ст. 492. Все нормативные правовые акты см. с изм. и доп.
[3] Российская газета. 2003. 10 июля.

предоставлении услуги доступа в сеть «Интернет»; фактический адрес (город, улица, дом, квартира).

Полученные из компании-провайдера сведения укажут, что именно с компьютерной техники конкретного абонента, находящейся по конкретному адресу, осуществлялись онлайн-транзакции, велась переписка и т. д.

3. Получить информацию о собственниках объекта недвижимости, где находится электронно-вычислительная техника – орудие преступления.

4. В установленном законом порядке произвести обыск в жилище с участием специалиста в области компьютерных технологий (сотрудников ЭКЦ, специализирующихся на производстве компьютерно-технических экспертиз или сотрудников Центра информационных технологий, связи и защиты информации (ЦИТС и ЗИ) ГУ МВД России по субъектам РФ). В ходе обыска обязательному изъятию подлежат следующие предметы и документы:

– компьютерная техника, электронные носители информации;

– документы, отражающие факты выдачи денежных средств;

– средства, предназначенные для защиты информации;

– свободные образцы почерка и подписи, содержащиеся в письмах, личных дневника, записных книжках, и т. д.;

– машинописные тексты;

– литература, содержащая сведения, которые относятся к этапам подготовки, совершения и сокрытия хищений денежных средств с использованием сети «Интернет»;

– фотографии, видеозаписи (особенно важно их изъятие при расследовании преступлений, совершенных организованными группами в целях доказывания наличия устойчивых межличностных связей между их участниками);

– иные предметы и документы, имеющие доказательственное значение.

5. Допросить в качестве подозреваемого лицо, совершившее преступление, выяснив у него:

– насколько он хорошо владеет навыками обращения с компьютерной техникой и программным обеспечением;

– имеется ли компьютерная техника по месту проживания и по месту работы, кто имеет доступ к пользованию ей, выяснить ее технические характеристики;

– перечень конкретных операций с компьютерной информацией, которые подозреваемый выполняет на своем рабочем месте;

– как часто осуществляет выход в Интернет, наиболее часто посещаемые ресурсы;

– каким интернет-браузером пользуется при осуществлении выхода в Интернет, каковы его настройки (сохраняются ли история посещений, cache-память, cookie-файлы и т. п.);

– установлены ли на компьютере антивирусные или защитные программы, если да, выяснить их наименование;

– имеются ли у него электронная почта, сайты, домашние страницы, каковы их реквизиты;

– каким образом настроен удаленный доступ к сети для выхода в Интернет (кто и когда производил настройку);

– каким образом взломана информационная защита компьютера потерпевшего: подбор или хищение ключей и паролей; отключение средств защиты; разрушение средств защиты; использование несовершенства защиты;

– знаком ли он с потерпевшим, если да, то с какого времени, в каких отношениях состоит;

– имеет ли он источник дохода, если да, уточнить его размер;

– имеются ли у него, его родственников, друзей счета в банках, электронные кошельки в платежных системах, как давно открыты, как часто пользуется этими счетами;

– поступали ли на указанные счета денежные средства, если да, то когда именно, от каких лиц, за какие услуги;

– осуществлял ли за конкретный период времени денежные переводы, в случае если осуществлял, то указать реквизиты денежного перевода;

– осуществлял ли за последнее время крупные покупки, если да, то когда именно, в какой период времени, каким способом производил оплату, имеются ли документы, подтверждающие факт покупки;

– имели ли место встречи с потерпевшим лично либо посредством видеосвязи (видеозвонки по мобильным устройствам, Skype и т. д.), если да, выяснить дату, время, место, цель встречи.

6. С учетом материалов уголовного дела избрать меру пресечения в отношении подозреваемого.

7. Произвести сбор материала, характеризующего личность подозреваемого.

8. Назначить по изъятой компьютерной технике и электронным носителям информации судебную экспертизу с целью выяснения следующих основных вопросов:

– имеются ли на предоставленном на исследование носителе информации сведения о сетевых соединениях в сети «Интернет» за период времени с (дата) по (дата) включительно?

– имеются ли на представленном на исследование носителе информации программы, которые определяются антивирусным программным обеспечением как «вредоносные»? Если да, то какие у них функциональные возможности, сетевые взаимодействия, способ проникновения и следы работы в системе?

– какие программы установлены в автозагрузку в оперативной системе на предоставленном на исследование носителе информации?

– имеются ли на представленном на исследование носителе информации компьютерные программы или другая компьютерная информация, которые имеют функциональные возможности скрытно от пользователя копировать информацию, необходимую для аутентификации в операционной системе, но при этом не являются компонентом операционной системы? Если да, то какие у них функциональные возможности, сетевые взаимодействия, способ проникновения в систему и следы работы в системе?

– имеются ли на представленном на исследование носителе информации средства удаленного администрирования и управления компьютером?

– имеются ли на представленном на исследование носителе информации сведения о логинах и паролях доступа к интернет-ресурсам, установленным программам, интернет-кошелькам, системам дистанционного банковского обслуживания и т. д.? Если да, то какие?

– имеются ли на представленном на исследование носителе информации сведения о человеке с ФИО (доступ к социальным сетям, переписка, паспортные данные и т. д.)? Если да, то каковы атрибуты соответствующих файлов, их содержащих?

– имеются ли в дампе оперативной памяти сведения о запущенных процессах, сетевых соединениях? Если да, то какие?

– имеются ли в дампе сетевого трафика сетевые соединения от/к следующим IP-адресам (перечисление IP-адресов)?

– имеется ли на машинных носителях информации представленных на исследование объектов программное обеспечение, позволяющее пользоваться услугами электронной почты? Если да, то какое программное обеспечение (название, версии)?

– имеются ли на машинных носителях информации файлы, содержащие электронные почтовые сообщения? О каких электронных почтовых ящиках имеются сведения на представленном на исследование системном блоке?

– имеется ли на машинных носителях информации представленных на исследование объектов программное обеспечение, позволяющее пользоваться услугами мгновенного обмена сообщениями в сети «Интернет»? Если да, то какое программное обеспечение (название, версии)?

– имеются ли на машинных носителях информации представленных на исследование объектов в обнаруженных программах для мгновенного обмена сообщениями следы переписки в сети «Интернет» с другими абонентами? Если да, то какие именно?

– какие mac-адреса имеет сетевое оборудование представленных на экспертизу объектов?

В случаях, когда в ходе производства экспертизы необходимо устанавливать наличие переписки, содержащейся в файлах различных мессенджеров или электронной почты, а также ее содержание, рекомендуется

перед ее началом получить постановление суда о разрешении производства осмотра корреспонденции. Получение указанного судебного решения будет в полной мере соответствовать уголовно-процессуальному принципу тайны переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений и гарантирует соблюдение соответствующего конституционного права.

9. Принять меры к установлению имущества подозреваемого, принадлежащих ему денежных средств, в том числе находящихся на расчетных счетах и в электронных кошельках, на которые для возмещения ущерба и обеспечения гражданского иска необходимо наложить арест на основании судебного решения в порядке ст. 115 УПК РФ.

Дальнейшее планирование и производство предварительного расследования по уголовным делам о хищениях, совершенных с использованием сети «Интернет», должно осуществляться исходя из доказательственной базы, собранной в рамках выполнения изложенного выше алгоритма.

Дополнительно укажем, что в случаях, когда для совершения преступления использовались сайты-однодневки или фишинговые сайты, следователю необходимо:

– направить поручение в подразделения «К» БСТМ регионального органа внутренних дел с целью установления организации – хостинг-провайдера, а также регистратора доменных имен;

– направить запрос в установленные компании с целью установления сведений о лице, зарегистрировавшем сайт (обратившегося за предоставлением услуг хостинга) с указанием IP-адресов обращения, администрирования, сведений о способах оплаты услуг с указанием номеров счетов или электронных кошельков;

– в последующем необходимо выполнить действия, указанные в основном алгоритме расследования.

Отметим проблему, встречающуюся при расследовании рассматриваемой категории уголовных дел, даже с учетом выполнения приведенного выше алгоритма. Этой проблемой является использование преступниками прокси-серверов. Сущность ее заключается в следующем: лица, совершающие преступления, производят все операции с подконтрольными им счетами и аккаунтами с использованием специализированного программного обеспечения, позволяющего производить обращение к ресурсам через сервера, расположенные за территорией России. В таком случае операторы ресурса в сети «Интернет» фиксируют IP-адрес прокси-сервера, а не лица, отправившего конкретную команду. Выходом из подобной ситуации является направление запроса об оказании правовой помощи в страну, в которой зарегистрирован провайдер, с IP-адреса которого передана команда на проведение операции, с целью выяснения сведений об IP-адресе обращения к серверу, который может быть истинным адресом преступника.

3. Алгоритм расследования преступлений о хищениях, совершаемых с использованием поддельных платежных карт

Как уже отмечалось, активное развитие информационной коммуникации, а также увеличение объема расчетов в России, проводимых с использованием платежных карт, обусловливают рост количества хищений, совершаемых посредством вышеуказанных средств платежа.

Способы совершения рассматриваемых преступлений постоянно видоизменяются и совершенствуются. При этом наиболее изощренным способом совершения преступления является создание поддельных платежных карт (карт-клонов) с использованием информации о реально существующей карте конкретного лица. Подобная информация получается преступниками в ходе использования фишинговых сайтов, скиммингового оборудования, а также атак на процессинговые центры кредитных организаций или платежных систем.

Анализ следственно-судебной практики позволил выработать алгоритм действий сотрудников следственных подразделений МВД России по эффективному расследованию хищений, совершаемых с использованием поддельных платежных карт, который будет изложен ниже.

1. Выполнить комплекс процессуальных действий с заявителем:

А. После принятия процессуального решения о возбуждении уголовного дела необходимо незамедлительно вынести постановление о признании заявителя потерпевшим в случае, когда известны данные о его личности, либо незамедлительно после установления сведений о личности потерпевшего.

Б. Допросить потерпевшего об обстоятельствах хищения принадлежащих ему денежных средств. В ходе допроса необходимо выяснить:

– когда и как были обнаружены признаки хищения;

– предпринимались ли им после этого какие-либо действия;

– какие события предшествовали совершению преступления. В рамках раскрытия этого вопроса необходимо подробно выяснить, сообщал ли потерпевший кому-либо сведения о своей платежной карте (ее номер, срок действия, информацию о держателе, трехзначный код проверки подлинности платежной карты), производил ли оплату товаров, работ, услуг на каких-либо сайтах в сети «Интернет» либо в других организациях, реализующих товары, оказывающих услуги или выполняющих работы (магазины, кафе и рестораны, заправочные станции, гостиницы и т. д.). Если будут установлены подобные факты, у потерпевшего нужно выяснить всю информацию, касающуюся передачи сведений о своей платежной карте, в том числе с какого номера приходили СМС-сообщения, на какие номера перезванивал, с кем общался, описание голоса и т. д.;

– имеются ли у него документы о получении платежной карты, а также иные документы, подтверждающие совершение преступления (в том числе скриншоты, на которых зафиксированы действия по совершению транзакций);

– точный размер причиненного преступлением ущерба. При этом необходимо также выяснить, является ли для потерпевшего причиненный ущерб значительным, если да, то необходимо выяснить размер его доходов, доходов семьи, наличие кредитных или иных имущественных обязательств, наличие иждивенцев;

– имеется ли у потерпевшего в распоряжении платежная карта, со счета которой было совершено хищение, не была ли эта карта утрачена, если да, то при каких обстоятельствах и где;

– передавалась ли платежная карта кому-либо ранее, если да, то кому именно, где, при каких обстоятельствах, под каким предлогом, на какой срок;

– оставлял ли потерпевший принадлежащую ему платежную карту где-либо без присмотра, если да, то где именно, когда, при каких обстоятельствах, на какой срок, кто имел доступ к месту, где карта была оставлена;

– где именно располагаются банкоматы, в которых потерпевший производил снятие денежных средств с использованием платежной карты, были ли случаи отказов в выдаче денежных средств без видимой на то причины (например, сумма денежных средств на карте явно была больше запрошенной к выдаче, однако банкомат не выполнил операцию, указав при этом на недостаток средств на счете).

В. Получить исковое заявление, вынести постановление о признании гражданским истцом.

Г. В случаях наличия у потерпевшего платежной карты, документов, подтверждающих факт совершения хищения (платежных поручений, приходных кассовых ордеров, кассовых чеков, скриншотов, фиксирующих осуществление транзакций), и/или документов, отражающих переписку потерпевшего с лицом, совершившим преступление (чаще всего скриншоты экрана с перепиской в социальных сетях или посредством электронной почты), вынести постановление о производстве их выемки, изъять в установленном порядке.

Д. Провести выемку, а затем осмотр компьютерной техники и средств мобильной связи потерпевшего, в ходе которого фиксировать сведения, имеющие доказательственное значение (переписка с лицом, совершившим преступление, сведения о передаче информации о платежной карте или совершении транзакций с ее использованием), желательно оформлять приложениями к протоколу следственного действия в виде скриншотов экрана компьютера или телефона (с целью обеспечения наглядности).

Е. Принять решение о признании и приобщении к материалам уголовного дела в качестве вещественных доказательств изъятых предметов и документов, при необходимости вернуть их часть потерпевшему.

2. Получить сведения о движении денежных средств в кредитной организации, эмитировавшей платежную карту, на основании запроса следователя, согласованного с руководителем следственного органа в соответствии с требованиями ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности».

Такой запрос позволит получить информацию о том, снимались ли денежные средства из принадлежащих конкретному банку банкоматов или осуществлялись ли неудачные попытки снятия денежных средств с использованием определенной платежной карты. В запросе необходимо указывать номер платежной карты, точный период времени, за который необходимо предоставить информацию, территорию осуществления операций. Путем направления подобного запроса можно выяснить, имеется ли запись камер видеонаблюдения банкоматов, в которых осуществлялись операции по поддельным платежным картам, что значительно облегчит мероприятия по их изъятию. При установлении факта наличия видеозаписи банкомата необходимо произвести ее изъятие в ходе выемки.

3. Если будет установлено, что банкомат располагался в специализированной зоне торговых центров, гостиниц или вокзалов, то необходимо получить сведения от администрации соответствующей организации о том, ведется ли за ним видеонаблюдение. При установлении факта наличия видеозаписи необходимо произвести ее изъятие в ходе выемки.

Аналогичные действия необходимо произвести в тех случаях, когда с использованием поддельных платежных карт было произведено не снятие наличных денежных средств из банкоматов, а приобретение товаров или оплата услуг посредством POS-терминалов.

4. Произвести осмотр видеозаписей, принять решение о признании и приобщении их к уголовному делу в качестве вещественных доказательств.

5. В случаях необходимости произвести выемку в банках с целью изъятия документов, содержащих сведения, составляющие банковскую тайну (на основании судебного решения), например заявлений об открытии счета, на получение платежной карты и т. д.

Также выемка платежных документов может быть проведена в организациях, в которых было произведено приобретение товаров или осуществлена оплата услуг посредством POS-терминалов.

6. Направить поручение в орган дознания с целью установления личности преступника, осуществлявшего снятие денежных средств с использованием поддельной платежной карты. К поручению обязательно приложить изъятые видеозаписи.

7. Получить информацию о собственниках объекта недвижимости, где проживает лицо, причастность которого к совершению преступления установлена органом дознания.

8. В установленном законом порядке произвести обыск в жилище с участием специалиста в области компьютерных технологий (сотрудников ЭКЦ,

специализирующихся на производстве компьютерно-технических экспертиз или сотрудников ЦИТС и ЗИ ГУ МВД России по субъектам РФ. В ходе обыска обязательному изъятию подлежат следующие предметы и документы:

• средства подготовки, совершения либо сокрытия преступления. К данной категории объектов можно отнести материалы и приспособления, которые были использованы для изготовления поддельных платежных карт, а именно: прессы, эмбоссеры, принтеры для печати по пластику, устройства чтения и записи информации на магнитную полосу карты (например, энкодерыCipher MSR различных моделей), голограммы, средства связи и любая электронно-вычислительная техника. Отметим, что необходимо изымать все виды вычислительной техники и носителей информации, так как информация, используемая для создания поддельных платежных карт, может храниться в цифровом виде на носителях, содержащихся в персональных компьютерах, ноутбуках, нетбуках, планшетных компьютерах, MP-3 плеерах, цифровых фотоаппаратах, смартфонах и т. д.;

• поддельные платежные карты, технические средства, предназначенные для незаконного получения компьютерной информации, в том числе скиммеры;

• литература, содержащая сведения, которые относятся к этапам подготовки, совершения и сокрытия хищений денежных средств с использованием поддельных платежных карт;

• свободные образцы почерка и подписи, содержащиеся в письмах, личных дневниках, записных книжках и т. д.;

• похищенные денежные средства, товары, приобретенные с использованием поддельных платежных карт, документы и предметы, свидетельствующие о месте хранения похищенных денежных средств и товаров (пластиковые карты, сберкнижки, ключи от камер хранения и банковских ячеек, квитанции о денежных переводах);

• фотографии, видеозаписи (особенно важно их изъятие при расследовании преступлений, совершенных организованными группами, в целях доказывания наличия устойчивых межличностных связей между их участниками);

• документы, отражающие факты выдачи денежных средств с использованием поддельных платежных карт либо приобретения товаров;

• средства, предназначенные для защиты информации;

• иные предметы и документы, имеющие значение для доказывания.

9. Допросить в качестве подозреваемого лицо, совершившее преступление, выяснив у него:

– место его жительства, род деятельности по основной и дополнительной работе, уровень образования, в каких организациях и на каких должностях работал ранее, уровень владения компьютерной техникой и знаний о технологии производства и использования платежных карт;

– если поддельная платежная карта была изготовлена самостоятельно, то необходимо выяснить, где приобреталась пустая заготовка карты («белый

пластик»), с использованием какой техники и какого программного обеспечения производилась запись информации на магнитную полосу карты, где, когда и при каких обстоятельствах такая техника и программное обеспечение были приобретены. Отдельно необходимо выяснить источник происхождения информации, которая была занесена на магнитную полосу поддельной платежной карты (установка скимминговых устройств, хакерские атаки, покупка у других лиц, в том числе с использованием сети «Интернет», и т. д.);

– если платежная карта была изготовлена иным лицом, то необходимо выяснить, где, когда, от кого и при каких обстоятельствах она была передана подозреваемому;

– сведения о местах хранения материалов, техники и информации, предназначенных для создания поддельных платежных карт;

– какие именно действия были осуществлены подозреваемым с поддельными платежными картами, точные суммы денежных средств, полученных с их использованием, описание товаров или услуг, которые были оплачены с использованием такой карты;

– где хранятся денежные средства или иные материальные ценности, полученные в ходе совершения преступления;

– совершались ли им ранее подобные действия, если да, то где, когда, при каких обстоятельствах, в каких размерах, были ли у него соучастники;

– наличие соучастников, виды осуществления коммуникации между ними в ходе совершения преступления (номера телефонов, электронные почтовые ящики, мессенджеры).

При получении ответов подозреваемого лица на вышеуказанные основные вопросы следователь должен самостоятельно определить перечень дополнительных вопросов исходя из полученной информации и имеющейся доказательственной базы.

10. С учетом материалов уголовного дела избрать меру пресечения в отношении подозреваемого.

11. Произвести сбор материала, характеризующего личность подозреваемого.

12. Назначить по изъятой компьютерной технике и электронным носителям информации судебную экспертизу с целью выяснения следующих основных вопросов:

– имеются ли на машинных носителях информации представленных на исследование объектов сведения о номерах платежных карт и пин-кодов к ним, которые возможно использовать для записи на пластиковые карты с магнитной полосой, если да, то какие именно и где они располагаются?

– имеются ли на машинных носителях информации представленных на исследование объектов следы доступа к интернет-ресурсу (указывается интересующий мессенджер, форум, блог и т. д.), какие именно, можно ли получить доступ к переписке, если да, то приобщить переписку с указанием «ников» участников общения;

– имеются ли на машинных носителях информации представленных на исследование объектов следы работы считывателей магнитных карт (например, наличие драйверов)?

– работоспособен ли представленный для исследования считыватель магнитных карт, каковы его технические характеристики и предназначение?

В случаях, когда в ходе производства экспертизы необходимо устанавливать наличие переписки, содержащейся в файлах различных мессенджеров или электронной почты, а также ее содержание, рекомендуется перед ее началом получить постановление суда о разрешении производства осмотра корреспонденции.

Для исследования изъятых поддельных платежных карт также возможно назначение судебной экспертизы с целью установления:

- какая именно информация содержится на магнитной полосе и в памяти чипа (микропроцессора) платежной карты, представленной на исследование;
- производилась ли перезапись (модификация, уничтожение, блокирование) компьютерной информации, содержащейся на магнитной полосе платежной карты или в памяти чипа;
- какая именно информация была удалена, скопирована, модифицирована, как изменялось ее содержание, время осуществления указанных действий;
- соответствует ли информация, записанная на магнитной полосе платежной карты, элементам ее внешнего оформления.

13. Принять меры к установлению имущества подозреваемого, принадлежащих ему денежных средств, в том числе находящихся на расчетных счетах и в электронных кошельках, на которые для возмещения ущерба и обеспечения гражданского иска необходимо наложить арест на основании судебного решения в порядке ст. 115 УПК РФ.

Дальнейшее планирование и производство предварительного расследования по уголовным делам о хищениях, совершенных с использованием поддельных платежных карт, должно осуществляться исходя из доказательственной базы, собранной в рамках выполнения изложенного выше алгоритма.

Отметим ряд особенностей, возникающих в случаях, когда хищение совершается с использованием поддельных платежных карт, оригиналы которых эмитированы банками иностранных государств (дополнение к основному алгоритму):

1) при расследовании указанных дел целесообразно принимать решение о признании потерпевшими банков-эквайеров, которые предоставляют услуги по обслуживанию платежных карт, эмитированных не только самой организацией, но и другими банками-эмитентами. Такая деятельность в первую очередь заключается в выдаче денежных средств с использованием банкоматов банков-эквайеров держателям платежных карт иных банков. При этом выда-

ваемые денежные средства являются собственностью банка-эквайера и для заполнения кассет банкоматов снимаются со счетов этого же банка.

Таким образом, в момент совершения преступления похищаются денежные средства, принадлежащие банку-эквайеру. Следовательно, предметом хищения в данном случае являются наличные деньги банка, а не безналичные деньги истинных держателей карт. При совершении краж происходит изъятие денег из чужого владения банка-эквайера, то есть собственника выдаваемых наличных денег, и обращение их преступниками в свою пользу или покушение на изъятие этих денег.

Последующее возмещение банками-эмитентами ущерба банкам, оказывающим услуги эквайринга, происходящее по заключенному договору с платежными системами, не влияет на юридическую оценку действий лиц, совершивших преступление. Таким образом, в случае поступления от банка-эмитента искового заявления он может быть признан гражданским истцом по уголовному делу. Кроме того, действующее гражданское законодательство позволяет взыскать банкам-эмитентам суммы, выплаченные в счет возмещения ущерба, в регрессном порядке с виновных лиц;

2) после производства обыска в жилище виновного лица необходимо провести осмотр изъятых поддельных платежных карт с целью установления их номеров (в случаях использования так называемого белого пластика). Такой осмотр можно провести в кассовом узле банковской организации по согласованию с ее руководством и с участием ее сотрудника;

3) направить в территориальное подразделение Центрального банка РФ запрос о предоставлении информации о банках (полное и сокращенное наименование организации, ФИО руководителя, адрес нахождения), осуществляющих обслуживание клиентов с использованием банкоматов с функцией выдачи наличных денежных средств на территории региона расследования;

4) после проведения осмотра изъятых поддельных платежных карт, получения ответа из ЦБ РФ и заключения эксперта необходимо направить запросы в банковские организации с целью установления фактов снятия или попыток снятия денежных средств с использованием установленных карт с указанием сумм операций и сведений о наличии записей камер видеонаблюдения банкоматов.

С целью установления причастности задержанных лиц к совершению аналогичных преступлений на территории всей России целесообразно направлять подобные запросы в центральные офисы всех банков, которые осуществляют обслуживание клиентов с использованием банкоматов с функцией выдачи наличных денежных средств;

5) при установлении наличия видеозаписей банкоматов либо видеозаписей торговых центров, фиксирующих место совершения преступления, необходимо провести их изъятие;

6) получить в организациях связи на основании судебных решений сведения о соединениях между абонентами и абонентскими устройствами

с обязательным указанием информации по базовым станциям, то есть по позиционированию абонентов;

7) установить эмитентов платежных карт с помощью ресурса «www.binbase.net» или на основании ответов на запросы из организаций ООО «Платежная система “Виза”» и ООО «МастерКард»;

8) все полученные предметы и документы (ответы на запросы из банков, детализации соединений, видеозаписи) необходимо осмотреть и оформить таблицу, которая позволит установить причастность задержанных лиц к совершению аналогичных преступлений. Таблица должна состоять из 5 столбцов: «Дата и время проведения операции», «Место расположения банкомата, его номер, принадлежность конкретному банку», «Сумма операции, отметка об ее успешности либо об отказе в ее проведении», «Номер использованной карты, банк-эмитент», «Сведения о лице, произведшем операцию из детализации соединений и видеозаписей».

В ходе расследования хищений, совершенных с использованием поддельных платежных карт, в случаях, если личность преступника не будет установлена в ходе производства ОРМ, может создаться ситуация, которая требует от следователя проведения огромного объема аналитической работы. Как показывает практика, клон платежной карты может использоваться преступниками в нескольких банкоматах, в том числе принадлежащих различным банкам, расположенным на территории города или региона. В этом случае следователю необходимо направить ключевым операторам связи региона (МТС, Билайн, Мегафон и т. д.) запросы с целью установления сведений о базовых станциях, в зону покрытия которых входит местонахождение банкомата.

После этого в порядке, предусмотренном ст. 186^1 УПК РФ, необходимо получить у операторов связи сведения о соединениях между абонентами и (или) абонентскими устройствами по установленным базовым станциям, совершенных в период проведения транзакций по поддельной платежной карте. После получения указанной информации следователю надлежит провести работу по выявлению фактов нахождения в зоне покрытия базовых станций одних и тех же абонентских номеров. В случае установления факта того, что одни и те же абонентские номера использовались в местах хищения денежных средств, необходимо получить у оператора связи сведения об их владельцах.

После этого необходимо направить поручение в орган дознания с целью установления факта причастности установленных следствием лиц к совершенному преступлению и перейти к выполнению действий, указанных в основном алгоритме.

Учитывая активно развивающееся многофункциональное взаимодействие банков и иных кредитных организаций, операторов платежных систем и их участников, операторов мобильной связи, интернет-магазинов, социальных сетей и прочего, возможно предположить дальнейший рост хищений, совершаемых с использованием сети «Интернет».

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Конституция Российской Федерации : (принята всенародным голосованием 12 декабря 1993 г.) : (с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 5 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ) [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 10.10.2016).

2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 6 июля 2016 г.) (с изм. и доп., вступ. в силу с 1 сентября 2016 г.) [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 10.10.2016).

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 6 июля 2016 г.) [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 10.10.2016).

4. О связи : федеральный закон от 7 июля 2003 г. № 126-ФЗ (ред. от 6 июля 2016 г.) // Российская газета. – 2007. – 10 июля.

5. Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 6 июля 2016 г.) [Электронный ресурс]. Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 10.10.2016).

6. О банках и банковской деятельности : федеральный закон от 2 декабря 1990 г. № 395-1-ФЗ (ред. от 3 июля 2016 г.) // Собрание законодательства РФ. – 1996. – № 6, ст. 492.

7. О национальной платежной системе : федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. от 3 июля 2016 г.) // Российская газета. – 2011. – 30 июня.

8. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 // Бюллетень Верховного Суда РФ. – 2008. – № 2.

9. *Лебедева, А. А.* Расследование мошенничества, совершенного с использованием информационных технологий / А. А. Лебедева // Библиотека криминалиста. – 2013. – № 5. – С. 234–244.

10. *Лебедева, А. А.* Расследование хищений, совершенных с использованием поддельных банковских платежных карт / А. А. Лебедева // Библиотека криминалиста. – 2013. – № 3. – С. 239–245.

11. *Мешков, В. М.* Некоторые аспекты формирования научных основ расследования преступлений, сопряженных с использованием средств

компьютерной техники / В. М. Мешков // Библиотека криминалиста. – 2013. – № 5. – С. 256–264.

12. *Мухин, Г. Н.* Особенности структуры и содержания методики расследования преступлений, связанных с посягательством на информационные ресурсы / Г. Н. Мухин // Библиотека криминалиста. – 2013. – № 5. – С. 280–286.

13. *Подольный, Н. А.* Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий / Н. А. Подольный // Библиотека криминалиста. – 2013. – № 5. – С. 116–127.

14. *Попов, И. А.* Правовое и организационное обеспечение раскрытия и расследования преступлений в сфере компьютерной информации: состояние и пути совершенствования / И. А. Попов // Библиотека криминалиста. – 2013. – № 5. – С. 314–327.

15. Официальный сайт Верховного Суда Российской Федерации. Режим доступа : http://www.vsrf.ru (дата обращения: 01.10.2016).

16. Официальный сайт Министерства внутренних дел Российской Федерации. Режим доступа : http://www.mvd.ru (дата обращения: 01.10.2016).

17. Официальный портал «РИА Новости». Режим доступа : https:/ria.ru (дата обращения: 11.10.2016).

18. Информация интернет-ресурса «TADVISER». Режим доступа : https:// clck.ru/AGUsK (дата обращения: 10.10.2016).

19. Справочная правовая система «ГАРАНТ» (интернет-версия). Режим доступа : http://www.garant.ru/iv/ (дата обращения: 10.10.2016).

Учебное издание

Климов Дмитрий Валерьевич

РАССЛЕДОВАНИЕ ХИЩЕНИЙ, СОВЕРШЕННЫХ
С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Учебное пособие

Редактор *Н.Б. Помадина*
Компьютерная верстка *Г.А. Федуловой*
Дизайн обложки *К.А. Быкова*

Подписано в печать 03.02.2017. Формат 60х84/16. Усл. печ. л. 1,45.
Тираж 60 экз. Заказ 120.

Редакционно-издательский отдел
Нижегородской академии МВД России

Отпечатано в отделении полиграфической и оперативной печати
Нижегородской академии МВД России

603144, Н. Новгород, Анкудиновское шоссе, 3