УДК 343.985

ЦЕЛЕВЫЕ КИБЕРАТАКИ КАК СПОСОБ СОВЕРШЕНИЯ ХИЩЕНИЯ ПУТЕМ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Н.Н. БЕЛОМЫТЦЕВ
(Академия МВД Республики Беларусь, Минск)

Рассматривается понятие способа совершения преступления с точки зрения криминалистики, определяется его значение для предварительного следствия по уголовному делу, приводятся наиболее распространенные способы целевых кибератак при хищении имущества путем использования компьютерной техники. Проанализированы типичные способы приготовления, совершения и сокрытия указанных хищений. Определены подходы систематизации и классификации способов данного вида преступлений, в частности выделены способы, направленные на получение программного контроля над банкоматами, а также процессингом банковских платежных карточек.

Ключевые слова: *целевые кибератаки, способ совершения преступления, хищение путем использования компьютерной техники, хищение с банкоматов.*

Анализ состояния преступности в Республике Беларусь свидетельствует о том, что количество регистрируемых хищений с использованием компьютерной техники из года в год остается достаточно высоким и в последнее время имеет тенденцию к росту. Так, в 2015 году было зарегистрировано 2069 таких преступлений, в 2016 году – 1844, в 2017 году – 2330. Наносимый материальный ущерб при этом из года в год значительно возрастает (за 2017 год он вырос на 2 557% по сравнению с 2016 годом). И эти данные только по выявленным и установленным фактам преступлений с учетом того, что компьютерная преступность характеризуется высокой латентностью. По данным управления по раскрытию преступлений в сфере высоких технологий, в 2017 году общий уровень раскрываемости такого вида хищений составил 59,5%. При этом в поле зрения правоохранительных органов попадает только 10–15% совершаемых компьютерных преступлений. Следует отметить, что из числа лиц, выявленных в результате деятельности по раскрытию преступлений в сфере высоких технологий в 2016, 2017 годах в Республике Беларусь, к уголовной ответственности привлечены 80% [1].

В этой связи для более эффективного, всестороннего, полного и объективного выявления и расследования такого вида преступлений и установления обстоятельств произошедшего необходимо уяснить, каким образом совершаются подобные хищения.

Важнейшим элементом преступного события, изучаемого криминалистикой, выступает способ совершения преступления. В нем содержится уникальная информация о личности преступника и следах его преступной деятельности. В отечественной литературе способу совершения преступления уделялось внимание еще в 40-е годы двадцатого века: Т.М. Браславским [2], С.А. Голунским [3], В.П. Громовым [4], Т.М. Арзуманяном [5] и другими учёными при разработке рекомендаций по расследованию хищений государственного и социалистического имущества. Дальнейшие теоретические исследования и практический опыт позволили разработать учение о способе совершения преступления, вклад в разработку которого внесли: Р.С. Белкин [6], А.И. Винберг [7], В.Ф. Ермолович [8], Г.Г. Зуйков [9], Г.А. Матусовский [10], В.Б. Вехов [11] и другие.

В настоящее время, как правило, под способом совершения преступления понимают единый комплекс взаимосвязанных действий, направленных на подготовку, совершение и сокрытие преступления, осуществляемых в определенное время, в определенном месте и с использованием необходимых орудий и средств [9].

Основная часть. Так, с учетом вышеизложенного можно говорить, что способ совершения хищения путем использования компьютерной техники может рассматриваться как система умышленных действий по подготовке, совершению и сокрытию незаконного, безвозмездного завладения имуществом потерпевшего путем изменения информации, обрабатываемой в компьютерной системе или хранящейся на машинных носителях, или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации и (или) сопряженного с несанкционированным доступом к компьютерной информации, охватываемая преступным единым замыслом, детерминированная психофизическими качествами личности расхитителя (расхитителей) и избирательным использованием им (ими) соответствующих орудий, средств, условий места, времени, а также с учетом возможных действий (бездействия) иных лиц. В связи с этим данные о способе хищения путем использования компьютерной техники, соответствующих ему типичных следах, механизме их образования и сокрытия позволяют получить значительную часть информации как о характере совершенного преступного завладения имуществом, так и о преступниках.

Вместе с тем, как показывает практика, сущность хищения путем использования компьютерной техники такова, что дать исчерпывающий перечень способов его совершения вряд ли возможно. В некоторых случаях можно говорить, что данные преступления совершаются менее квалифицированными или усеченными способами первого типа (при которых осуществляется совершение и сокрытие преступлений); менее квалифицированными или усеченными способами второго типа (подготовка и совершение преступлений), неквалифицированными или упрощенными способами (состоят только из действий по совершению преступлений) [12, с. 6].

Рассмотрение статьи 8 Конвенции ООН «О преступности в сфере компьютерной информации» (заключена в Будапеште 23 ноября 2001 г.) позволяет говорить о следующих способах преднамеренного и без каких-либо прав на это лишения другого лица его собственности путем: а) любого ввода, изменения, удаления или блокирования компьютерных данных; б) любого вмешательства в функционирование компьютерной системы мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица [13].

Кодификатор рабочей группы Интерпола в общем виде хищения с использованием компьютерной техники предлагает определять и классифицировать следующим образом [13]:

1) компьютерные мошенничества, связанные с хищением наличных денег из банкоматов;

2) компьютерные подделки – мошенничества и хищения из компьютерных систем путем создания поддельных устройств;

3) мошенничества и хищения, связанные с игровыми автоматами;

4) манипуляции с программами ввода-вывода – мошенничества и хищения посредством неверного ввода в компьютерные системы или вывода из них путем манипуляции с программами;

5) компьютерные мошенничества и хищения, связанные с платежными средствами;

6) телефонное мошенничество – доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

Анализ следственной и судебной практики, статистических данных, а также опрос пользователей компьютеров (иных технически сложных устройств) и сотрудников правоохранительных органов позволяет констатировать, что на протяжении последних трех лет 95% всех преступлений, возбужденных по одной из частей статьи 212 Уголовного кодекса Республики Беларусь, совершаются с использованием банковских платежных карточек (далее – БПК) либо их реквизитов.

Вопросы хищений денежных средств с БПК широко исследовались как отечественными, так и зарубежными учеными: В.Б. Веховым, Т.И. Абдурагимовой, А.В. Макаревичем, В.В. Хилютой, А.В. Пасынковым, И.Г. Мухиным и другими. Известны конкретные наработки, практические рекомендации по эффективному противодействию таким способам хищений, выявлению и расследованию преступлений. Результаты глубокой разработки проблемы хищений с использованием БПК [14–16] нашли свое практическое применение. В связи с широкой научной разработанностью и практическим опытом следователи не испытывают серьезных затруднений при расследовании подобных преступлений.

Представляется, что в свете современных реалий целесообразно говорить и разрабатывать комплекс мер по профилактике, установлению, пресечению, полному и всестороннему расследованию преступлений, в результате совершения которых наносится крупный, либо особо крупный ущерб пострадавшей стороне. В качестве такового может выступать сложная целевая кибератака, так называемая APT (Advanced persistent threat, с английского – «развитая устойчивая угроза»; или «целевая кибератака») [17].

Сегодня финансовые институты (банки, страховые компании, инвестиционные фонды и компании, пенсионные фонды, криптовалютные проекты и др.) имеют негативный опыт потери собственного и клиентского имущества, в связи с чем постоянно внедряют и используют все более развитую систему комплексной информационной защиты.

В свою очередь, расхитители постоянно осуществляют поиск новых возможностей для преступных схем и хищений. Чтобы получить информацию (доступ к ней), необходимую для проведения незаконных операций, надо также атаковать сети телекоммуникационных операторов, интернет-провайдеров, применять сложные схемы с использованием социальной инженерии (получать необходимый доступ к информации, основанный на особенностях психологии людей), при этом всесторонне автоматизируя эту деятельность, виртуозно распределяя вычислительную нагрузку среди других ЭВМ. Причем преступники делают это тайно, быстро, высокоорганизованно и целенаправленно, зная, «где именно и у кого лежат деньги».

В связи с вышеизложенным используемые преступниками способы подготовки, совершения и сокрытия хищений путем использования целевых кибератак в большей или меньшей степени использовались ранее, в том числе по отдельности, как самостоятельные преступления, и используются при иных более простых способах хищений. Вследствие этого при их анализе становятся понятными современные тенденции способов хищений путем использования компьютерной техники.

Как правило, хищения путем использования компьютерной техники при целевых кибератаках имеют следующие стадии: подготовка к кибератаке; совершение преступления: проникновение в инфор-

мационную систему, распространение вредоносного программного обеспечения, достижение преступной цели; сокрытие следов преступления.

Рассмотрим каждую стадию более подробно:

1. На стадии *подготовки к кибератаке* происходит установление конкретной цели (у кого будет похищаться имущество) получение необходимой информации о путях и паролях доступа к информационной системе организации. Осуществляется разработка стратегии нападения, всевозможных схем и методов стадий атаки. Также осуществляется приискание и (или) создание необходимого программного обеспечения для сбора, обработки, внедрения, распространения, хищения и сокрытия следов преступления, а также иных действий с информацией для успешной реализации атаки. Причем могут использоваться готовые программные комплексы (в том числе легитимные, например средство удаленного управления компьютером Lite Manager), либо создаваться новые, для конкретной информационной системы. Для получения конфиденциальных данных жертвы, сотрудников и лиц, имеющих доступ к информационной системе объекта нападения, как правило, используется социальная инженерия, всевозможные фишинговые ссылки (на поддельные сайты с вредоносным содержанием), взлом оригинальных сайтов для размещения на них вредоносных программ и ссылок на них.

Как правило, производится массовая рассылка электронных писем, содержащих вредоносные вложения, на адреса организаций кредитно-финансовой сферы. В случае запуска вредоносного вложения из письма на компьютере получателя происходит скрытное внедрение специализированных программ, чаще всего загрузчика (системное программное обеспечение, обеспечивающее загрузку операционной системы непосредственно после включения компьютера (процедуры POST (самотестирования) и начальной загрузки). В частности, личная почта не защищена корпоративными средствами защиты. Поэтому для атак на некоторые банки злоумышленники собирали адреса личной электронной почты сотрудников, чтобы в рабочие часы отправлять им письма с вредоносными вложениями, закамуфлированными под легальные.

В некоторых случаях вектором распространения вредоносных программ становится не спам, а взломанные популярные сайты, в том числе финансовой и юридической тематики. Так, на главных страницах нескольких крупных новостных сайтов был обнаружен зловредный скрипт, приводивший к загрузке на компьютер банковского трояна Buhtrap [18]. Может также использоваться SIM-карты по поддельным документам для восстановления паролей и получения контроля над счетом в различных финансовых сервисах [19].

Промежуточными целями кибератак, на той или иной стадии могут выступать: офис правления компании (неудовлетворительная защита ЭВМ от физического, логического и программного повреждения); центры обработки данных и функционирование многочисленных серверов, а также приложений, работающих на них; сеть поставщиков и партнеров; базы данных (взломщики могут использовать доступ администратора); офисные сети; мобильные устройства (сотрудники часто вводят в их память конфиденциальные данные, которые можно похитить).

2. На стадии *совершения преступления*, в частности проникновения в информационную систему, происходит внедрение средств удалённого доступа, управления и администрирования (как легальных (официально используемых), так и вновь созданных). При этом может использоваться целевой фишинг (обман конкретного человека), эксплоиты (компьютерная программа, фрагмент программного кода или последовательность команд, использующих уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему), знания инсайдеров, программы-шпионы, иные способы социальной инженерии, инвентаризация сети (получение сведений о состоянии системы в целом) и всевозможные комбинированные техники.

Бестелесные и вредоносные скрипты – новый (и теперь уже основной) принцип проведения атак. Так, используются «бестелесные» программы, которые работают только в оперативной памяти и уничтожаются после перезагрузки. Кроме того, скрипты на PowerShell, VBS, PHP помогают им обеспечивать персистентность (закрепление) в системе, а также автоматизировать некоторые этапы атаки.

В большинстве случаев используются скрытые каналы связи, в том числе легитимные средства для установки таких скрытых каналов, например, Plink или AmmyAdmin и т.п. [19].

На практике также встречается, что после скачивания загрузчика на компьютере устанавливается компонент Beacon – основной инструмент из набора Cobalt Strike (набор программ и команд для удаленного управления зараженными компьютерами, а также включают утилиты, предназначенные для сбора информации о сети организации и хищения данных (паролей, документов и прочего). Атакующий получает возможность удаленного доступа к зараженному компьютеру, производится анализ работы информационной системы компьютера и локальной сети.

Далее, при распространении программного влияния и управления на информационную сеть объекта атаки происходит программное закрепление в системе, поиск ключевой информации и методов достижения преступной цели. Заражение и дальнейшее получение доступа к управлению данными, распространение RAT (средств удаленного администрирования), бэкдоров (дефект алгоритма, который наме-

ренно встраивается в него злоумышленником и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом).

Атакующий проводит исследование доступных с зараженного компьютера сегментов сети и пытается установить доступ к контроллеру домена сети с целью последующего получения паролей администраторов. Для получения пароля могут быть использованы возможности специальных инструментов (Mimikatz – восстановление пароля из памяти работающей операционной системы; другие). Далее проводится поиск в сети интересующих серверов и компьютеров, прежде всего с которых есть доступ в подсеть, где находятся банкоматы или иные сегменты сети, например, в сегмент процессинга платежных карт.

На банкоматах устанавливается программное обеспечение, взаимодействующее, предположительно, через программный интерфейс XFS (стандартное расширение для финансовых услуг) и обеспечивающее выдачу денежных средств по команде, подаваемой удаленно. Например, заражение через скачиваемые обновления, якобы официально подготовленные производителем.

В настоящее время трендом является автоматизация некоторых этапов атаки, а именно: получение доступа к любому компьютеру в сети; получение логинов и паролей с первого зараженного компьютера; подключение с полученными логинами и паролями к соседним компьютерам и получение паролей с них до тех пор, пока не будет найден пароль администратора домена. Данные этапы злоумышленники заскриптовывают (программно автоматизируют), что приводит к масштабным заражениям не только корпоративной сети, но и других компаний, подключенных к зараженным [20].

3. На заключительной стадии происходит непосредственно реализация основной цели атаки – завладение имуществом и его хищение. При этом используются кейлоггеры (программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя – нажатие клавиш на клавиатуре компьютера, движения и нажатие клавиш мыши и т.д.), всевозможное программы-шпионы, перехват нужной информации и управления ключевой инфраструктурой, изменение данных, дальнейшие манипуляции с финансовыми процессами. Преступной группой проводится ряд мероприятий по сокрытию и уничтожению следов хищения и своего присутствия как на программном уровне, так и (в случае необходимости) физически [21].

Например, для уничтожения следов используются такие инструменты, как SDelete, MBRKiller, самописные утилиты для затирания данных и иные программы для безвозвратного удаления файлов. Более того, новым способом уничтожения следов после целенаправленной атаки стало использование программ-вымогателей, шифрующих данные компьютера.

В случаях если кибератака была направлена на получение контроля над банкоматами, к процессу привлекаются соучастники («дропы», «мулы»), занимающиеся получением денежных средств. Их задача – присутствие около банкоматов в условленное время для получения денег.

Яркий пример целевой кибератаки – хищение денежных средств из банкоматов ЗАО «Альфа-Банк». За несколько часов было похищено 527 000 долларов США, 67 500 евро и почти 109 000 белорусских рублей из 27 банкоматов, расположенных в Минске, Могилеве и Витебске [22]. В ходе расследования уголовного дела выяснилось, что к данному преступлению причастна международная преступная группировка Cobalt, участники которой по указанной выше схеме рассылали фишинговые письма сотрудникам банка, содержащие зараженные файлы, впоследствии был осуществлен несанкционированный доступ в информационную систему, после чего реализовывалась возможность удаленного управления банкоматами. Позднее в Беларуси задержали двух граждан, которые были вовлечены в преступную схему Cobalt. Один из них – соорганизатор, так называемый организатор «обнала», – отвечал за подбор исполнителей («мулов») в разных городах: 29-летний мужчина с гражданством Республики Молдова и Российской Федерации (суд Партизанского района в феврале 2018 года приговорил его к 11 годам 6 месяцам лишения свободы). В уголовном деле фигурировали еще шесть исполнителей («мулов»), которые непосредственно получали деньги из банкоматов. Один из них 49-летний рижанин, который приехал в Беларусь по совету знакомого. В зачет долга ему нужно было приехать в Беларусь, подъехать по нескольким адресам к банкоматам и в нужное время забрать деньги, которые без каких-либо предварительных манипуляций выдавало устройство. В августе 2017 года его задержали в Софии болгарские правоохранители, почти через 4 месяца он был экстрадирован в Беларусь. Жертвами Cobalt стали более 100 банков из 40 стран, общий ущерб превысил миллиард долларов. По имеющимся данным Европола, каждый из преступников получил до 10 миллионов евро. Главой группировки испанские полицейские назвали 34-летнего украинца Дениса К., который с 2014 года жил в испанском городе Аликанте, где и был задержан в 2018 году. По его словам, он отдавал предпочтение российским банкам, так как их системы защиты часто являются «устаревшими и относительно легко поддаются взлому» [23]. Несмотря на озвученные задержания и действия по пресечению преступной деятельности группа Cobalt, хотя и не так активно, но продолжает атаки на финансовые учреждения [24].

В случае получения доступа к процессингу платежных карт привлекаются соучастники, занимающиеся оформлением на подставных лиц (тех же «мулов») платежных карт атакованной организации.

Данные карты консолидируются в руках лиц, занимающихся получением денежных средств. Их задача – обеспечить снятие денежных средств в банкоматах непосредственно после того, как балансы и лимиты карт будут повышены в системе процессинга. В процессе получения денег соучастниками оператор может при необходимости продолжать поднимать лимиты по снятию и балансы карт.

Фокусировка атак на банкоматах и карточном процессинге привела к уменьшению среднего ущерба от одной атаки, однако позволяет атакующим проводить атаки более безопасно для «мулов», обналичивающих украденные деньги. Например, атакующие находятся в одной стране, их жертва (банк) – в другой, а обналичивание происходит в третьей [19].

В случае получения доступа к компьютерным средствам сегмента платежной системы или системы переводов SWIFT (Society for Worldwide Interbank Financial Telecommunications – международная межбанковская система передачи информации и совершения платежей) производятся платежи на заранее подготовленные счета, с которых денежные средства далее переводятся и обналичиваются по стандартным схемам для компьютерной преступности (через индивидуальных предпринимателей, фирмы-однодневки, похищенные БПК, их реквизиты, либо «мулов», покупку товаров в сети интернет и т.д.). SWIFT – это система, позволяющая финансовым и нефинансовым организациям передавать транзакции посредством «финансовых сообщений». Логика работы системы – отправка сообщений, которые бывают входящими и исходящими. Атакующие манипулируют этими сообщениями и похищают имущество.

Кибератака на клиентов кредитных организаций, использующих бухгалтерские системы, осуществляется несколько по-иному. Основная характерная особенность атак – автоматическая подмена платежных поручений на этапе их передачи из бухгалтерской системы в систему дистанционного банковского обслуживания (далее – ДБО).

В общем виде атака выглядит следующим образом: клиент формировал в бухгалтерской программе платежные поручения и отправлял их на экспорт для системы ДБО. Бухгалтерская система сформировала текстовый файл экспорта-импорта; вредоносная программа отслеживала появление (изменение) этого файла и производила подмену реквизитов получателя на заранее подготовленные злоумышленником. При этом название получателя оставалось неизменным, подменялись банковские идентификационные коды кредитной организации, номер счета, ИНН получателя; клиент производил вход в систему ДБО и загружал подготовленные (и уже измененные) платежные поручения, которые успешно направлял на обработку. В некоторых случаях от клиентов требовались подтверждения платежей по внеполосным каналам, что и делалось. В иных случаях подмена производилась после отправки корректных платежных поручений, но до их фактической передачи банку.

От момента заражения и до момента фактического хищения средств в среднем проходило от семи до одного месяца. Заражение происходило, как правило, при посещении скомпрометированных специализированных бухгалтерских и финансовых сайтов (официальных) с вредоносным содержимым. В других случаях распространение вредоносных программ данного типа происходило с использованием традиционных спам-рассылок по электронной почте.

В 2017 году для атак рассматриваемого типа, чаще всего использовались вредоносные программы TwoBee, Fibbit (она же Ranbyus) и их клоны. Существует несколько модификаций TwoBee, основное отличие которых – прописывание реквизитов получателей непосредственно в файлах вирусного программного обеспечения или же их получение от командного сервера в процессе развития основной фазы атаки. Ранние версии получали реквизиты с командного сервера, поздние содержали счета непосредственно в исполняемых файлах.

Когда целью выступают платежные шлюзы (аппаратно-программный комплекс, который позволяет автоматизировать процесс приема платежей в сети Интернет). Первыми такие атаки провели члены преступной группы Anunak, затем аналогичные атаки проводили независимые хакеры, а также вышеуказанная преступная группа Cobalt. Цель – не только банки, но и компании, управляющие платежными терминалами. Тактика атакующих отличается лишь на этапе, когда получен удалённый доступ в сеть организации, после которого атакующие ищут платежные шлюзы, где осуществляется поиск скриптов и файлов журналов, чтобы понять типичный формат передачи сообщений для осуществления транзакций. Далее запускается SOCKS-прокси (расположен между локальной сетью и Интернет-каналом) на внутренних хостах для обеспечения связи с платежными шлюзами или используются другие средства удаленного доступа. После чего создают и запускают в локальной сети скрипт, который автоматически формирует тысячи транзакций на маленькие суммы пополнения БПК и (или) балансов подконтрольных абонентских номеров. Другой скрипт переводит деньги с телефонов на счета БПК, и далее запускается стандартная процедура «отмывания денег». В отличие от атак на банкоматы, ущерб от одной атаки был значительно больше – на 1–4 млн долларов США [25].

Заключение. Все вышеизложенное указывает на то, что разновидности способов хищений путем использования компьютерной техники, детерминированы совершенствованием данной техники и техно-

логий, причем способы защиты от преступных посягательств в настоящий момент отстают. Как правило, о фактах нового способа хищения становится всем известно (кроме расхитителей) постфактум.

По нашему мнению, наилучшим решением задач, связанных с профилактикой, выявлением, пресечением и расследованием данного вида преступлений, являются:

- подготовка специалистов для борьбы с киберпреступлениями и переподготовка имеющихся кадров, что связано с необходимостью точного, быстрого реагирования, поиска, фиксации, изъятия и сбора доказательств, проведения оперативно-розыскных мероприятий в электронной форме;

- активное участие регуляторов в информационной сфере Республики Беларусь при сборе, обработке, аккумулировании поступающей информации о данных происшествиях, оказании технической помощи и участие в международном сотрудничестве с представителями иностранных государств в данной сфере;

- взаимодействие и постоянное сотрудничество (стимулирование сотрудничества) трех групп специалистов: представителей правоохранительных органов (оперативных работников, следователей, экспертов), сотрудников пострадавшей стороны (специалистов в области банковских, финансовых, блокчейн и иных инновационных технологий), специалистов в области защиты информации и лиц, занятых в данной сфере какой-либо вспомогательной деятельностью (вычислительной, интеллектуальной и т.д.).

ЛИТЕРАТУРА

1. Министерство внутренних дел Респ. Беларусь. Статистические данные [Электронный ресурс]. – Режим доступа: http://mvd.gov.by. – Дата доступа: 30.05.2018.
2. Браславский, Т.М. Техника и методика расследования дел о нарушениях финансово-бюджетной дисциплины / Т.М. Браславский. – М. : Советская юстиция. – 1933. – № 19. – С. 3–20.
3. Голунский, С.А. Методика расследования дел при хищениях государственного и общественного имущества / С.А. Голунский, Б.М. Шавер // Криминалистика / П.Н. Тарас-Радионов, М.И. Ласкин. – М., 1939. – С. 27–164.
4. Громов, В.П. Следственная тактика в примерах : пособие для следователей / В.П. Громов. – М., 1948. – Раздел III: Расследование хищений и растрат.
5. Арзуманян, Т.М. Общие указания о методике расследования хищений государственного и общественного имущества / Т.М. Арзуманян. – М. : Юриздат, 1949.
6. Белкин, Р.С. Курс криминалистики : в 3 т. / Р.С. Белкин. – М. : Юристъ, 1997. – Т. 3 : Криминалистические средства, приемы и рекомендации. – 480 с.
7. Белкин, Р.С. Криминалистика. Общетеоретические проблемы / Р.С. Белкин, А.И. Винберг. – М. : Юрлит., 1973. – 182 с.
8. Ермолович, В.Ф. Криминалистическая характеристика преступлений / В.Ф. Ермолович. – Минск : Амалфея, 2001. – 304 с.
9. Зуйков, Г.Г. Поиск преступников по признакам способа совершения преступления / Г.Г. Зуйков. – М. : ВШ МВД СССР, 1970. – 191 с.
10. Матусовский, Г.А. Экономические преступления: криминалистический анализ / Г.А. Матусовский. – Харьков : Консум, 1999. – 480 с.
11. Вехов, В.Б. Компьютерные преступления. Способы совершения, методики расследования / В.Б. Вехов. – М. : Право и закон, 1996. – 182 с.
12. Уткин, М.С. Особенности расследования и предупреждения хищений в потребительской кооперации / М.С. Уткин. – Свердловск : СЮИ, 1975. – 78 с.
13. Вопросы международного сотрудничества в борьбе с компьютерными преступлениями [Электронный ресурс]. – Режим доступа: http://www .crime-research.ru/news. – Дата доступа: 31.01.2018.
14. Вехов, В.Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов / В.Б. Вехов. – Волгоград : ВА МВД России, 2005. – 280 с.
15. Абдурагимова, Т.И. Раскрытие и расследование изготовления, сбыта и использования поддельных кредитных и расчетных пластиковых карт : дис. … канд. юрид. наук / Т.И. Абдурагимова. – М. : ЮИ МВД России, 2001. – 201 с.
16. Организация расследования преступлений в сфере высоких технологий : учеб. пособие / П.В. Гридюшко [и др.] ; под общ. ред. И.Г. Мухина. – Минск : Акад. МВД, 2017. – 139 с.
17. APT [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/APT#cite_ref-_6ffe97e274898d9e_1-3. – Дата доступа: 15.04.2018.
18. Плохие новости: троян Buhtrap атакует счета организаций через новостные сайты [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/buhtrap-drive-by/20028/?utm_source=newsletter&utm_ medium=Email&utm_campaign=kd%20weekly%20digest. – Дата доступа: 16.04.2018.

19. Group-IB Hi-Tech Crime Trends 2017 [Электронный ресурс]. – Режим доступа: https://www.pacifica.kz/upload/Group-IB_Hi-Tech_Crime_Trends_2017.pdf. – Дата доступа: 16.04.2018.
20. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf. – Дата доступа: 17.04.2018.
21. Advanced Persistent Threat (APT) Таргетированные или целевые кибератаки «Развитая устойчивая угроза» [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/ index.php/. – Дата доступа: 17.04.2018.
22. Завершено расследование против мошенника, который участвовал в краже более 600 тысяч долларов у банков [Электронный ресурс]. – Режим доступа: https://finance.tut.by/news585838.html. – Дата доступа: 18.04.2018.
23. В Беларуси задержали двух участников синдиката Cobalt, укравшего миллиард евро [Электронный ресурс]. – Режим доступа: https://42.tut.by/586581. – Дата доступа: 18.04.2018.
24. Group-IB: несмотря на арест лидера, группа Cobalt продолжает атаки на банки [Электронный ресурс]. – Режим доступа: https://www.group-ib.ru/media/gib-cobalt-activity/. – Дата доступа: 19.04.2018.
25. Основные типы атак в кредитно-финансовой сфере в 2017 году [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/StaticHtml/File/14435/gubzi_17.pdf. – Дата доступа: 18.04.2018.

Поступила 11.10.2018

TARGETED CYBER ATTACKS AS A MEANS OF COMMITTING THEFT BY MEANS OF COMPUTER TECHNOLOGY

N. BELOMYTTSEV

The article analyzes the concept of the method of committing a crime from the point of view of forensic science, determines its significance for preliminary investigation in a criminal case, lists the most common methods of targeted cyber attacks when stealing property using computer equipment. Typical methods for the preparation, commission and concealment of these thefts are analyzed. Approaches to systematization and classification of the methods of this type of crimes are defined, in particular, the ways aimed at obtaining software control over ATMs, as well as the processing of bank payment cards, are highlighted.

Keywords: *targeted cyberattacks (advanced persistent threat), a way of committing a crime, theft by using computer equipment, theft from ATMs.*