Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

Расследование преступлений, связанных с хищениями денежных средств из устройств самообслуживания

Учебное пособие

Рекомендовано Ученым советом
Московского университета МВД России имени В.Я. Кикотя
в качестве учебного пособия для курсантов и слушателей

Москва
Московский университет
МВД России имени В.Я. Кикотя

2023

УДК 343.71
ББК 67.410.2
Р24

Рецензенты:
начальник Управления международного сотрудничества МВД России **Р. А. Терентьев**; доцент кафедры уголовного права Санкт-Петербургского университета МВД России кандидат юридических наук **Е. А. Маркова**; преподаватель цикла общеправовых и социальных дисциплин ЦПП ГУ МВД России по Саратовской области кандидат юридических наук, доцент **И. А. Гревнова**

Авторский коллектив:
В. В. Гончар, Е. П. Полянская,
Н. В. Михайленко, С. В. Мурадян, Р. А. Чурин

Р24 **Расследование преступлений, связанных с хищениями денежных средств из устройств самообслуживания** : учебное пособие / [В. В. Гончар и др.]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2023. – 146 с.
ISBN 978-5-9694-1366-5

В учебном пособии в обобщенном и систематизированном виде представлены способы и механизм совершения преступлений, связанных с хищениями денежных средств из банковских устройств самообслуживания, предложена методика расследования указанной категории преступлений, проанализированы проблемы, возникающие при их расследовании.

Предназначено для обучающихся образовательных организаций системы МВД России, а также сотрудников правоохранительных органов, осуществляющих оперативно-разыскную деятельность, предварительное следствие и дознание.

УДК 343.71
ББК 67.410.2

ISBN 978-5-9694-1366-5

Оглавление

Введение

Развитие цифровых технологий представляет для нас благо ровно настолько, насколько и несет в себе угрозу. В последние несколько лет популярен безналичный расчет, являющийся привлекательным не только для пользователей, но и для преступников. Это не означает, что устройства самообслуживания, а именно терминалы и банкоматы, отходят на второй план. Анализ судебно-следственной практики и статистических данных свидетельствует о большом количестве хищений денежных средств с таких устройств.

Данная форма хищения является одной из наиболее сложных и тяжело расследуемых преступлений, отличающихся высоким уровнем латентности. Раскрытие и расследование таких преступлений требуют не только новых тактических подходов, но и совершенствования практики доказывания.

Некоторые методы, взятые на вооружение злоумышленниками, являются относительно новыми и еще малоизученными. Понимание наиболее популярных из них способствует построению качественной системы защиты в финансово-кредитных учреждениях. Правоохранительные органы, в свою очередь, смогут быстро сориентироваться на месте происшествия и правильно составить план расследования.

В представленном учебном пособии предложен системный анализ деятельности следователя по расследованию основных видов хищений денежных средств из устройств самообслуживания и с их использованием; нашли отражение уголовно-правовые, уголовно-процессуальные, криминалистические и организационно-правовые аспекты деятельности сотрудников правоохранительных органов по расследованию указанного вида преступлений.

Глава I Общая характеристика хищений денежных средств из устройств самообслуживания и с их использованием

§ 1.1. История создания устройств самообслуживания и пластиковых банковских карт к ним

Устройства самообслуживания (УС) являются неотъемлемой частью современной жизни. Они обеспечивают людям простой доступ к деньгам, одновременно с этим повышая уровень финансовой защищенности населения. По сути, данные устройства обеспечивают автоматизированное кассовое самообслуживание клиентов банка посредством использования последними специальных пластиковых идентификационных карточек.

Все устройства находятся в непосредственной связи с банком-эмитентом и банком-эквайером.

С каждым годом банками предоставляется все бóльший спектр клиентских услуг. Они подвергаются серьезной модификации, оснащаются системами биометрического распознавания клиентов, инженерно-техническими средствами защиты.

Если изначально устройство работало только с выдачей денежных средств, то в настоящее время мы можем использовать широкий функционал, связанный с оплатой коммунальных услуг, налогов, телекоммуникационных услуг, а также переводами денежных средств, погашением кредитных платежей, операциями с валютой и т. д. К устройствам самообслуживания относятся банкоматы и терминалы различной модификации. Само по себе устройство самообслуживания представляет собой электронный программно-технический комплекс, предназначенный для совершения без участия работника банка операций выдачи (приема) наличных денежных средств (в том числе с использованием платежных карт), передачи распоряжений клиента о перечислении денежных средств с банковского счета (счета вклада) клиента и др.[1]

Классификация УС сравнительно небольшая. Выделяют информационно-платежные терминалы, банкоматы с функцией приема наличных, банкоматы без функции приема наличных и банкоматы с функцией ресайклинга. Не стоит путать банкомат и платежный терминал. Далее представлены несколько видов терминалов (рис. 1, 2). Их функционал зависит от выполняемых задач.

Действительно, устройства самообслуживания имеют некоторые схожие внешние и функциональные свойства. Терминалы появились сравнительно недавно, а именно с момента доступности населению мобильных устройств. Изначально телефонные счета пополнялись в офисах операторов либо салонах сотовой связи. Позже появились терминалы, позволяющие быстро осуществлять перечисление денежных средств со снятием небольшого комиссионного сбора.

Рис. 1. Платежные терминалы

Рис. 2. Платежные терминалы

На сегодняшний день функционал платежных терминалов существенно расширен, пользователям предоставлена возможность осуществлять оплату всех видов платежей и услуг, осуществлять трансферт денежных средств на электронные кошельки, счета в системе быстрых переводов, пополнять счет аккаунтов онлайн-игр.

Платежный терминал может принадлежать частному предпринимателю либо юридическому лицу, не имеющему лицензии банка и осуществляющему свою деятельность на основании договора, при этом доход формируется с осуществленных платежей. Все платежи при использовании подобного терминала являются относительно анонимными, что зависит от вида и модификации.

Основной же функцией банкомата является выдача денежных средств при использовании банковской карты. Принадлежит он банку, обладает высокоуровневой программной и физической защитой в отличие от терминала, где хранится, как правило, небольшая сумма денежных средств, привлекающая куда меньшее количество преступников. Банкомат появился существенно раньше, чем терминал, и имеет более чем полувековую увлекательную историю создания, которой мы обязаны обладателю патентов, связанных с оптикой и электроникой, самому универсальному изобретателю и предпринимателю Америки Лютеру Джорджу Симджяну (рис. 3). Он создал механизм, позволяющий каждому владельцу банковского счета в любое удобное время получить доступ к принадлежащим ему денежным средствам.

Рис. 3. Лютер Джордж Симджян

В 1939 г. был представлен прототип аппарата, названного впоследствии банкоматом. Однако посредством данного аппарата снималось только определенное количество денежных средств, ведь между банкоматом и банковской организацией отсутствовала связь, что делало невозможным их автоматическое списание. Попытка внедрения в работу банковской организации данного аппарата, к сожалению, не привела к успеху.

После демонстрации Л. Д. Симджяном банкомата руководителям крупнейшего банка City Bank of New York он тестировался около шести месяцев, но не получил одобрения для внедрения в работу. Поняв, что изобретение не является перспективным, Л. Д. Симджян прекратил его разработку.

В 1967 г. компания De La Rue, располагавшаяся в Великобритании, приняла решение о внедрении банкомата в лондонское отделение банка Barclay's. Альтернативой пластиковым картам послужили бумажные ваучеры на разовое получение денежных средств в размере 10 фунтов.

Указанная компания по сей день осуществляет деятельность по производству бумаги, предназначенной для печатания денежных купюр. 1967 г. является датой официального рождения банкоматов (рис. 4).

Рис. 4. Актер Рег Вэрни первым опробовал банкомат

В последующем совершенствованием банкомата стал заниматься Джон Шеперд-Бэррон, на тот момент являвшийся управляющим директором компании De La Rue[2]. Известно, что его не устраивало отсутствие возможности получить денежные средства в любое время дня и ночи, в результате чего возникла идея создания аппарата, выдающего наличность и работающего в круглосуточном режиме. Действительно, позже на вопрос, как у него родилась идея создания банкомата, он ответил, что как-то раз не смог попасть в свой банк, чтобы снять деньги. Эта неудача запомнилась ему и не давала покоя.

Идея «автоматического кассира» пришла в голову неожиданно: «Я вдруг понял, что есть возможность взять

деньги в любом месте в Великобритании или во всем мире. Я подумал об автомате, который продает шоколадки, и решил заменить шоколадки деньгами».

Разработанное устройство стало называться именем компании De La Rue Automatic Cash System (DACS). Одновременно выпускается специальная карточка для осуществления взаимодействия с разработанным аппаратом. Принцип работы родоначальника аналогичен алгоритмам работы современных банкоматов, владельцу карточки также было необходимо вставить ее в приемник и ввести четырехзначный пароль для получения необходимой суммы со счета.

Пластиковых карточек в то время еще не существовало, и для нового устройства использовались схожие с карточкой специальные чеки, пропитанные слаборадиоактивным углеродом-14. Д. Шеперд-Бэррон утверждал, что никакого вреда здоровью они не несли. Автомат принимал чек и ждал ввода «персонального идентификационного номера», ныне всем знакомого ПИН-кода. Его тоже придумал Д. Шеперд-Бэррон. Он помнил свой шестизначный солдатский номер, но перед тем, как предложить шесть цифр банку, решил посоветоваться с женой Кэролайн, которая посоветовала для удобства запоминания использовать четыре цифры. Впоследствии они стали мировым стандартом.

В своем интервью Д. Шеперд-Бэррон предрекал, что денежные средства скоро выйдут из обращения: «Доставка денег стоит денег. Я думаю, наличные деньги доживают свой век». Спустя 40 лет после успешного внедрения в работу банкомата Джон Шеперд-Бэррон был удостоен ордена Британской империи.

Примерно через год население Германии получило возможность использовать функционал банкомата. К 1969 г. его

установили на улице. Тогда же им заинтересовался руководитель компании Docutel Дон Ветцель, а покупателем стал банк Chemical.

Главным отличием данного устройства стал прием пластиковых карт с магнитной полосой. Благодаря разработке Дона Ветцеля указанный банкомат явился прародителем устройств, используемых в настоящее время. Однако этому предшествовало множество различных проблем, включая неодобрение его идеи руководством. Негативный отзыв созданию Ветцеля был дан банкиром – единственным членом совета директоров. По сути, это вполне логично исходя из менталитета сотрудников банка того времени, считавших что они «должны работать с клиентами напрямую, так им можно продать им дополнительные услуги»[3]. Однако здесь присутствует доля лукавства. Сотрудниками банка на самом деле не продавались дополнительные услуги, их позиция была следующей: «Вы принесли чек, в обмен на который я дам вам деньги, и если я буду работать быстро, то смогу обслужить всех клиентов в очереди и все будут счастливы»[4].

С наступлением 1980-х гг. распространение банкоматов происходило в геометрической прогрессии. Ни работники банка, ни граждане в должной мере еще не осознавали, какие преимущества им предоставлялись данными устройствами. Если ранее их активному распространению мешало отсутствие связи с банком, то в середине 1980-х гг. была внедрена технология, позволяющая в онлайн-режиме производить списание денежных средств со счета.

Следует отметить, что предыдущие банкоматы выдавали только ограниченное количество купюр в отдельном конверте, а также не были оснащены экраном, позволявшим видеть остаток на счете.

Банкоматы того времени имели достаточно большие габариты. Об их уменьшении говорить было невозможно ввиду изготовления внутренних деталей из стали. Первый уличный банкомат помещался в металлический корпус, толщина стенок которого составляла 1,6 см. Данные меры предпринимались в целях избегания взломов и хищений денежных средств. Для вскрытия такого корпуса потребовалось бы непрерывное восьмичасовое воздействие газовой горелки. Кроме того, такой банкомат имел множество проводов. При устранении неполадок либо обрыва инженерам требовалось несколько часов только на поиск проблемы.

В течение продолжительного времени разработчики банкоматов и владельцы банков работали над расширением функционала устройства и его габаритами. В настоящее время мы видим компактные банковские терминалы за счет изготовления большинства компонентов из пластика, внедрения операционной системы, схем, систем защиты и т. д.

В конце XIX в. на рынке появились банкоматы, при помощи которых клиенты банка могли пополнить свой счет или погасить кредит. В первое время перечисление денег занимало более одного дня.

Важной особенностью тех банкоматов являлась необходимость использования отдельного конверта, в который клиент складывал вносимую на счет сумму. Зачисление денег на счет происходило только после того, как инкассаторы вынимали этот конверт и пересчитывали вручную наличные средства. По мере развития технологий все больше банков стали внедрять банкоматы, принимавшие наличные купюры в режиме реального времени. Развитие функционала устройств и расширение списка предоставляемых услуг привело к тому, что современные банкоматы стали распознавать информацию, которая содержится на банковских

чеках. Клиенту остается лишь внести необходимые данные, после чего деньги перечисляются на указанный счет. Банкоматы «научились» распознавать информацию, которая кроется в штрихкоде квитанции.

На мировом рынке сегодня представлено множество компаний, занимающихся производством банкоматов. Лидерами среди них являются четыре организации: NCR, Wincor Nixdofr, Diebold Incorporated (возникла еще в середине XIX столетия), Nautilus Hyosung.

Начав со скромного старта 50 лет назад, банкоматы проникли практически везде. Однако их успех стал понятен не раньше 1980-х гг. Сегодня же дебетовые и кредитные карты стали платежным средством по умолчанию. Практически полная всемирная интеграция сетей банкоматов означает, что почти в любой точке мира мы можем путешествовать с кусочком пластика в кармане и иметь доступ к наличным в самых удаленных уголках планеты. В настоящее время у банкомата имеется множество функций, но самой главной остается быстрое получение наличных.

В настоящее время сложно представить более востребованный и удобный платежный инструмент, чем пластиковая карта. Не исключено, что через пару десятилетий, а может и ранее, мы увидим, как она утратит свою актуальность. «В 2013 г. в США количество платежей с кредитных карт превысило количество платежей с чеков, а дебетовые карты достигли той же отметки в 2004 г. Магнитную карту постепенно вытесняют чиповые карты, и весь пластик может уйти из-за мобильных платежей, таких как Apple Pay»[5].

Путь возникновения платежной карты имеет очень интересную историю. Самым ранним предком современной платежной карты являются металлические жетоны (рис. 5).

Их повсеместное распространение приходится на начало XX в. Тогда их стали выдавать покупателям в универмагах для отслеживания покупок. Продавцами осуществлялся оттиск жетона в книге учета рядом с именем покупателя.

Рис. 5. Металлические жетоны для отслеживания покупок

Таким образом предприимчивые бизнесмены пытались заманивать в свои торговые точки покупателей. Сейчас мы наблюдаем подобную систему, когда речь идет о накопительных и скидочных картах. Они делают выгодным возвращение к той торговой организации, где она может быть использована (к примеру, бонусная карта торговой сети «Пятерочка»).

Существенным минусом металлических жетонов являлась ограниченная локация действия, ведь за пределами местности они не были актуальными, да и в целом подобные торговые сети имелись далеко не везде, к тому же сами жетоны являлись достаточно тяжелыми. В 1880-х гг. президент компании American Express, ввиду необходимости использования кредитных писем для получения денег, поручил одному из под-

чиненных разработать альтернативу. Так появились дорожные чеки (рис. 6). Данный инструмент используется по сей день. Расплатиться ими может только владелец, а в случае кражи или утери их восстанавливают в офисах American Express и его партнеров.

Рис. 6. Дорожный чек

Немного позже, в 1920 г., компанией Texaco были разработаны и выпущены картонные карты, позволявшие клиентам использовать их на автозаправочных станциях (рис. 7).

Рис. 7. Картонные карты для использования
на автозаправочных станциях

В последующем выяснилось, что использование данных карт не отвечает требованиям практичности и удобства, в связи с чем компанией Farrington Manufacturing было принято решение о выпуске стальных эмбоссированных карт, позволяющих автоматизировать процесс оплаты (рис. 8). Клерку надлежало только отпечатать данные.

Рис. 8. Стальная эмбоссированная карта в чехле

Документ, оформляемый при осуществлении покупки с помощью банковской платежной карты, называют слипом[6]. Подходящим для выдавливания букв стал шрифт Farrington 7B, используемый в настоящее время для тиснения пластиковых карт.

В 1940–1950-е гг. во времена «торгового бума» в США система безналичного расчета стала постепенно замещать чековые книжки. Начало кредитным картам было положено специалистом по потребительскому кредитованию Национального банка Flatbush в Бруклине Джоном С. Биггинсом, организовавшим в 1946 г. систему Charge It, где покупатели оплачивали товары расписками, магазин отдавал расписки в банк и оплачивал товары со счетов покупателей (рис. 9). Фактически принцип этой цепочки не изменился, кроме молниеносной скорости[7].

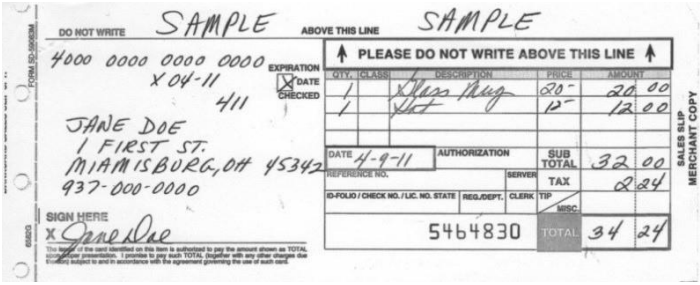


Рис. 9. Чек из чековой книжки

Одной из первых независимых кредитных компаний, работавших с платежными картами, предназначенными для оплаты путешествий и развлечений, стала Diners Club, основанная в 1950 г. Воплощение идеи в жизнь началось с забытого дома кошелька основателем компании (в 1949 г.), которому не удалось оплатить ужин в ресторане. «Целью проекта стала возможность посетителям таких заведений не ограничиваться наличностью. Клуб выдавал карты, выступал поручителем по обязательствам, оплачивал выставленные счета, а члены клуба раз в месяц получали выписку и должны были за две недели выплатить клубу всю сумму. В 1950 г. компания Diners Club выдала первые 200 кредитных карт, держателями которых в основном являлись друзья основателя компании.

Карты были выполнены из бумаги, на оборотной стороне содержалось 14 адресов ресторанов г. Нью-Йорка, принимавших их»[8]. Первые карты компании Diners Club приведены ниже (рис. 10).

Рис. 10. Первые карты компании Diners Club

К концу 1950 г. насчитывалось около 20 тыс. владельцев карт, которые могли расплатиться в 285 ресторанах. С середины 1950 г. компания вышла на международный рынок, Американскую фондовую биржу, а в 1981 г. ее купил Ситибанк.

В СССР первые кредитные карты начали действовать в 1969 г., когда в магазинах «Березка» стали принимать к оплате карты компании Diners Club. С 2004 г. пластиковые карты из США и Канады получили логотип MasterCard, появилась возможность расплачиваться ими в любой точке, где принимают карты этой системы. 1 июля 2008 г. компания Discover Financial Services купила Diners Club International за 165 млн $.

До 1958 г. у компании Diners Club не было конкурентов, пока не появились карты компании BankAmericard.

В 1958 г. в целях сокращения издержек, связанных с платежами в малом бизнесе, свой эксперимент начал Bank of America. Около 60 тыс. банковских кредитных карт BankAmericard были отправлены жителям г. Фресно в Калифорнии[9]. Они представляли собой готовые к использованию карты, для которых являлось необязательным заполнение заявки в банковской организации. Сегодня подобная беспечность закончилась бы хищением, что и происходило в последние годы, но в 1950-х гг. таких случаев не возникало.

По подобным картам присутствовал лимит в 500 $. В связи с отсутствием серьезных информационно-телекоммуникационных технологий информация в банковскую организацию уходила по прошествии длительного времени, и за кредитом, соответственно, никто уследить не мог.

К 1959 г. таких карт было более 2 млн и 20 тыс. предпринимателей принимали их для платежей. Тогда при оформлении покупки делался отпечаток данных с карты на квитанции – слипе, без удобных терминалов, компьютеров и интернета. Автоматизации помогали эмбоссированные на карте данные, расположенные в нижней части (рис. 11).

Рис. 11. Эмбоссированные пластиковые карты BankAmericard

В том же году компания Bank of America стала предоставлять свою систему другим американским банкам, однако не

всех устраивало такое положение вещей. Это равно как представить, что на кредитной карте «ВТБ» будет написано «Альфа-Банк». По этой причине решили придумать название, фигурируемое на карте, которое не ассоциировалось бы с конкретным банком.

Таким образом, на картах появилась отметка Visa, а компания Bank of America передала операции с ними National BankAmericard, специально созданной для этого. Позже ее переименовали в Visa USA, затем – в Visa International[10] (рис. 12).

Рис. 12. Усовершенствованные эмбоссированные пластиковые карты с отметкой Visa

В 1960 г. компанией IBM впервые выпущена пластиковая карта с нанесенной на нее магнитной полосой. Необходимо было разработать способ безопасного хранения данных, а штрихкоды и перфорация надежностью не отличались. В результате этого было решено использование магнитного носителя, широко применявшегося для хранения информации в компьютерах (рис. 13).

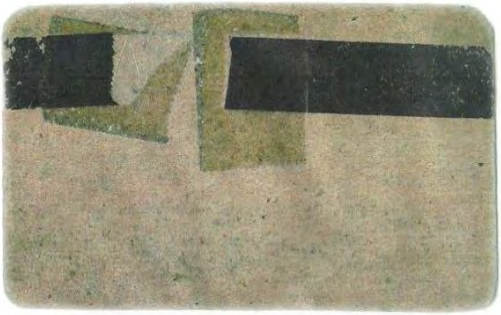


Рис. 13. Прототип карты с магнитной полосой

Инженер Форрест Перри пытался приклеить полосу, но она разорвалась. Он рассказал об этом жене, которая предложила попробовать вплавить полосу в пластик с помощью обычного утюга, что явилось действительно возможным.

Сейчас производство карт с магнитной полосой выглядит так: печатается пластиковая основа, обе ее стороны накрывают двумя листами ламината, закрепляют на поверхности магнитную полосу и укладывают в термопресс, где все обрабатывается при температуре 160°.

Выпущенные на тот момент карты имели магнитную полосу на лицевой стороне (рис. 14).

Рис. 14. Пластиковая карта с магнитной полосой
на лицевой стороне

Система MasterCard была создана как конкурент BankAmericard и изначально называлась Interbank. Компанию основали в 1966 г., когда несколько банков договорились об использовании единой системы и образовали Interbank Card Association.

В 1968 г. MasterCard с помощью европейской системы Eurocard вышел на рынок Европы. Их договоренность предусматривала взаимный прием платежей в двух системах. С основания и по 1979 г. продукт от ассоциации называли Master Charge: The Interbank Card (рис. 15), а в 1979 г. система обрела свое нынешнее название – MasterCard.

Рис. 15. Первое название платежной системы Master Charge: The Interbank Card

В 1996 г. компания заключила контракт с AT&T для создания операционной инфраструктуры в целях сокращения времени на обработку запросов. К 1998 г. появились банкоматы, принимающие MasterCard в Антарктике.

В начале 1990 г. в Европе начали разрабатывать стандарты банковских смарт-карт – пластиковых карт с встроенной микросхемой, напоминающей сим-карту. Патент на технологию был выдан в 1982 г., а в 1983 г. во Франции стали

производить чиповые карты для оплаты телефонных счетов. Такие карты используют и в системе здравоохранения Франции. И именно во Франции в 1992 г. все дебетовые карты обзавелись микрочипами. В 1990-е гг. появились сим-карты на смарт-картах[11] (рис. 16).

Рис. 16. Одна из первых полноразмерных сим-карт на дебетовой карте

Установленный внутри карты RFID-чип позволял совершать бесконтактные платежи по технологиям PayPass и PayWave.

История создания и совершенствования POS-терминалов, являющихся специализированным банковским оборудованием, предназначенным для использования на предприятиях торговли и сервиса и позволяющих принимать к оплате банковские платежные карты, менее богата.

Первое упоминание о внедрении электронного платежного терминала – EFTPOS пришлось на 1979 г., но техническое обеспечение его работы не имело такого успеха, как это было с банкоматом, и длительное время о нем мало что было известно.

Самым главным событием для введения POS-терминального оборудования явилось представление в 1993 г. Дэвидом Чаумом технологии для реализации идеологии «электронных денег», что предопределило появление системы eCash, являющейся базой для современных платежных систем цифровой наличности.

Достижения в данной сфере получили стремительное развитие, и через короткое время была разработана моновалютная микропроцессорная карточка для мелких покупок (Proton), а платежная система Mondex создала электронный кошелек. В 1996 г. из-за большой величины транзакций были определены требования к технологии изготовления микропроцессорных карт (EMV) и специальный протокол для осуществления электронных транзакций (SET).

Исторически первой российской электронной платежной системой является CyberPlat, образованная в 1997 г. Первая транзакция в системе была осуществлена в марте 1998 г., а в августе произведен первый платеж через интернет в пользу оператора «Билайн».

Что касается финансово-кредитных учреждений, то, взяв за основу указанную выше технологию, компания MasterCard в 2012 г. представила карту с клавиатурой и жидкокристаллическим экраном. Микрокомпьютер внутри карты генерировал одноразовые пароли и хранил в памяти историю операций, а также показывал баланс счета[12].

Современные терминалы для приема карт (рис. 17) связываются с банком через мобильную сеть и могут работать от аккумуляторов, что делает их удобными, например, для оплаты в ресторанах. В настоящее время устройства поддерживают бесконтактную оплату.

Рис. 17. Современные терминалы для приема карт

В 2014 г. MasterCard совместно с Apple включили функционал мобильного бумажника в iPhone.

Преступные действия с кредитными картами начались сразу после их появления. Американцы поняли, что, имея большой кредитный лимит, можно набрать товаров, продать часть из них и уехать в другой штат или страну. Следующей волной был бум интернет-коммерции в середине 1990-х гг. На сайтах появились кнопки «купить».

Злоумышленники использовали номера украденных карт и известные имена, например Микки Мауса, Лекса Лютора, Джона Уэйна, Билла Клинтона. Тогда системы не предполагали проверки имени плательщика и сопоставления его с номером карты, поэтому продавцам пришлось внести изменения.

На территории России также появились различные схемы хищения денежных средств, совершенствующиеся со временем (см. главу II).

§ 1.2. Понятие хищения и особенности его квалификации при использовании устройств самообслуживания

Как уже отмечалось, устройства самообслуживания в современном мире выступают одним из основных элементов автоматизации процессов банковских операций и, как следствие, являются распространенным объектом преступного посягательства.

По данным Банка России, количество и объем операций по переводу денежных средств с использованием электронных средств платежа (ЭСП) физических лиц составляют 40,3 млрд ед. и 71,03 трлн ₽ соответственно. Количество и объем операций с использованием платежных карт (в банкоматах и в интернете) составили 39,2 млрд ед. и 63,7 трлн ₽ соответственно, аналогичные показатели по операциям в системе дистанционного банковского обслуживания (ДБО) – 1,1 млрд ед. и 7,3 трлн ₽ соответственно.

В 2019 г. было зафиксировано 40 тыс. случаев использования платежных карт (за исключением предоплаченных) без согласия их владельцев в банкомате или терминале. Из них почти четверть (22,4 %) произошли в результате использования злоумышленниками приемов социальной инженерии. Общая сумма ущерба по хищениям через банкоматы и терминалы составила свыше 525 млн ₽, при этом банки вернули клиентам более 10 % похищенных средств (54,4 млн ₽).

Факторами, способствующими совершению таких хищений в столь крупных объемах, являются:

- Недостаточность нормативно-правового регулирования. Безусловно, процесс нормативно-правового регулирования имеет тенденцию к постоянному совершенствованию, но, что вполне закономерно для такого рода преступности, идет вслед за ней, создавая большие пробелы до момента принятия должных нормотворческих решений.
- Недостаточный информационный обмен. Правоохранительные органы не всегда могут получить необходимую информацию для раскрытия преступлений по горячим следам достаточно оперативно, поскольку указанный процесс требует внутренних согласований в банках.
- Низкий уровень финансовой грамотности населения. В настоящее время цифровая гигиена имеет колоссальное значение для обеспечения финансовой безопасности обычного гражданина.
- Сложность выявления подобных преступлений. Граждане нередко предпочитают не обращаться в правоохранительные органы ввиду стеснения, малозначительности или элементарного недоверия к системе и отсутствию уверенности в квалифицированности сотрудников.
- Трудоемкость процесса расследования. Процесс расследования подобных преступлений требует подготовку большого количества запросов, а соединение отдельных эпизодов в единое преступление – долгой и кропотливой работы и больших временных затрат, что не всегда представляется возможным в силу высокой загруженности сотрудников правоохранительных органов.
- Сложность в пресечении преступлений. Указанному способствует целый ряд факторов, среди которых

можно выделить иногда достаточно большой промежуток времени между непосредственно моментом совершения преступления и обращением граждан в правоохранительные органы, общением мошенника с потерпевшим удаленно, использованием мошенниками данных с карт или же копированных карт за пределами Российской Федерации и др.

По оценкам многих специалистов, новые способы хищения появляются примерно каждые полгода. Это связано с тем, что банки стараются обеспечить безопасность своих клиентов и мошенники различными способами пытаются обойти систему безопасности устройств самообслуживания. Несмотря на то, что хищение денежных средств и информации из банкоматов и терминалов или с их использованием пресекается законом, количество желающих незаконно обогатиться на этом только растет[13].

Следует учитывать и территориальную распространенность совершаемых преступных деяний. 82 % по количеству и 74 % по объему операций приходится на банки Московского региона. Второе место по количеству занимает Центральный федеральный округ – 11,3 %, по объему – Санкт-Петербург (11,5 %). На долю операций, совершенных за пределами Российской Федерации, приходится 42,5 % от количества и 29,3 % от объема всех операций физических лиц, совершенных в 2019 г.

Можно выделить следующие причины роста совершаемых преступлений в отношении устройств самообслуживания:

- Многие банкоматы и терминалы не обеспечены необходимыми техническими средствами охранной сигнализации.

- Зачастую не соблюдаются условия безопасной установки банкоматов и терминалов.
- Информация о способах кражи из банкоматов и терминалов широко доступна в интернете.

Следует отметить, что из терминала похищается информация о владельце карты, а в банкоматах – как информация, так и денежные средства. В некоторых терминалах старой модификации могут иметься кассеты с денежными средствами.

Вместе с тем для полноты понимания исследуемого материала необходимо проанализировать направления деятельности служб безопасности банков по борьбе с кражами из устройств самообслуживания или электронных средств платежа. На основе выявленных угроз разрабатываются новые методы и способы защиты устройств самообслуживания. Однако следует отметить, что банки в первую очередь пытаются обеспечить именно физическую безопасность банковских устройств и денежных средств, при этом необоснованно упуская современные методы совершения хищений, которые, как правило, связаны с цифровыми технологиями и удаленным доступом.

В настоящее время выделяют следующие виды мероприятий по повышению безопасности банковских устройств:

- Мероприятия по обеспечению общей технической укрепленности мест расположения банкоматов и банковских терминалов.
- Настройка специальных средств, позволяющих получить оперативную информацию о несанкционированном доступе. Подобные данные в первую очередь передаются в специально созданные центры мониторинга безопасности.
- Оборудование банкоматов специализированными средствами воздействия на взломщиков и иных преступников, посягающих на имущество организации.

Использование средств, которые полностью уничтожают или делают невозможными к использованию денежные средства банка в случае их утраты или взлома терминалов и банкоматов организации.

Подобные меры прежде всего используются по причине их общей дешевизны, а также состоятельности как видов защиты. В данном ключе интерес вызывает, например, подход, при котором кассеты с хранящимися в них денежными средствами оборудуются красящим веществом, портящим банкноты и не позволяющим их использовать. Вместе с тем остаются практически полностью без защиты клиенты банка, так как преступники могут свободно получить доступ к их персональным данным и удаленно воспользоваться банковскими карточками и счетами. Также вне поля защиты остаются технологические способы хищения, например с использованием особого программного обеспечения и т. д.

Приступая к анализу хищений из устройств самообслуживания и с их использованием, необходимо отметить, что в соответствии с примечанием к ст. 158 УК РФ под хищением понимается совершенное с корыстной целью противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или иному владельцу этого имущества.

Преступления против собственности, совершаемые из устройств самообслуживания или с их использованием, продолжают оставаться одними из самых труднораскрываемых по причине специфики механизма совершения преступления. Данные деяния могут совершаться любым лицом, имеющим необходимые навыки работы. Причем круг этих лиц существенно отличается в зависимости от способа соверше-

ния указанной группы преступлений. Потерпевшим от данных преступлений может стать любой человек, имеющий банковский счет, привязанный к банковской карте, а также сам банк. Особенно остро проблема раскрываемости касается регионов, где в настоящее время ощущается нехватка соответствующего технического оснащения и специфических профессиональных навыков у сотрудников органов внутренних дел.

Анализ следственно-судебной практики свидетельствует о том, что на данном этапе практика применения норм уголовного закона при их квалификации достаточно противоречива. Основной проблемой в данном случае является объективное установление признаков совершенного преступления. Необходимо выяснить, что же на самом деле произошло: кража, мошенничество, разбой, внесение поддельных денег в устройство самообслуживания или преступление, связанное с кибератакой на него. Следует отметить, что последний вид преступлений является наиболее актуальным и сложным с точки зрения квалификации видов преступлений. Ответственность за хищения денежных средств, совершаемые из устройств самообслуживания или с их использованием, в зависимости от способа хищения предусмотрена ст.ст. 158, 159, 159.6, 161, 162, 163 УК РФ.

Говоря про структуру преступлений против собственности, следует отметить, что первое место занимает мошенничество, второе место кражи, совершаемые с использованием современных информационных технологий. При этом доля преступлений, предусмотренных ст. 159.3 УК РФ, демонстрирует беспрецедентно низкие значения после внесения изменений в постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Федеральным законом от 23 апреля 2018 г. № 111-ФЗ в Уголовный кодекс Российской Федерации (УК РФ) введен п. «г» ч. 3 ст. 158 – кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ). Для квалификации по этому пункту необходимо, чтобы действия виновного были тайными, т. е. в отсутствие собственника, иных лиц либо незаметно для них. Например, когда денежные средства изымаются из устройства самообслуживания тайно путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата без участия уполномоченного работника кредитной организации. Если хищение с банковской карты совершено путем обмана или злоупотребления доверием, действия виновного квалифицируются также по ст. 158 УК РФ.

Так, как тайное хищение следует квалифицировать действия и в том случае, когда виновным потерпевший введен в заблуждение или обманут, под воздействием чего он сам передает злоумышленнику свою карту или сообщает персональный идентификационный номер – ПИН-код, а снятие денег с банкомата происходит без потерпевшего (п. 17 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

Кражу, ответственность за которую предусмотрена п. «г» ч. 3 ст. 158 УК РФ, следует считать оконченной с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате чего владельцу этих денежных средств причинен ущерб. Исходя из особенностей предмета и способа данного преступления местом его совершения является, как правило, место совершения лицом действий, направленных на незаконное

изъятие денежных средств (например, место, в котором лицо с использованием чужой или поддельной платежной карты снимает наличные денежные средства через банкомат либо осуществляет путем безналичных расчетов оплату товаров или перевод денежных средств на другой счет) (п. 25.2 постановления Пленума Верховного Суда Российской Федерации от 27 февраля 2002 г. № 29 «О Судебной практике по делам о краже, грабеже, разбое»).

В августе 2021 г. в УМВД России по г. Нижневартовску обратился с заявлением 32-летний местный житель о неправомерном списании денежных средств с банковского счета. Органами предварительного расследования установлено, что неизвестный позвонил заявителю и, представившись сотрудником банка, под предлогом пресечения несанкционированного списания денежных средств, сообщил, что потерпевший должен передать сотруднику службы безопасности банка принадлежащую ему банковскую карту и сообщить пин-код для осуществления доступа к ней. Таким образом сотрудники службы безопасности смогут пресечь готовящееся в отношении него преступление, переведя все деньги на безопасный счет. После чего он сможет получить в банке новую недискредитированную банковскую карту. Завладев картой и пин-кодом к ней, злоумышленник похитил у жителя Югры денежные средства в общей сумме почти 120 тыс. ₽. По данному факту полицией возбуждено уголовное дело по п. «г» ч. 3 ст. 158 УК РФ (кража, совершенная с банковского счета)

По ст. 158 УК РФ следует квалифицировать:

- Совершение хищения при помощи поддельных платежных карт.
- Совершение хищений при помощи утерянной или украденной банковской карты. Данный способ возможен, когда преступнику известен соответствующий карте ПИН-код.
- Хищение денежных средств путем физического воздействия на устройство самообслуживания.

В случаях, когда в целях завладения банковской картой на потерпевшего совершается нападение с применением насилия, опасного для жизни или здоровья, действия лица следует квалифицировать по ст. 162 УК РФ.

12 января 2017 г. около 2 часов ночи А. и Н. прибыли к банку ВТБ 24 на пересечении улиц Ново-Садовая и XXII Партсъезда, переоделись в белые комбинезоны. А. принес с собой ноутбук и необходимые приспособления – телефон, веб-камеру, USB-модем, хаб, шнур и шуруповерт. Вход в помещение, где установлено устройство самообслуживания, был свободный. Н. пошел осматривать его, а А. остался на улице наблюдать за обстановкой. Н. должен был высверлить шуруповертом два отверстия в месте расположения USB-входа и вставить в устройство самообслуживания USB-шнур для обеспечения доступа к нему. Однако просверлить второе отверстие Н. не смог, так как после первого отверстия сел аккумулятор шуроповерта. А. и Н. попробовали неудачно подключиться через одно отверстие, после чего они решили покинуть банк. В результате действия лиц были квалифицированы как покушение на кражу[14]

Не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного уголовным законом, но в силу малозначительности не представляющее общественной опасности. При решении вопроса о том, является ли малозначительным деяние, например кража, формально содержащая квалифицирующие признаки состава данного преступления, судам необходимо учитывать совокупность таких обстоятельств, как степень реализации преступных намерений, размер похищенного, роль подсудимого в преступлении, совершенном в соучастии, характер обстоятельств, способствовавших совершению деяния, и др.

Если виновный открыто похищает непосредственно банковскую карточку, знает ПИН-код или при помощи применения насилия к потерпевшему его получает, такие действия, несмотря на последующее снятие денежных средств посредством устройства самообслуживания в отсутствие потерпевшего, надлежит квалифицировать в зависимости от конкретных обстоятельств по ст. 161 или 162 УК РФ.

В случаях, связанных с тайным хищением чужого имущества (ст. 158 УК РФ) или осуществлением его посредством вымогательства (ст. 163 УК РФ) с использованием при этом неправомерного доступа к охраняемой законом компьютерной информации, квалификацию таких деяний необходимо дополнить статьями УК РФ, защищающими компьютерную информацию (ст.ст. 272–274.1).

В августе 2021 г. в дежурную часть городского округа Чехов Московской области обратилась с заявлением товаровед местного магазина «Верный» села Троицкое. Она рассказала, что глубокой ночью в 02:30 в помещение магазина, отжав металлическим предметом входную пластиковую дверь, проникли двое неизвестных в масках. Угрожая ей и товароведу-приемщику металлической трубой, они выгнали сотрудников из магазина, после чего заложили в купюроприемник самодельное взрывное устройство. Путем закачки газа злоумышленники подорвали его, далее похитили находящиеся в нем кассеты с денежными средствами, а затем скрылись. Сумма ущерба оценивается в 3 млн ₽. Возбуждено уголовное дело по ч. 3 ст. 161 УК РФ

Если лицо использовало чужую похищенную, поддельную банковскую карту, предъявляя ее для оплаты, например в торговой организации или работнику банка, для снятия наличных как свою, тем самым обманывая сотрудников, фактически не сообщая о незаконном использовании этой карты, то такие действия подлежат квалификации по ст. 159.3 УК РФ. При этом виновный при расчете за приобретенные товары или оказанные услуги не принадлежащей ему банковской картой сообщает заведомо ложные сведения о принадлежности такой карты на законных основаниях (активная форма) или умалчивает о незаконном владении им платежной картой (пассивная форма) сотруднику кредитной, торговой или иной организации, уполномоченному в силу занимаемой должности производить списание денежных средств с платежной карты. Средством совершения преступления, предусмотренного ст. 159.3

УК РФ, являются поддельная или принадлежащая другому лицу кредитная, расчетная, иная платежная карта.

17 октября 2018 г. А. похитил банковскую кредитную карту, оформленную на имя Б. в ПАО «Сбербанк России». Зная ПИН-код, А. в период с 17 октября 2018 г. по 25 октября 2018 г. посредством неоднократных расчетов за купленный товар, а также неоднократного снятия наличных денежных средств с помощью терминала самообслуживания ПАО «Сбербанк» тайно похитил с банковского счета Б. денежные средства на общую сумму 21 352 ₽, причинив Б. значительный ущерб. Мариинский городской суд Кемеровской области, соглашаясь с доводами государственного обвинителя, пришел к выводу, что действия А. подлежат переквалификации с п. «г» ч. 3 ст. 158 УК РФ на п. «в» ч. 2 ст. 158 УК РФ

Государственный обвинитель в своих доводах по указанному выше делу просил переквалифицировать действия подсудимого А. в связи тем, что по смыслу закона квалифицирующий признак хищения «с банковского счета, а равно в отношении электронных денежных средств» может иметь место только при хищении безналичных и электронных денежных средств путем их перевода в рамках применяемых форм безналичных расчетов в порядке, регламентированном ст. 5 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». В соответствии с п. 19 ст. 3 вышеуказанного федерального закона электронное средство платежа – это средство и (или) способ, позволяю-

щие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств. Принимая во внимание, что А. каких-либо действий по переводу денежных средств в рамках применяемых форм безналичных расчетов не совершал, т. е. не совершал незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети путем ввода, удаления, блокирования или модификации компьютерной информации, а похитил денежные средства потерпевшей путем получения наличных денежных средств через банковский терминал, оплачивая покупки в магазине зная ПИН-код банковской карты, в его действиях отсутствует квалифицирующий признак хищения чужого имущества «с банковского счета»[15].

Анализ правоприменительной практики позволяет сделать вывод, что схожие преступления нередко в одном случае квалифицируются по соответствующей части ст. 158 УК РФ, в другом – по соответствующей части ст. 159.3 УК РФ. Ряд судебных практик указывает на возможность применения и иных статей УК РФ при хищении денежных средств через или с помощью устройств самообслуживания.

Рассматривая причины подобного явления, следует отметить, что основное различие между кражей и мошенничеством заключается в способе изъятия имущества. В рассматриваемой ситуации – это денежные средства на банковском счете клиента банка.

Кража – это тайное хищение чужого имущества, а мошенничество – это хищение чужого имущества путем обмана или злоупотреблением доверием. Лицо использует либо полностью поддельную кредитную или расчетную карту (изготовленную способом, который именуется «чистый белый пластик» (White Plastic Crime), либо чужую карту, т. е. лицо прибегает к обману при хищении денежных средств из устройства самообслуживания.

Для более детального анализа сути вопроса необходимо определиться с понятием обмана. В соответствии с п. 2 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» обман – это сознательное сообщение заведомо ложных, не соответствующих действительности сведений, либо умолчание об истинных фактах, либо умышленные действия, направленные на введение владельца имущества или иного лица в заблуждение. Под иными лицами в данном случае понимается не любое лицо, а именно держатель банковской карты и работник банка.

В 2019 г. мошенники воспользовались новаторской идеей ПАО «Сбербанк России», где, учитывая высокий возрастной ценз большой части своей клиентской базы, использовали алгоритм, при котором в случае превышения времени операции клиенту не нужно заново вставлять карту в устройство самообслуживания и вводить ПИН-код, и применили схему «сначала операция – потом карта». Платежный терминал дает возможность сначала выбрать необходимую операцию (пополнить баланс на телефоне, перевести деньги, заплатить за услуги ЖКХ) и только потом вставить в терминал карту и ввести ПИН-код. При этом, если на последнем этапе

оставить устройство в покое и отойти от него, оно еще полторы минуты будет ожидать от клиента дальнейших действий. Мошенники выбирали операцию зачисления денег на счета своих мобильных телефонов и отходили в сторону. Когда следующие клиенты видели на экране надпись «Вставьте карту», они выполняли указания машины, вводили ПИН-код, после чего аппарат отправлял деньги злоумышленникам.

Стоит отметить тот факт, что обман является лишь способом облегчения доступа к денежным средствам владельца банковской карты. Данный вывод подтверждается в п. 17 указанного постановления Пленума Верховного Суда Российской Федерации, согласно которому действия лица следует квалифицировать по ст. 159.3 УК РФ в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой.

В процессе юридической оценки содеянного сотрудникам правоохранительных органов надо учитывать, что если преступная деятельность связана с мошенничеством, то квалификация усложняется разграничением мошенничества с использованием средств социальной инженерии, осуществляемым с помощью IT-технологий от кибермошенничества. Первый вид мошенничества предполагает психологическое манипулирование людьми в целях совершения определенных действий или разглашения конфиденциальной информации[16], однако и в данном случае не исключается использование рассылок (если они не привели к уничтожению,

блокированию, копированию или модификации компьютерной информации), размещение недостоверной информации в социальных сетях и других ресурсах сети Интернет.

Отличительной чертой кибермошенничества (ст. 159.6 УК РФ), в свою очередь, являются последствия манипуляции с компьютерной информацией в форме уничтожения, блокирования, копирования или модификации этой информации или иного вмешательства в функционирование средств хранения, обработки или передачи информации или информационно-телекоммуникационных сетей. Дополнительное толкование относительно квалификации кибермошенничества дают положения п. 20 постановления Пленума от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». Квалификация по ст. 159.6 УК РФ будет осуществляться в случае, если имеет место целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, компьютеры (в том числе портативные), снабженные соответствующим ПО, или на информационно-телекоммуникационные сети, нарушающее установленный процесс хранения, передачи и обработки компьютерной информации и позволяющее преступнику незаконно завладеть чужим имуществом.

Интерес вызывает и то, что в связи с динамичным ростом хищений денежных средств с использованием высоких технологий (в том числе в банковской сфере) преступники постоянно изобретают новые способы, методы, приемы, направленные на совершение подобных преступлений, создаются специальные технические устройства, способствующие хищению денежных средств из устройств самообслуживания и с их использованием. Одним из таких устройств является скимминговое оборудование (см. главу II).

По информации ПАО «Сбербанк России» впервые нештатное оборудование на устройствах самообслуживания финансово-кредитных организаций России, идентифицированное как скимминг, было обнаружено в 2002 г. Данное устройство выглядело как достаточно громоздкое сооружение, имитирующее лицевую панель банкомата либо терминала. Монтировалось оно в течение нескольких минут, требовало точной настройки и частой подзарядки. В результате неточных действий установщика навесная конструкция нередко демонтировалась в момент проведения операции. Современные технологии скимминга импортированы в Россию из-за рубежа.

В большинстве случаев скиммер – это оборудование, представляющее собой достаточно компактное, насыщенное электронными компонентами штатное или имитирующее штатное навесное оборудование (пассивные антискимминговые накладки на картридере или заглушки, закрывающие технологические отверстия устройства самообслуживания), различного рода накладки, закамуфлированные под корпоративные цвета банка – владельца банкомата либо терминала, задача которых получить персональные данные банковской карточки. Нештатное оборудование может быть как двухкомпонентным, т. е. состоять из двух элементов – накладки на картридер и планки с видеокамерой или накладной клавиатуры, так и однокомпонентным, совмещающим в себе считыватель магнитной полосы и накопитель ПИН-кодов.

Следует отметить, что государство реагирует на подобные изобретения путем внесения соответствующих изменений в законодательство, в том числе в УК РФ. Так, Федеральный закон от 8 июня 2015 г. № 153-ФЗ «О внесении измене-

ний в статью 187 Уголовного кодекса Российской Федерации» направлен на усиление уголовной ответственности за указанные преступления.

Данный закон внес изменения в ст. 187 УК РФ «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов». Изменилось название статьи «Неправомерный оборот средств платежей». Статья 187 УК РФ дополнилась новым положением об установлении ответственности за «изготовление, приобретение, хранение, транспортировку в целях использования или сбыта электронных средств и носителей информации, иных технических устройств, компьютерных программ, предназначенных для неправомерного перевода денежных средств в рамках применяемых форм безналичных расчетов».

Теперь лицам, занимающимся скиммингом, грозит наказание в виде принудительных работ на срок до пяти лет либо лишение свободы на срок до шести лет со штрафом в размере от 100 тыс. до 300 тыс. ₽, или в размере заработной платы, или иного дохода осужденного за период от одного года до двух лет.

Если преступление совершается организованной группой, то предусмотрено наказание до семи лет лишения свободы со штрафом в размере до 1 млн ₽ или в размере заработной платы, или иного дохода осужденного за период до пяти лет или без такового.

В настоящее время не существует единообразия в квалификации и расследовании хищений, совершенных с использованием скимминговового оборудования. Подобные деяния квалифицируются по различным статьям УК РФ.

По приговору Суджанского районного суда Курской области, вынесенному 20 февраля 2016 г. по делу № 1-13/2016, подсудимый М.Д.С. был признан виновным в совершении преступления, предусмотренного п. «в» ч. 3 ст. 158 УК РФ. Обвиняемый, имея умысел на тайное хищение чужого имущества в крупном размере, вступил в преступный сговор с А. и Б., разработав план совершения преступления. Последний предусматривал установку на устройства самообслуживания внештатного оборудования (скимминг), предназначенного для считывания информации с банковских карт на банкомате, а также установку планки с видеорегистратором, необходимой для видеофиксации ПИН-кодов банковских карт финансово-кредитных учреждений, вводимых гражданами, владельцами банковских карт при пользовании устройствами самообслуживания[17]

По приговору Советского районного суда г. Казани № 1-23/2016 группа лиц была осуждена по п. «б» ч. 4 ст. 158 УК РФ и ст. 138.1 УК РФ за кражу, совершенную в особо крупном размере, а также незаконный оборот специальных технических средств, предназначенных для негласного получения информации. Деяние было совершено посредством использования скиммингового оборудования группой лиц, за что они впоследствии и были осуждены

По приговору Чертановского районного суда г. Москвы от 25 февраля 2015 г. № 1-19/15 А. и Г. осуждены по пп. «а», «б» ч. 4 ст. 158, ч. 3 ст. 30, ч. 3 ст. 183 УК РФ за тайное хищение чужого имущества в крупном размере с причинением значительного ущерба гражданину, сопряженным с собиранием незаконным способом из корыстной заинтересованности сведений, составляющих банковскую тайну, и неправомерным из корыстной заинтересованности доступом к охраняемой законом компьютерной информации, если это деяние повлекло копирование компьютерной информации, путем установления на банковских терминалах оборудования для снятия информации о платежных картах клиентов банка и ПИН-кодов, ее записи на изготовленные дубликаты банковских карт с последующим снятием с изготовленных дубликатов карт в устройствах самообслуживания денежных средств в сумме... руб.

Данные примеры наглядно демонстрируют разные подходы судов при квалификации схожих преступлений.

Сравнительно новым способом хищения денежных средств из устройств самообслуживания и с их использованием является кибератака на программное обеспечение банкомата либо платежного терминала. Она считается наиболее опасной, но не самой распространенной, учитывая сложность технического исполнения.

Тем не менее мошенники начинают использовать все более сложные схемы и методы, например:

- Реверс-инжиниринг.

- Перехват сигнала.
- Скимминг при помощи Bluetooth или WI-FI.

Данный перечень видов кибератак на программное обеспечение банкоматов и банковских терминалов не является исчерпывающим. Широко известна атака типа Jailbreak, суть которой заключается в том, что при определенных настройках программного обеспечения устройства самообслуживания можно получить доступ к командам операционной системы и файловой системе. На основе данного способа у злоумышленников появляется возможность заражения вредоносной программой программного обеспечения банкомата, либо терминала для дальнейшего хищения денежных средств. По нашему мнению, логичнее всего подобные действия квалифицировать по соответствующей части ст. 273 УК РФ (создание, использование и распространение вредоносных программ) и соответствующей части ст. 158 УК РФ по совокупности преступлений. Однако, как мы отмечали ранее, сегодня отсутствует единообразие в квалификации подобных преступлений.

Еще один интересный с точки зрения квалификации способ хищения денежных средств из устройств самообслуживания – это Black Box.

Приговором Новокуйбышевского городского суда Самарской области О. и С. признаны виновными в совершении преступления, предусмотренного п. «а» ч. 4 ст. 158 УК РФ. О. и С. совершили Blackbox – атаку на банкомат ПАО «БАНК УРАЛСИБ». Подключив переносное устройство к банкомату, ответчики при помощи программного обеспечения подали управляющие команды на выдачу наличных денежных средств. Банкомат исполнил программные команды, выдав деньги преступникам на общую сумму 590 тыс. ₽[18]

Выявленные проблемы, связанные с отсутствием единообразия уголовно-правовой квалификации подобных преступных действий, не позволяют в полной мере реализовать принцип справедливости (ст. 6 УК РФ), что, на наш взгляд, отчасти обусловлено отсутствием соответствующих разъяснений в специальном постановлении Пленума Верховного Суда Российской Федерации.

Пока не принято подобное решение, целесообразно внести положения в постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» и от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», которые более детально разъясняли бы правила квалификации хищений денежных средств из банкоматов и с их использованием.

Неоднозначность в законодательстве приводит к отсутствию единообразного толкования правоприменения со стороны надзирающих прокуроров и суда, формирует различную правоприменительную практику при схожих признаках преступлений. Так, в территориальных органах

предварительного следствия ГУ МВД России по Краснодарскому краю в 2019 г. в зависимости от требований надзирающей прокуратуры по преступлениям, совершенным путем сообщения потерпевшим ложной информации (например, под предлогом страхования денежных средств необходимо сообщить персональные данные карты и перечислить денежные средства на указанный неустановленным лицом счет), возбуждаются уголовные дела по ст. 159 УК РФ, хотя согласно постановлению Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» действия неустановленных лиц в таких случаях необходимо квалифицировать по п. «г» ч. 3 ст. 158 УК РФ.

Апелляционная коллегия по уголовным делам Самарского областного суда от 16 октября 2019 г. прекратила уголовное преследование в отношении К., осужденного судом первой инстанции по ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ к одному году лишения свободы условно за покушение на хищение денежных средств потерпевшего в размере 148 тыс. ₽, находившихся на банковской карте, найденной обвиняемым на улице. При этом последний фактически смог завладеть денежными средствами в размере 2,1 тыс. ₽, приобретя на указанную сумму продукты в магазине

В представленном выше примере апелляционная коллегия указала на отсутствие объективных данных, указывающих на осведомленность обвиняемого о сумме, находящейся

на расчетном счете, а также что последний не оказывал несанкционированного воздействия на информационно-телекоммуникационные сети, компьютеры, серверы или их программное обеспечение.

В результате коллегия пришла к выводу о наличии в действиях подсудимого признаков преступления, предусмотренного ч. 1 ст. 158 УК РФ. Исходя из размера причиненного ущерба деяние не образует состава преступления[19].

Вместе с тем сложившаяся ситуация в области кибербезопасности вызывает серьезные вопросы. При этом мошенничества и кражи, рассмотренные в данном разделе, составляют 47 % и 34 % соответственно от общего количества киберпреступлений, совершаемых на территории Российской Федерации.

Вопросы для самоконтроля

1. Назовите исторические этапы создания устройств самообслуживания и пластиковых банковских карт к ним.
2. Раскройте следующие понятия: «банкомат», «безналичный расчет», «дебетовая карта», «кредитная карта», «платежный терминал», «расчетный счет», «электронное средство платежа».
3. Охарактеризуйте виды хищений, совершаемых из устройств самообслуживания, а также при использовании электронных средств платежа.
4. Перечислите особенности квалификации хищений, совершаемых из устройств самообслуживания, а также при использовании электронных средств платежа.
5. Что будет являться местом окончания преступления при хищении электронных средств платежа?

6. Чем обусловлен рост хищений денежных средств из устройств самообслуживания и с их использованием?

7. Какие меры по повышению защищенности банковских устройств предпринимаются со стороны государственных органов и коммерческих организаций?

Глава II Преступные схемы хищений денежных средств из устройств самообслуживания и с их использованием

§ 2.1. Устройство терминала и система его охраны

Количество банкоматов и платежных терминалов на территории страны выросло в геометрической прогрессии. Примерно 10 лет назад насчитывалось порядка 92 тыс. банкоматов и 354 тыс. терминалов, в 2020 г. было установлено 202 593 банкомата и 2 913 026 терминалов (3,1 млн устройств), в 2021 г. в эксплуатации находились 3,6 млн устройств. Банкоматы и терминалы всегда остаются «лакомой добычей» для «охотников» за легкими деньгами. Фактически это самый доступный сейф с денежными средствами. Легче похитить его, чем проникнуть в хранилище банка и совершить хищение денежных средств, к тому же устройство всегда заполнено наличностью. По этой причине службы безопасности разрабатывают все новые системы защиты[20].

Прежде чем приступить к рассмотрению видов и способов совершения преступлений, следует понять, как устроено устройство самообслуживания. Банковский автомат, также именуемый как АТМ (Automated teller machine), является программно-техническим комплексом, осуществляющим авто-

матизированные выдачу, прием как посредством использования пластиковой карты, так и без нее, а кроме того, выполнение иных действий, касающихся оплаты услуг, товаров, составления документов и т. д. Терминал же отличается ограниченным количеством функций, связанных с выдачей, а иногда и внесением денежных средств. Большинство граждан использует функцию снятия денежных средств либо оплату услуг. Мало кто знает, но при массовом внедрении программно-технических устройств они были оснащены широким функционалом: полноформатным принтером А4, 101-клавишной клавиатурой, ночным депозитором для инкассаторов, а некоторые даже устройством выдачи монет. В Российской Федерации данный функционал не ставили ввиду низкой грамотности граждан и опасений возникновения затруднений при работе с банковским автоматом, а позже необходимость в этом отпала ввиду внедрения усовершенствованной системы интернет-банкинга и операционной системы.

Для пользователя отличия банкоматов и терминалов условны, и те за счет внешнего вида либо функционала. Для производителя же они принципиальны: важны качество, функционал, скорость работы оборудования, операционной системы, системы защиты, требования к обслуживанию и т. д.

Обывательское мнение, что банковский автомат либо терминал является китайским (хотя на самом деле корейский) и поэтому менее качественный, чем американский (на самом деле – венгерский), в корне неправильно.

Имеется несколько вариантов установки устройств самообслуживания:

- В офисах либо помещениях.
- Межстенный: снаружи имеется только персональная часть, включающая экран и щели для приема пластиковых карт, выдачи/приема денежных средств и картридер; для его обслуживания инкассаторам должен быть предоставлен доступ внутрь помещения.
- Уличный: расположен на открытом воздухе в непосредственной близости с какими-либо действующими объектами, организациями, предприятиями. Имеет серьезные отличия от других программно-технических устройств. Сейфовыми стенками оборудована не только сейфовая часть, но и верхняя, с клиентской частью и процессором. В нем находится более мощное вентиляционное и отопительное оборудование.

Таким образом, каждое устройство имеет сервисную и сейфовую зоны.

Вся работа комплексного программно-технического устройства осуществляется посредством специального программного обеспечения.

В клиентской части устройства расположен картридер, в подавляющем большинстве являющийся моторизованным (рис. 18).

Однако прогресс не стоит на месте, оборудование устройств самообслуживания постоянно совершенствуется. Картридеры даже способны бороться с фишингом и скимингом, правда, часто за счет дополнительных устройств.

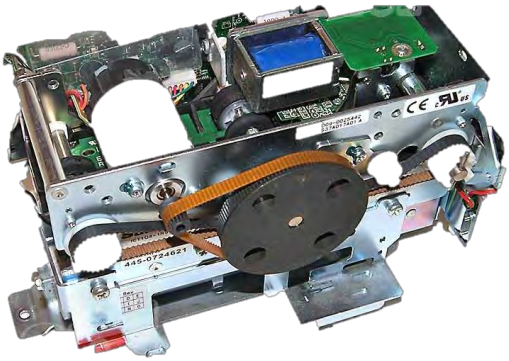


Рис. 18. Моторизованный картридер

Все оборудование находится в непосредственной связи. После того как ридер считал информацию с магнитной ленты пластиковой карты, устройство выполняет необходимую операцию, чековый принтер (термопринтер) осуществляет печать чека, разрез и посредством ремней направляет его в специально отведенную щель. Ранее применялись матричные принтеры. Для связи с банками в верхней части машины устанавливается модем или иное соответствующее устройство. Такое устройство банковского автомата позволяет устранять ошибки либо неполадки без осуществления физического доступа.

В нижней части помимо сейфа, вмещающего денежные средства, располагается специальное устройство – диспенсер. Именно он пересчитывает и выдает сумму, указанную клиентом. Причем сами диспенсеры бывают разных конструкций, в зависимости от производителя. За один раз может быть выдано не более 40 купюр, что связано с самим механизмом подачи. Злоумышленники изобретают ловушки

и предпринимают различные попытки в целях извлечения денежных средств из диспенсера. Для того чтобы совершить хищение денежных средств из кассет, преступники совершают взлом. Сейф имеет градацию по классам устойчивости ко взлому. При третьем классе стенки выполняются из стали толщиной в 2 см, при самом высоком – пятом – устанавливаются дополнительные замки и утолщенные стенки с бетонной прослойкой.

Фактически нет комплексных программно-технических устройств, которые не имели бы в сейфовой части кассеты с купюрами. Вместимость кассеты, как правило, составляет 2,5 тыс. банкнот. Информация, «сообщающая» банкомату о том, какой номинал имеют деньги, хранящиеся в сейфе, записана на отдельной флешке. В случае если инкассатор перепутал местами кассеты, чип, расположенный в кассете, не позволит выдать из нее денежные средства. Размер кассеты по выбраковке в два раза меньше стандартной.

Сегодня применяются четыре вида устройств самообслуживания:

- Банкоматы для снятия наличных денежных средств. Обычно устанавливаются в местах с высокой проходимостью.
- Банковские терминалы для приема наличных средств, применяемые также для погашения кредитов, оплаты коммунальных и других услуг. Обычно устанавливаются в отделениях банков.
- Банкоматы, объединяющие весь перечисленный выше функционал. Их существенным отличием является высокая стоимость производства, ввиду чего они менее распространены.
- Биометрические банкоматы – программно-технические устройства нового типа, осуществляющие

прием и выдачу наличных денежных средств, а также другие операции на основе биометрической идентификации владельца счета. Использование функционала данного банкомата возможно при предоставлении биометрических данных банку. Биометрические банкоматы имеют самый высокий класс защищенности по сравнению с другими устройствами, что предотвращает несанкционированный доступ к счетам клиентов[21].

Устройство самообслуживания начинает работать после того, как клиент, вставивший карту, ввел четырехзначный ПИН-код – комбинацию из четырех цифр или просто пароль, который позволяет пользователю пластиковой карты получить денежные средства на ней.

Устройство через модем связывается с обслуживающим банком. Последний проверяет состояние счета, остаток наличных средств и другую информацию. Если сумма, введенная пользователем, соответствует размеру имеющихся у него средств, банк одобряет операцию по снятию денег.

Следом за этим подключаются алгоритмы банкомата, благодаря которым производится набор требуемого количества банкнот. В завершение деньги выдаются клиенту.

Пока купюры проходят путь от сейфа до «пункта назначения», их сканирует множество разнообразных датчиков. Один из них оценивает состояние банкноты, определяя наличие потертостей и других параметров. Если датчик обнаруживает несоответствие заданным условиям, купюра отправляется в специальную кассету, а ее место занимает новая. При возникновении каких-либо проблем на пути (например, одна из них застряла) банкомат останавливается, а на мониторе возникает сообщение о неисправности.

Если клиент по каким-либо причинам не взял деньги или карту, аппарат по истечении определенного периода забирает их обратно, помещая в соответствующие кассеты. В последующем неснятые денежные средства зачисляются гражданину на счет его банковской карты.

Низкий уровень раскрываемости мотивирует людей на совершение новых преступлений по хищению денежных средств. В связи с этим службами безопасности разрабатываются новые методы защиты устройств самообслуживания.

Основной акцент службами безопасности банков делается на обеспечение мер физической защиты банковских устройств и денежных средств в них. Мероприятия для повышения безопасности разделяются на четыре категории:

- Обеспечение технической укрепленности мест, в которых расположены устройства самообслуживания.
- Оперативная передача сигналов о несанкционированном доступе в центр мониторинга.
- Использование технических средств для воздействия на взломщиков и их остановки.
- Применение средств, приводящих денежные средства в негодность в случае взлома.

Практика показывает, что лучший способ предотвратить преступление по похищению денежных средств из устройства – это испортить их. Для этого используются специальные кассеты с красящим составом. При атаках на банкомат злоумышленники ставят цель – открыть кассеты с деньгами. При вскрытии красящей кассеты деньги моментально покрываются стойкой краской, которая делает невозможным дальнейшее использование купюр.

Не менее эффективным способом предотвращения преступлений является укрепление помещений, в которых находятся платежные устройства.

На взлом банкомата, который прикручен к стене либо встроен в нишу, у преступников уйдет на порядок больше времени, чем хищение денег из незащищенного устройства. К мерам укрепления также относится использование сейфов, которые отличаются высокой степенью взломоустойчивости.

Внутри аппарата размещаются датчики, реагирующие на вторжение извне. В первую очередь это датчики наклона, передвижения и задымления. Если преступники попытаются похитить аппарат для вскрытия в тихом, безопасном месте, извещатели сработают и сигнал тревоги будет отправлен на пульт охраны. При попытке взлома на месте при помощи резака или взрыва системы задымления датчики вибрации и температуры также сработают.

Системы защиты банкомата укомплектованы охранной сигнализацией с возможностью отправки тревожных сигналов на пульт станции мониторинга. Использование охранной сигнализации не оставляет злоумышленникам шанса на быстрый взлом, а наличие нескрытой системы видеонаблюдения снижает вероятность того, что взлом вообще начнется.

Сигнализационные системы, которые используются в современных устройствах самообслуживания, разделяются на два типа. Первый тип – комплекс видеонаблюдения, второй – охранная сигнализация. Каждый из них предоставляет в распоряжение охраны массу функций:

- Ведение видеозаписи. Трансляция может вестись как в режиме реального времени независимо

от текущей ситуации, так и при срабатывании охранной сигнализации либо датчика движения.

- Синхронизация данных о транзакциях и показаний сигнализационных датчиков с видеоархивом. Эта функция видеонаблюдения оказывает большую помощь при расследовании совершенных преступлений.
- Возможность просмотра данных транзакций, видеокадров и архива, а также текущих трансляций из удаленного места. Это особенно актуально для наблюдения за устройствами самообслуживания, стоящими не в отделениях.
- Оперативная передача тревожных сообщений, данных транзакций, видеокадров и другой информации на удаленный пункт мониторинга или пульт охраны.

Главным предназначением охранной сигнализации банкоматов является оперативная передача тревоги на пульт службы быстрого реагирования.

После получения этого сигнала на место срабатывания тревоги выезжает группа, которая предотвращает взлом или хищение банкомата.

В среднем на похищение неукрепленного банкомата без средств физической защиты у злоумышленников уходит 5–10 минут.

Служба реагирования добирается на место тревоги до 7 минут.

Время зависит от удаленности банкомата, дорожной ситуации, времени суток и загруженности группы реагирования. При этом дежурный пункта центральной охраны в режиме реального времени видит все происходящее в поме-

щении, где расположены банкоматы, и в случае противоправных действий со стороны граждан докладывает о случившемся сотрудникам службы безопасности, которые незамедлительно выезжают на место происшествия. Кроме того, на место срабатывания тревоги осуществляют выезд сотрудники сервисного центра, обслуживающие банкомат, в целях оказания содействия в осмотре места происшествия. Что касается банковских терминалов, то они не подвержены хищениям, либо потому что в них не имеется кассет с денежными средствами, либо имеются (в случае если терминал работает на прием), но их сумма, как правило, небольшая. Банковские терминалы в большей степени подвержены краже информации о банковском счете или банковской карте держателя для последующего хищения денежных средств.

§ 2.2. Виды и способы хищений денежных средств из устройств самообслуживания и с их использованием

В настоящее время в связи с широким распространением среди населения расчетных операций, совершаемых при помощи банковских карт, растет количество афер, связанных с хищениями денежных средств посредством их использования.

Все способы хищения денежных средств из устройств самообслуживания или с их использованием на территории

Российской Федерации можно классифицировать в зависимости от способа получения преступниками доступа к денежным средствам:

- Преступления, которые совершаются с использованием методов социальной инженерии в отношении держателей карт.
- Преступления, совершаемые путем физического воздействия на платежные терминалы (механические взломы, взрывы, хищения банкоматов).
- Преступления, направленные непосредственно на сами денежные средства, которые похищаются непосредственно из сейфа банкомата или с помощью монтажа определенного устройства на механизм, отвечающий за выдачу денежных средств (скимминг, траппинг, кэш-траппинг, Black Box и Drilled Box).
- Преступления, направленные на банковскую карту или ее реквизиты («ливанская петля»).
- Преступления, направленные на получение ПИН-кода и магнитного трека банковской карты, чтобы в дальнейшем использовать эту информацию в своих корыстных целях – изготовить дубликат карты и снять денежные средства (фарминг как установка фальшивого банкомата).
- Кибермошенничество (имитация банковского сайта).
- Кибератаки (подключение к системам администрирования; получение реквизитов карты путем незаконного доступа в систему банкомата и к каналам его связи).

Рост информационных технологий в России, как и во всем мире, обусловил расширение сфер применения мобильных

технологий, платной дистрибуции контента через мобильные магазины производителей популярных моделей телефонов, мобильных платежей, интернет-банкинга с подтверждением транзакций по SMS и банковским мобильным приложениям в предпринимательской деятельности и в повседневной жизни. При таких условиях развитие технологий непременно создает предпосылки для их использования в преступных целях.

Все новое – это хорошо забытое старое. Подобного мнения придерживаются и преступники. Тут следует отметить, что одним из частых способов хищений является способ из области социальной инженерии. Его особенность состоит в том, что не используется какое-либо оборудование или хитрый способ извлечения денег, а только банковская карточка злоумышленника и преступная группа из нескольких человек.

Данные преступления совершаются не в офисах банков, а в иных точках установки устройств самообслуживания, при этом подбирается момент, когда будут отсутствовать посторонние свидетели преступного деяния. Суть хищения состоит в том, что человек, подходя к банкомату или банковскому терминалу, видит, что предыдущий клиент забыл банковскую карточку, и, как правило, достает ее из картоприемника или просто берет ее в руки. В этот момент подходит злоумышленник и сообщает, что потерял или забыл карту, а через некоторое время, спохватившись, указывает на отсутствие определенной суммы на своем счету, обвиняет в этом человека. После появляется «свидетель», который все видел, и человеку предлагается вернуть деньги без вызова полиции, ведь на карточке его отпечатки пальцев и следует решить все «мирным» путем.

В данной ситуации большинство людей соглашается отдать свои деньги, а злоумышленники скрываются с места

преступления. Опасность такого способа хищения состоит в том, что оно направлено на самые незащищенные категории людей, как правило пенсионеров, которые не могут дать отпор, теряются и отдают собственные деньги преступникам. В последнее время рассматриваемый способ мошенничества встречается все чаще, что вызывает закономерные опасения, особенно с учетом практической невозможности расследования данного преступления, в том числе при условии, что большинство людей не обращаются за помощью в правоохранительные органы.

В настоящее время продолжает сохранять актуальность вопрос противодействия преступлениям, совершенным с использованием скиммингового оборудования.

Скимминг предназначен для копирования данных с карты путем установки перед картридером специального устройства «скиммера», имитирующего по внешнему виду стандартное оборудование устройства самообслуживания, таким образом, чтобы клиент, пользующийся им, визуально не замечал установленного внештатного оборудования. Вместе с накладкой на картоприемник (со встроенным считывателем магнитной полосы карты), накладкой на клавиатуру устройства самообслуживания (предназначенной для получения ПИН-кода) устанавливается вторая накладка в виде пластиковой планки с вмонтированной микровидеокамерой и собственным цифровым носителем, например микрофлэшкартой либо передатчиком GSM (для фотофиксации и сохранения ПИН-кода карты).

Известны случаи, когда считывающее устройство устанавливается на входной двери офиса банка. Это происходит в том случае, когда устройство самообслуживания работает

круглосуточно и находится в закрытом помещении, куда доступ возможен только с помощью банковской карты, помещаемой в картридер на входной двери. Именно на него и устанавливается оборудование.

Используемое скимминговое оборудование полностью совпадает по цвету и размеру со штатным оборудованием банкомата, на которое оно устанавливается (рис. 19).

Рис. 19. Пример исполнения скимминговой оборудования

Данное оборудование, как правило, изготавливается в странах Восточной Азии и заказывается через распространенные интернет-магазины alibaba.com или aliexpress.com. По прибытии в Россию данные накладки дорабатываются «местными умельцами» до оборудования, предназначенного для негласного получения информации.

Доработанное скимминговое оборудование крепится на устройство самообслуживания с помощью клейкой массы или двусторонней клейкой ленты. Данное оборудование чаще всего устанавливают ранним утром, а снимают поздно вечером. Тем самым преступники сводят к минимуму количество возможных очевидцев (рис. 20–21).

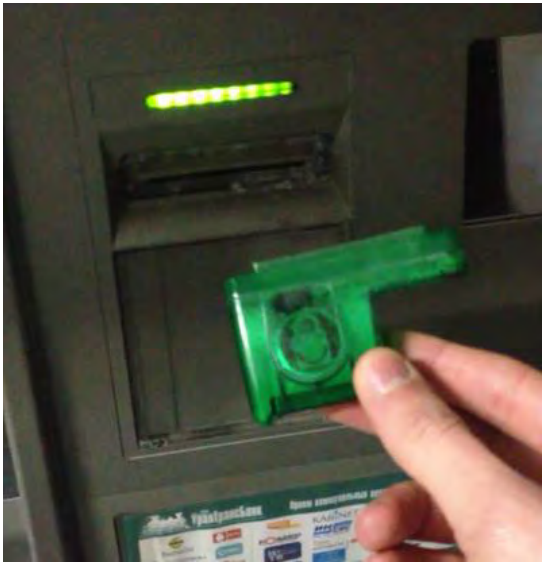


Рис. 20. Процесс установки скимминговой оборудования

Рис. 21. Пример изображения, полученного с помощью скимминговой оборудования

После того как оборудование снято с устройства самообслуживания, полученные данные с магнитной полосы кредитной карты копируются с носителя, вмонтированного в скимминговое оборудование, на персональный компьютер. Далее создаются дубликаты банковских карт, магнитные полосы которых были считаны ранее. Созданные дубликаты получили название «белый пластик» (рис. 22).

Рис. 22. Пример исполнения «белого пластика»

Еще несколько лет назад при помощи данных карт происходило значительное количество хищений денежных средств со счетов законных владельцев карт. Однако в настоящее время это сделать стало достаточно затруднительно, так

как большинство банков перешло на карты со встроенным микрочипом, соответственно, устройства самообслуживания этих банков обрабатывают только карты, имеющие подобный чип.

Следует отметить, что скимминговое оборудование постоянно совершенствуется: устанавливается в недоступных для обнаружения местах (внутрь картоприемника), уменьшается в размерах, снабжается техническими устройствами для передачи считанной информации с использованием беспроводных технологий (GSM, 3G, 4G и др.). В ряде случаев отмечается использование нового вида скимминговых оборудования – перископного. Факт появления новых скимминговых устройств свидетельствует об актуальности и перспективности использования данного оборудования преступниками, необходимости выработки способов противодействия использованию данного оборудования со стороны правоохранительных органов и сотрудников финансово-кредитных учреждений.

Следует выделить разновидность скимминга, которая получила название шимминг. Так, для противоправного доступа к устройству самообслуживания используется специальное электронное устройство, представляющее из себя гибкую плату толщиной около 0,2 мм. Опасность заключается в том, что данное устройство практически полностью незаметно для держателя карты. Для совершения противоправного деяния злоумышленник помещает шиммер в щель картридера, после чего происходит считывание данных банковской карты. Рассматриваемое устройство используется в комплексе со специализированными приспособлениями, например накладками на клавиатуру устройства самообслуживания, миниатюрными видеокамерами, посредством которых производится считывание ПИН-кода пользователя.

Особую актуальность исследования данного вида преступления вызывает тот факт, что в настоящее время единственная возможная защита от шимминга – это использование пластиковых карт, оснащенных чипом.

Безусловно, в России скимминг уже не так распространен, поскольку банкоматы стали оснащаться чипами безопасности, благодаря чему копирование магнитной полосы потеряло свою актуальность. Скопировав и расшифровать данные с чипа достаточно сложно, а воспользоваться копией без данных не представляется возможным.

Кроме того, мошенники чаще всего снимали деньг с копированных карт за пределами Российской Федерации, что стало также невозможным ввиду санкций международных платежных систем.

Однако, это не значит, что такой способ хищения полностью утратил свою актуальность. В силу тех же санкций граждане России стали активно оформлять карты в банках за рубежом, в связи с чем у шиммеров появилась возможность похищать данные с карт, у которых неправильно настроены чипы. А в некоторых государствах наличие чипа или безопасной магнитной полосы и вовсе не считается обязательным требованием.

Следующий способ хищения персональной информации клиента банка и денежных средств – траппинг или «ливанская петля». Данный способ был придуман мошенниками для получения банковской карты и ее ПИН-кода более простым способом, чем скимминг. Происходит это следующим образом: правонарушитель вставляет в картридер устройства самообслуживания блокиратор (как правило, в качестве него используется обычная фотопленка), который препятствует возврату карты из устройства самообслуживания.

Клиент вводит банковскую карту в устройство, где она блокируется, как следствие, он не может получить ее обратно. В подобных случаях клиент находится в замешательстве и не знает, что ему делать. Далее правонарушитель, представившись сотрудником банка, подходит к клиенту и начинает ему «активно помогать».

Мошенник предлагает ввести ПИН-код одновременно с нажатием одной из клавиш, к примеру «Ввод» или «Отмена». В том случае, если клиент вводит ПИН-код, мошенник запоминает его и еще какое-то время пытается «помочь клиенту». Соответственно, клиенту банка не удается получить свою карту обратно, и мошенник предлагает обратиться в банк с заявлением на возврат карты из устройства самообслуживания. Клиент уходит, а мошенник достает из банкомата «ливанскую петлю» вместе с банковской картой и, используя зафиксированный ранее ПИН-код, снимает все денежные средства, нередко на том же банкомате или банковском терминале.

Одним из видов траппинга является кэш-траппинг, когда накладка устанавливается на кэш-диспенсер и препятствует выдаче наличных денежных средств из устройства самообслуживания в целях их последующего извлечения мошенниками.

Еще один вид мошенничеств с платежными картами – фарминг. Выделяют два вида такого мошенничества:

- Имитация банковского сайта.
- Фальшивое устройство самообслуживания.

Интересен второй вид, когда устройство самообслуживания на некоторое время «зажевывает» карту и клиенту ка-

жется, что он просто неисправен. Но затем карта возвращается клиенту, правда без выполнения заданной задачи банкоматом или банковским терминалом. За это время устройство самообслуживания успевает считать и скопировать данные карты, а установленная в помещении или непосредственно над клавиатурой в устройстве портативная камера записывает момент ввода клиентом ПИН-кода.

Следующий типичный способ хищения денежных средств из устройства самообслуживания или с их использованием – кибератаки. Данный способ является относительно новым, но одним из наиболее распространенных на сегодняшний день видов преступлений, связанных с банковскими устройствами.

Анализируя кибератаки, необходимо помнить, что современный банкомат или банковский терминал – это в первую очередь компьютер, запрограммированный на решение определенных задач, но пригодный к запуску любого кода, в том числе вредоносного. Устройство самообслуживания, как и любой другой компьютер, контактирует со многими специализированными устройствами, через которые его можно взломать. Но можно и не взламывать, перехватив управление устройством для выдачи наличных или клавиатурой для ввода ПИН-кода.

Обычно банкоматы и терминалы очень хорошо защищены по сравнению с иными устройствами, но и внимание к ним у киберпреступников намного выше: на кону реальные денежные средства.

Несмотря на то, что лишь в последние несколько лет кибератаки на устройства самообслуживания получили значительное распространение, одна из первых версий программы, предназначенной для данной цели, – Skimer появи-

лась еще в 2008 г. Данная программа была специально создана для организации атак непосредственно на банкоматы и банковские терминалы: после заражения устройства им можно было управлять, вставив в него подготовленную карту с «ключом» на магнитной полосе.

В соответствии со своим названием вредоносная программа Skimer может активировать сбор данных с вставляемых в устройство самообслуживания карт, ее также можно использовать и для хищения наличных денежных средств – соответствующая команда предусмотрена в меню управления. Skimer встраивается в легитимный процесс SpiService.exe, в результате чего получает полный доступ к XFS – универсальному клиенту – серверной архитектуре финансовых приложений для Windows-систем. Обмен сообщениями с процессинговым центром происходит по direct connect – протоколам (NDC или DDC), пользователи общаются с GUI, а за работу каждого модуля устройства отвечают соответствующие сервис-провайдеры (своеобразные шлюзы в эти модули). Для трансляции команд в сервис-провайдеры и далее в оборудование, а также для возврата статусных сообщений используется уровень, называемый XFS Manager, согласно концепции WOSA.

В начале 2020 г. в Москве злоумышленником были инициированы сбои в терминалах, приведшие к неправомерному зачислению денежных средств на счета преступника. Таким способом злоумышленник совершил хищение более 800 тыс. ₽. Впоследствии преступник был установлен, после чего возбуждено уголовное дело по ч. 3 ст. 158 УК РФ

Еще в 2009 г. «уфимские мошенники» одни из первых сумели осуществить хакерскую атаку на компьютерную систему устройства самообслуживания. Взломав сервисный код и установив завышенный курс доллара, злоумышленники обменяли 800 $ на 1,2 млн ₽. По данному факту было возбуждено уголовное дело по пп. «а», «б» ч. 4 ст. 159 УК РФ. Однако даже после задержания одного из хакеров дополнительной квалификации его действий как преступления в сфере компьютерной информации не последовало

В Ставрополе в суд было передано уголовное дело в отношении членов банды – жителей Пермского края. Согласно обвинительному заключению группа из девяти человек похитила более 16 млн ₽ из 22 банковских терминалов, после того как их сообщники взломали систему защиты одного из местных банков. Кражи имели место в гг. Ставрополе, Пятигорске, Кисловодске и Минеральных Водах. Обвиняемые были задержаны в Москве, Санкт-Петербурге, Перми и Краснодаре. Одному из обвиняемых предъявлено обвинение в совершении преступления, предусмотренного ч. 1 ст. 210 УК РФ (руководство входящим в преступное сообщество (преступную организацию) структурным подразделением в целях совершения нескольких тяжких преступлений), ч. 4 ст. 158 УК РФ (тайное хищение чужого имущества, совершенное организованной группой, в особо крупном размере), остальным обвиняемым – по ч. 2 ст. 210 УК РФ (участие в преступном сообществе), ч. 4 ст. 158 УК РФ

Другим примером вредоносного «боевого» программного обеспечения, предназначенного атаковать банкоматы, является программа Tyupkin. В отличие от Skimer атака Tyupkin, исследованная в «Лаборатории Касперского» в 2014 г., не использует подготовленные карты. Вместо этого предусмотрена активация вредоносного кода в определенное время суток, причем даже в это время перехватить управление банкоматом можно только после ввода динамического кода авторизации.

Наиболее интересным является процесс заражения, который подчас приходится восстанавливать по записям камер видеонаблюдения. В случае с Tyupkin вредоносная программа устанавливается с помощью оптического диска, т. е. у правонарушителей изначально имеется физический доступ к внутреннему содержимому банкомата.

Специалисты «Лаборатории Касперского» обнаружили схему хищения денег из банкоматов, связанную с необходимостью дополнительной квалификации как преступления в сфере компьютерной информации. Проверка обращений финансовых организаций привела специалистов к выводу о том, что причиной «произвольной» выдачи банкоматами денежных средств людям, которые никаких действий не производили, было наличие вредоносной программы в компьютере, входящем в единую сеть с банкоматами. Путем неправомерного доступа к персональным компьютерам сотрудников кредитно-финансовых учреждений злоумышленники уже легальными методами вывода средств переводили деньги с помощью системы SWIFT и обналичивали их в банкоматах.

В связи с этим следует отметить, что киберпреступники будут атаковать корневую инфраструктуру финансовых организаций, пока у них будет такая возможность, т. е. пока она будет уязвимой. Как показывает история с хищением через

систему межбанковских переводов SWIFT, даже критически важные элементы финансовой инфраструктуры не всегда защищены должным образом. Банковское сообщество активно устраняет выявленные уязвимости. Однако, учитывая то, что киберпреступники активно работают над совершенствованием существующих и применением новых способов хищения из устройств самообслуживания и с их использованием, именно такие преступления претендуют на сомнительную привилегию долгосрочной «головной боли» финансово-кредитных учреждений и сотрудников правоохранительных органов, занимающихся расследованием подобных преступлений.

Кибермошенники используют следующие наиболее популярные вредоносные программы:

- Trojan.Downloader. Это вредоносная программа, главная цель которой – загрузка и установка на компьютер различных вредоносных и «троянских» программ. Такого рода программы содержат в себе заранее прописанные имена и расположение файлов, скачиваемых загрузчиком с управляющего сервера.
- Trojan.Encoder. Это вредоносная программа, шифрующая файлы на жестком диске компьютера и требующая деньги за их расшифровку. В результате зашифрованными могут оказаться файлы *.doc, *.docs, *.pdf, *.jpg, *.rar и т. д.
- Backdoor. Это вредоносная программа, назначение которой – скрытое от пользователя удаленное управление злоумышленником компьютером жертвы (фактически, по функционалу это программа удаленного администрирования).

- Exploit. Это вредоносная программа, содержимое которой (некоторые данные, исполняемый код) позволяет использовать имеющиеся уязвимости в ПО, установленном на компьютере.
- Trojan. Dropper. Это вредоносная программа, предназначенная для установки на компьютер содержащихся в теле «троянской» программы других вредоносных программ. Обычно установка вредоносных программ происходит без разрешения пользователя и скрытно от него. В некоторых случаях пользователю приходят ложные сообщения об ошибке в архиве, в программе при открытии файла и т. д.
- Trojan. PWS. Это класс вредоносных программ, предназначенных для кражи пользовательских авторизационных данных (логина и пароля, в некоторых случаях – сертификатов пользователей).

Рассмотренные выше виды хищений денежных средств из устройств самообслуживания можно называть технологичными, однако существуют и иные подходы, получившие название механических. Суть состоит в том, что хищение совершается на виду, как правило, в ночное время суток, когда существует минимальная возможность контакта с посторонними лицами. Данные хищения за некоторым исключением прежде всего завязаны на быстродействии, чтобы покинуть место расположения банкомата до приезда охраны или полиции.

В настоящее время подобные способы хищения участились, так как они больше всего не несут с собой существенных затрат на высокотехнологическое оборудование и связаны с механическим воздействием на отдельные части или весь банкомат в целом. Выделяют следующие виды подобных хищений:

- Вскрытие с помощью отмычек или ключей, когда сейф банкомата открывается специальными

отмычками или, например, похищенными ранее ключами уполномоченных лиц, при этом нередки случаи, когда помощь в доступе могут предоставить сами сотрудники банка, выступая пособниками. Как правило, для защиты от подобного вида хищения необходимо использовать магнитоконтактный извещатель.

В Пензе 7 апреля 2020 г. злоумышленник, который ранее занимал должность серверного инженера по обслуживанию банкоматов, с помощью силиконовой маски и одежды, имитирующей инкассаторскую, совершил хищение 23 млн ₽ из банкоматов, расположенных в двух торговых центрах. Однако всего через три дня злоумышленник был задержан, а денежные средства возвращены

- Разрушение внешней и внутренней оболочки банкомата с помощью механического воздействия или высверливания замка. В некоторых случаях данный способ может использоваться и в рабочее время, тогда признаком станет вибрация. Таким образом, защититься поможет вибрационный извещатель.
- Кража банкомата – самый «громкий» способ хищения, при котором банкомат перемещается из места своего нахождения, а денежные средства достаются из него в дальнейшем. В качестве защиты следует предусматривать наличие

магнитоконтактных или электроконтактных датчиков положения и отрыва.

Хотя многие специалисты объективно считают, что способ хищения денежных средств через хищение самого банкомата является устаревшим видом, однако и на сегодняшний день встречаются прецеденты подобных преступлений.

В августе 2021 г. неизвестные вынесли банкомат из межрайонной больницы в Ленинградской области. При этом было похищено более 3,5 млн ₽. Преступники проникли в вестибюль больницы, взломав входную дверь. На месте происшествия были обнаружены лом, гидравлическая тележка, фонарик и инструкция по взлому банкомата. По факту произошедшего возбуждено уголовное дело по ч. 4 ст. 158 УК РФ (кража)

Еще одним примером, вызывающим интерес, является хищение банкомата, произошедшее в Свердловской области 25 апреля 2020 г. Несколько человек ворвались в помещение продуктового магазина, после чего специальными тросами закрепили банковский терминал и выдернули его из помещения посредством автомобиля с закрашенными номерами. Впоследствии сам банкомат обнаружили неподалеку в лесу, все денежные средства были похищены[22]

Взрыв банкомата.

Указанный способ пришел из стран Восточной Европы и Южной Америки. В Европе за 2016 г. насчитывалось более 1 000 взрывов банкоматов. Если еще несколько лет назад в Российской Федерации не было зафиксировано ни одного такого случая, то сейчас практически каждый день совершаются попытки подрывов банкоматов. В основном злоумышленники используют бытовые газы (пропан, бутан и их смеси), которые хорошо подходят для таких целей. Их очень легко раздобыть и практически невозможно отследить ввиду их доступности. Злоумышленник вставляет шланг и электровзрыватель в сейф банкомата, закачивает взрывоопасный газ и производит его поджог. От энергии взрыва банкомат раскрывается, злоумышленник забирает кассеты с деньгами и скрывается. Этот способ отличается от всех других скоростью вскрытия сейфа: группы реагирования часто не успевают предотвратить кражу денежных средств. Информацию, видеоролики и инструкции по подрыву банкоматов можно легко найти на просторах интернета.

Взрыв банкомата опасен не только для денежных средств банков, но и для жизни людей. Уже зафиксированы случаи гибели самих преступников. Злоумышленники не являются специалистами-взрывотехниками, а банкоматы очень часто расположены на первых этажах жилых домов. Неправильно рассчитанное количество взрывоопасного газа может привести к разрушению не только сейфа банкомата, но и близлежащих построек и гибели непричастных людей. Банки начали оснащать свои банкоматы датчиками газа, но из-за скоротечности процесса вскрытия это не позволяет выиграть какое-либо значимое время. На сегодняшний день в России появились устройства, которые позволяют не только

обнаружить взрывоопасный газ в банкомате, но и предотвратить саму возможность взрыва. Для этого в банкомат устанавливают сигнализатор газа и емкость с веществом-флегматизатором. Сигнализатор газа обнаруживает самое начало закачки газа в банкомат и дает команду на подачу флегматизатора. Состав газовой смеси меняется, и взрыв становится невозможен. Крупнейшие российские банки уже начали внедрять решения для противодействия взрывам сейфов в свои банкоматы.

21 апреля 2020 г. в Свердловской области произошел подрыв банкомата. Злоумышленник произвел накачку газа в банкомат, который был расположен в одном из сетевых магазинов, после чего произвел подрыв газа. Впоследствии преступник похитил денежный средства и скрылся с места преступления

Одним из новейших способов хищения и вместе с тем одним из самых труднораскрываемых преступлений является хищение вида Black Box или Drilled Dox.

Black Box – это устройство, подключаемое к внутренней шине банкомата, которое без вскрытия сейфа дает команду на выдачу наличных. Оно устанавливается в верхний кабинет банкомата, а команду на выдачу наличных может получить и удаленно. Человек просто подходит к банкомату, не трогает его, а банкомат начинает выдавать деньги. В связи

с тем, что те, кто устанавливают Black Box, и те, кто забирают деньги, могут быть разными людьми, то практически невозможно доказать что-либо при их задержании.

В настоящее время можно выделить два основных вида атак типа Black Box:

- Программный Black Box, например вирус Tyupkin.
- Аппаратный (или классический) BlackBox. При подобной атаке ЭВМ атакуемого банкомата не задействована. Злоумышленник подключается напрямую к диспенсеру банкнот (через порт или врезаясь в шину) и подает команду по протоколу XFS на выдачу наличных.

Drilled Box представляет собой устаревшую разновидность Black Box. Для доступа к шине данных банкомата злоумышленник сверлит или прожигает отверстие в определенном месте. Эти способы эффективны лишь для достаточно старых устройств, так как в более современных применяется криптозащита передаваемых данных внутри банкомата. Но в любом случае допускать злоумышленников даже в верхний кабинет банкомата нельзя, и его также необходимо оснащать охранной сигнализацией. Вместе с тем Сбербанк России заявил, что некоторые производители пренебрегают подобной защитой, что негативным образом сказывается на общей криминогенной ситуации.

Еще одним примером новейшего вида хищения можно назвать преступления, совершаемые с помощью «специальных» фальшивых денег. Чтобы обмануть банкомат и положить туда фальшивки, мошенники наклеивают на поддельную купюру специальную ленту, после чего банкомат считывает ее как настоящую и зачисляет деньги на счет. Далее

мошенники снимают уже в другом банкомате ту сумму, которая была внесена фальшивками, но получают уже настоящие деньги. Выявить такие преступления сразу достаточно непросто, так как фальшивки обнаруживают после того, как в банкомате заканчиваются наличные деньги и их начинают пересчитывать. Опасность подобного способа хищения заключается в сложности его раскрытия. Как правило, установить злоумышленника можно только по косвенным признакам. Важно отметить, что при указанном способе совершения преступления особую криминалистическую ценность для расследования имеет снятие информации с журналов записей терминалов самообслуживания (лог-файлы), фиксирующих все действия, включая внесение каждой отдельной купюры и совершение любых транзакций. Лог-файл представляет собой «бортовой журнал» компьютера, сервера или коммуникационного оборудования, – последовательную запись технической информации, в которой отражаются в хронологическом порядке все обращения к данному оборудованию и раскрываются сведения о совершенных как локальными, так и удаленными пользователями действиях. Проще говоря, исходя из лог-файла, можно выяснить информацию о том, когда и как преступником совершались те или иные действия.

В Саратове в июле 2020 г. мошеннику удалось вытаскивать деньги из платежного терминала с помощью прочной нити, прикрепленной к пятитысячной купюре. Он много раз опускал купюру в терминал для зачисления на счет и извлекал обратно. Так, преступнику удалось «вытащить» 200 тыс. ₽

В анализе векторов будущих атак на устройства самообслуживания специалисты не ограничиваются непосредственной кражей наличности. К этой цели добавим кражу данных о клиентах для последующего вывода средств в больших объемах с меньшими шансами «засветиться» на камеру наблюдения. Но и это не все. Если присмотреться внимательно, то во всей IT-«обвязке» сети банкоматов не получится найти такое место, которое нельзя было бы атаковать. К основным необходимым мерам, направленным на снижение риска хищений, следует отнести внедрение технологий, связанных с подтверждением операции по альтернативному каналу связи, а также дальнейшее развитие антифрод-систем, в том числе более широкий охват указанными системами каналов проведения операций, включая ДБО, СМС-банкинг. Немаловажным фактором борьбы с несанкционированными операциями может стать внедрение антивирусного программного обеспечения в банковские приложения, устанавливаемые на устройства клиента, а также более точных систем и методов аутентификации клиента.

Интересным примером современного способа защиты устройства самообслуживания от атаки является биометрическая идентификация клиентов – это относительно новая технология, позволяющая либо заменить, либо дополнить стандартные средства авторизации – по ПИН-коду, с помощью NFC и подобных технологий. Кража биометрических данных теоретически возможна через соответствующим образом усовершенствованные скиммеры либо через атаку на инфраструктуру финансовой организации. Однако это достаточно сложное и дорогостоящее действие, не имеющее пока прецедентов. Отметим важный нюанс: если киберпреступники научатся это делать, мы получим аналог ситуации

с «клонированными» кредитными картами, но без возможности «перевыпуска» (отпечатков пальцев, голоса и пр.). И это является одной из основных проблем защиты устройства самообслуживания в ближайшем будущем.

Характерным примером является атака, организованная в июле 2016 г., на банк First Commerce Bank, повлекшая хищение денежных средств из банкоматов на сумму 2,4 млн $. Злоумышленникам удалось совместить самые популярные средства совершения мошеннических действий в течение последних двух лет – фишинговые письма, содержащие вредоносные исполняемые файлы, с системой записи голоса. В результате хакеры получили учетные данные банковских сотрудников, которые дали возможность завладеть устройствами самообслуживания, внедрив вредоносный код. Сама схема атаки довольно сложна. Она началась в лондонском филиале банка, где хакеры использовали систему записи голоса для кражи учетных данных администратора домена и получения доступа к тайваньскому филиалу. После этого, используя поддельный пакет обновления для банкомата, хакеры включили службу Telnet на машинах, что позволило им загружать различные программы. После успешного завершения атаки хакеры удалили все вредоносные программы из банкомата.

В мае 2021 г. М. загрузил в банкомат Россельхозбанка 521 купюру из «банка приколов» номиналом 2 тыс. ₽ на общую сумму более 1 млн ₽, перевел сумму на несколько банковских карт и обналичил. Банкомат считал сувенирные деньги как настоящие. Возбуждено уголовное дело о мошенничестве

Исследователи из Италии и Нидерландов разработали метод машинного обучения, способный определять вводимый человеком ПИН-код в устройство самообслуживания. Новый метод работает даже в тех случаях, когда клиент устройства прикрывает рукой панель ввода.

Разработанный метод включает обучение сверточной нейронной сети (CNN) и модуля долгосрочной краткосрочной памяти (LSTM) на видеозаписях ввода ПИН-кода, прикрытого рукой. Система, отслеживающая движения руки и позиционирование во время ввода ПИН-кода, может предсказать 41 % 4-значных и 30 % 5-значных ПИН-кодов за три попытки (максимальное количество попыток, которое банк допускает перед блокировкой счета клиента). В тестах приняли участие 58 добровольцев, которые использовали случайные ПИН-коды.

Поскольку экран банкомата или банковского терминала вряд ли будет скрыт во время ввода ПИН-кода, время нажатия клавиши может быть установлено путем синхронизации движений руки с появлением «замаскированных» цифр (обычно звездочек), которые появляются на экране устройства в ответ на запрос пользователя. Синхронизация показывает точное расположение рук в «скрытом» сценарии в момент ввода.

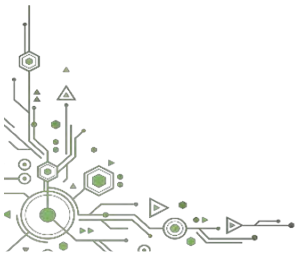
Сбор данных проводился в течение двух сеансов с использованием волонтеров-правшей. Каждый участник набрал 100 случайно сгенерированных 5-значных ПИН-кодов, обеспечивая равномерное покрытие всех 10 возможных нажатий на клавиатуре. Таким образом, исследователи собрали 5 800 индивидуальных вводов ПИН-кода.

Наборы данных были разделены на наборы для обучения, проверки и тестирования, причем обучение проводилось на

процессоре Intel Xeon, работающем на E5-2670 2,60 ГГц и оснащенном 128 ГБ оперативной памяти. Данные были реализованы на Keras 2.3.0-tf (TensorFlow 2.2.0) и Python 3.8.6 на трех графических процессорах Tesla K20m с 5 ГБ видеопамяти каждый.

Рассматривая меры противодействия существующим системам, исследователи считают, что реально действенных средств защиты от такого рода атак не существует. Увеличение минимального числа необходимых цифр в ПИН-коде затруднит запоминание чисел. Случайный порядок расположения цифровых клавиш на программной клавиатуре сенсорного экрана также вызывает проблемы с удобством использования, а защитные пленки для экрана не только будут дорогими для установки на существующие банкоматы и терминалы, но и, возможно, сделают способ атаки еще более простым в реализации. Исследователи утверждают, что их атака работоспособна даже тогда, когда скрыто 75 % клавиатуры (закрытие большего количества затрудняет ввод текста пользователем).

В связи с этим особое опасение вызывают последние тенденции, когда происходит кража биометрических данных человека через телефон (например, человека ненавязчивым разговором подводят к произношению некоторых фраз, которые после обрабатываются специальной программой, подбирающей биометрический ключ) и, хотя эксперты заявляют, что системы защиты в данной отрасли более чем совершенны, сами тенденции вызывают серьезные опасения.



Вопросы для самоконтроля

1. Дайте характеристику видам устройств самообслуживания и укажите их предназначение.
2. Перечислите основные элементы устройства самообслуживания.
3. Охарактеризуйте системы защиты устройств самообслуживания и мест их расположения.
4. Раскройте следующие понятия: «скимминг», «трапинг», «фарминг», «фишинг», «шимминг».
5. Охарактеризуйте способы хищений денежных средств из устройств самообслуживания и с их использованием.
6. Назовите способы заражения устройств самообслуживания вредоносным программным обеспечением, а также суть данной атаки.
7. Опишите признаки наличия на устройстве самообслуживания скрытого скиммингового оборудования.

Глава II

Содержание деятельности сотрудников правоохранительных органов по раскрытию и расследованию преступлений, связанных с хищениями информации и денежных средств из устройств самообслуживания и с их использованием

§ 3.1. Действия членов следственно-оперативной группы при выезде на место происшествия

После сообщения о преступлении, связанном с хищением денежных средств из устройства самообслуживания, на место выезжает следственно-оперативная группа в составе следователя, оперуполномоченного, специалиста-криминалиста, ответственного от руководства. В зависимости от предполагаемого способа хищения в состав группы также может быть включен кинолог.

Еще до момента непосредственного выезда желательно успеть ознакомить специалиста-криминалиста с подробностями произошедшего, чтобы полученная информация помогла ему оперативно принять верное решение о том, какие специальные технико-криминалистические средства будут

ему необходимы при производстве осмотра места происшествия.

Участковый уполномоченный полиции после получения сообщения о преступлении и указания следователя или дознавателя незамедлительно осуществляет меры по установлению свидетелей, обеспечению охраны места происшествия и прочие действия, необходимые к исполнению до приезда следственно-оперативной группы. В случае угрозы уничтожения следов и вещественных доказательств под воздействием дождя, ветра, снега и других факторов участковый уполномоченный полиции принимает меры к их сохранению, закрывая фанерой, ящиками, брезентом, картоном, шифером и другими подручными средствами. Перемещение вещественных доказательств с предварительной фиксацией их первоначального положения допускается лишь в случае возникновения угрозы их порчи или уничтожения по погодным и другим обстоятельствам.

После того как следственно-оперативная группа прибыла на место, ее руководитель осуществляет следующие действия:

- Удаляет посторонних лиц с места происшествия.
- Принимает меры для сохранности следов и обстановки места происшествия.
- Проводит в составе следственно-оперативной группы изучение обстановки на месте происшествия, изучает следы, предметы, орудия преступления и иные вещественные доказательства, которые могут быть использованы для установления истины произошедшего, после чего на основе полученной информации планирует и осуществляет

неотложные мероприятия, необходимые для раскрытия преступления.

Дает поручения оперативным сотрудникам о проведении отдельных оперативно-разыскных мероприятий (ОРМ).

Оперуполномоченный, при наличии участников, принимает от них соответствующие заявления, делает запросы на предоставление данных с камер видеонаблюдения и устанавливает все обстоятельства, изложенные в заявлении. Кроме того, оперативные сотрудники принимают меры по ликвидации последствий происшествия, организации мероприятий по задержанию лиц, участвующих в хищении денежных средств из банкомата, по горячим следам, выявлению очевидцев и других лиц, осведомленных об обстоятельствах происшедшего.

Согласно ст. 166 УПК РФ в ходе производства осмотра места происшествия ведется протокол. Указанное процессуальное действие регламентировано ст.ст. 176–178 УПК РФ. В ходе осмотра следователь путем непосредственного наблюдения, обнаружения, восприятия, закрепления и анализа различных объектов устанавливает их признаки, свойства, состояние, взаиморасположение и определяет их значимость в качестве доказательства по будущему уголовному делу.

Следователь путем измерения, составления черновых записей, схем, фотографирования, видеосъемки фиксирует обстановку на месте происшествия, положение отдельных предметов, их внешний вид, наличие на них видимых следов, расстояние между предметами, состояние самого устройства самообслуживания, имеющиеся на нем повреждения либо приспособления.

При составлении протокола осмотра места происшествия необходимо полно, точно и четко излагать сведения, воздержаться от личностной или эмоциональной оценки произошедшего. При описании и составлении протокола следует идти от общего к частному. Так, сначала производится описание помещения, проводится привязка к иным объектам, сооружениям, указывается адрес места происшествия, после чего осуществляется переход к предметам обстановки и только после этого описываются отдельные объекты.

Следователь (дознаватель) как руководитель следственно-оперативной группы обеспечивает качество, полноту и результативность осмотра места происшествия, в том числе изъятие, упаковку и сохранность изъятых следов преступления. Цель следственного осмотра как раз и заключается в том, чтобы получить доказательства, которые в дальнейшем будут способствовать расследованию преступления.

Исходя из изложенного можно выделить следующие задачи следственного осмотра места хищения из устройства самообслуживания:

- Изучение обстановки места происшествия с выяснением динамики действий лиц, участвующих в хищении из устройства самообслуживания.
- Выявление и фиксация в процессуальных документах всех найденных следов совершенного преступления.
- Установление возможных источников получения новых доказательств.

- Структурирование информации, позволяющей выдвинуть первичные следственные версии.
- Создание первичного аналитического профиля преступника.
- Решение вопроса о приобщении к делу того или иного предмета в качестве вещественного доказательства.
- Проверка собранных по делу доказательств.

Руководитель следственно-оперативной группы обеспечивает указание в протоколе осмотра места происшествия всех участвующих в нем лиц, в том числе ответственных от руководства ОВД. При наличии поводов и оснований, предусмотренных ст. 140 УПК РФ, руководитель следственно-оперативной группы принимает решение о возбуждении уголовного дела в порядке, установленном ст.ст. 146 и 147 УПК РФ. Необходимо помнить, что передача в орган дознания составленного протокола осмотра места происшествия и других собранных материалов при наличии в них признаков преступления не разрешается.

Специалист-криминалист, входящий в состав следственно-оперативной группы, в своей деятельности оказывает всестороннее содействие руководителю группы в осуществлении следующих действий:

- Определение границ места происшествия.
- Выдвижение версий произошедшего.
- Определение перечня и последовательности действий следственно-оперативной группы.
- Осуществление фото- и видеосъемки на месте происшествия.

- Описание обстановки и предметов, которые располагаются на месте произошедшего события.

Фиксация признаков следов и объектов производится при составлении протокола осмотра места происшествия и при детальной масштабной фотосъемке. Расположение следов и объектов определяется по отношению к двум предметам, местоположение которых не изменяется (например, угол дома).

Средства для закрепления и изъятия следов специалист-криминалист применяет после производства фотосъемки, исключив случайное уничтожение следов, а также изъятие следов, оставленных участниками осмотра. Для этого члены следственно-оперативной группы на месте осмотра передвигаются по заранее намеченным маршрутам, а места нахождения следов маркируют (обводят мелом и т. п.) и защищают от случайных повреждений и воздействия окружающей среды, например коробкой или ящиком.

Специалист-криминалист в первую очередь использует для выявления следов и объектов методы, которые не изменяют и не повреждают объект, производит их детальную фотосъемку, предъявляет участникам следственного действия обнаруженные следы и объекты непосредственно на местах обнаружения до их изъятия.

Изъятые следы упаковываются таким образом, чтобы исключить к ним доступ и их повреждение при транспортировке и хранении. Кроме того, упаковка должна иметь пояснительные надписи, удостоверенные подписями понятых и участников осмотра, опечатана органом внутренних дел.

В соответствии с действующим уголовно-процессуальным законодательством (ст.ст. 140, 144 УПК РФ) следователь, руко-

водитель следственного органа обязаны принять, проверить сообщение о любом совершенном или готовящемся преступлении. При этом проверка сообщения о преступлении дает возможность получить дополнительные сведения и материалы, необходимые для правильного разрешения вопроса о возбуждении уголовного дела. Можно согласиться с А. М. Багметом, который указывал: «Проверка сообщения о преступлении является сердцевиной деятельности на стадии возбуждения уголовного дела. Насколько быстро, эффективно и целенаправленно будет проведена доследственная проверка и по ее результатам принято законное и обоснованное процессуальное решение, настолько результативной будет реализация назначения уголовного судопроизводства и обеспечен успех на всех стадиях уголовного судопроизводства»[23].

Среди мероприятий доследственной проверки по указанным преступлениям важна деятельность оперуполномоченных и следователя по обнаружению и изъятию видеозаписей с камер видеонаблюдения, которая включает в себя несколько этапов:

1) проверку информации о наличии камер видеонаблюдения на территории, где произошло преступление. Для этого оперуполномоченный или следователь может обратиться к органам местного самоуправления, управляющим компаниям или другим организациям, имеющим доступ к такой информации;

2) поиск записей с камер видеонаблюдения, расположенных на территории, где произошло преступление. Для этого оперуполномоченный или следователь может использовать различные методы, например обращение к операторам связи или запросы в соответствующие организации;

3) изъятие записи с камеры видеонаблюдения, которая содержит информацию, необходимую для расследования уголовного дела. При этом следователь должен соблюдать все требования закона, касающиеся обработки и хранения персональных данных;

4) анализ полученной информации и составление протокола осмотра места происшествия. В протоколе должны быть указаны все детали, связанные с преступлением, а также информация о том, какие данные были получены в результате изъятия записи с камеры видеонаблюдения;

5) представление доказательств в суде. Если запись с камеры видеонаблюдения является важным доказательством в уголовном деле, то следователь должен представить ее в суд вместе с другими доказательствами.

Многочисленные исследования, проведенные учеными-процессуалистами, статистические данные, публикации в средствах массовой информации свидетельствуют о том, что именно на этапе проверки сообщения о преступлении и первоначальном этапе расследования следователями допускается наибольшее количество упущений по проверке поступившей информации. Например, не всегда соблюдается процессуальный порядок производства следственных действий (проведение которых возможно до принятия решения о возбуждении уголовного дела), что в дальнейшем влечет признание полученных доказательств недопустимыми.

Дополнительные сложности связаны с постоянно изменяющимися нормами уголовного и уголовно-процессуального законодательства. Так, Федеральным законом от 19 февраля 2016 г. № 23-ФЗ «О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уго-

ловно-процессуальный кодекс Российской Федерации» внесен ряд изменений в нормативные правовые акты, которые коснулись, в частности, порядка рассмотрения сообщения о преступлении. Кроме того, законодатель дополнил ст. 144 УПК РФ новыми частями, существенно изменившими ее первоначальную редакцию[24].

Так, урегулирован порядок получения объяснений на стадии возбуждения уголовного дела и их использования в качестве доказательств при расследовании преступлений, расширен перечень процессуальных действий, которые возможно проводить при проверке сообщения о преступлении. Однако внесенные изменения, частично устранив одни сложности, добавили другие.

Например, неоднозначная трактовка положений ч. 1 ст. 144 УПК РФ в части, касающейся возможности изъятия документов и предметов, привела к тому, что некоторые следователи ошибочно считают возможным и производят на этапе проверки сообщения о преступлении такое следственное действие, как обыск или выемка, нарушая тем самым действующее законодательство. Многие ошибки, допускаемые следователями на стадии возбуждения уголовного дела, связаны с отсутствием необходимого опыта и достаточных знаний в области расследования киберпреступлений.

Для решения вопроса о возбуждении уголовного дела необходимы соответствующие повод и основание.

Поводом для возбуждения уголовного дела, согласно ст. 140 УПК РФ, является:

- Заявление о преступлении.
- Явка с повинной.
- Сообщение о совершенном или готовящемся преступлении, полученное из иных источников.

- Постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании.

Основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления.

Заявление о преступлении как один из поводов для возбуждения уголовного дела по факту хищения денежных средств из устройств самообслуживания или с их использованием имеет ряд особенностей.

Заявление о факте совершения преступления может подаваться как в устной, так и в письменной форме. Устная форма оформляется соответствующим протоколом, где указываются данные пострадавшего и документы, удостоверяющие его личность. Лицо предупреждается об уголовной ответственности за ложный донос. Что касается письменной формы заявления о преступлении, то оно подается, как правило, в правоохранительные органы по месту совершения преступления.

В данном заявлении пострадавшему необходимо указать время совершения преступления и место, где именно было совершенно преступление (как правило, это адрес, по которому находится банкомат или банковский терминал), подробно и четко изложить обстоятельства, при которых лицо пострадало от преступления, также следует указать вид и размер ущерба, причиненного преступлением. К заявлению пострадавшего о хищении денежных средств из банкомата или с его использованием могут прилагаться сведения из банка, т. е. владельца банкомата, а именно выписки с расчетных счетов заявителя.

Далее следователь проводит проверку данного сообщения, и если факт совершенного преступления находит свое подтверждение в результате предварительной проверки, то следователь возбуждает уголовное дело, о чем выносится соответствующее постановление.

Уголовное дело по данному виду преступления может возбуждаться без заявления потерпевшего в том случае, если сообщение о факте хищения денежных средств поступило из иных источников. Такими источниками могут быть письменные сообщения от общественных организаций и иных учреждений, опубликованные в средствах массовой информации и содержащие сведения о совершенном или готовящемся преступлении. В данном случае следователь после соответствующей проверки принимает решение о возбуждении уголовного дела.

Нередко факт установки внештатного оборудования (используемого для хищения денежных средств) на устройствах самообслуживания выявляется сотрудниками банков при проведении их осмотра. «Как сообщили в пресс-службе Дальневосточного Сбербанка, банк принял оперативные меры по расследованию причин данных транзакций. Пострадавшим клиентам необходимо обратиться в любой филиал Сбербанка России и составить претензионное обращение о несанкционированном списании средств с карты. По каждому обращению будет проведено оперативное расследование. Клиентам, пострадавшим от мошеннических операций, средства будут возмещены в полном объеме и в самое ближайшее время. В настоящее время Сбербанк России блокирует скомпрометированные банковские карты только тех клиентов, которые написали обращение в Банк», – говорится в сообщении пресс-службы Сбербанка России[25].

При выявлении внештатного оборудования (как правило, это происходит путем получения обращения от работников банка, граждан, а также в ходе проведения оперативно-разыскных мероприятий), установленного на банкоматы по самообслуживанию клиентов банков, о данном факте незамедлительно докладывается руководителю соответствующего подразделения органов внутренних дел, после чего принимаются безотлагательные меры по проведению оперативно-разыскных мероприятий в следующих целях:

1) для установления правонарушителей, фиксации их действий и задержания, для чего необходимо провести ОРМ «наблюдение» (после проведения данного ОРМ составляется акт наблюдения в произвольном порядке, но с обязательным соблюдением норм и правил, предъявляемых к доказательствам согласно УПК РФ), при этом необходимо установить наблюдение как за банкоматом (или терминалом самообслуживания), на котором установлено внештатное оборудование, так и прилегающей к банкомату территорией. Своевременное проведение данного ОРМ необходимо для установления возможных соучастников преступления. Для проведения ОРМ «наблюдение» рекомендуется привлекать как штатных, так и внештатных сотрудников органов внутренних дел;

2) установления непосредственного визуального контакта за заподозренным, для чего необходимо провести видеозапись происходящего (видеозапись можно производить как на магнитные, так и на цифровые носители информации). Видеозапись необходима для фиксации действий заподозренного, а именно: его перемещений, встреч с возможными соучастниками, при задержании заподозренного необ-

ходимо фиксировать возможный «сброс» технического оборудования. Кроме того, необходима фиксация первоначального объяснения задержанного;

3) задержания. Следует составить соответствующий протокол, произвести личный досмотр, при котором следует акцентировать внимание на выявление технических устройств (скимминговое оборудование, видеокамеры, электронные носители информации), другие технические и электронные устройства (ПК, ноутбуки, планшеты, карты памяти, переносные HDD и т. п.);

4) установления наличия используемого автотранспорта. При его обнаружении необходимо организовать задержание и последующий осмотр;

5) установления соучастников. Следует ориентировать личный состав полиции на их задержание; при задержании соучастников заподозренного – организовать в их отношении вышеперечисленные мероприятия;

6) принятия мер к установлению мест проживания заподозренного и его соучастников.

При подтверждении полученной информации и установлении признаков преступления незамедлительно решается вопрос о возбуждении уголовного дела по рассматриваемому факту хищения денежных средств из устройства самообслуживания или с его использованием. Соответствующая квалификация противоправного деяния зависит от момента выявления преступления и способа совершения хищения денежных средств. К примеру, уголовное дело при совершении хищения денежных средств из устройства самообслуживания с использованием скимминговой оборудования возбуждается, как правило, по совокупности соответствующих частей ст.ст. 138.1, 158, 183 и 187 УК РФ.

§ 3.2. Особенности осуществления отдельных следственных действий на различных этапах расследования

При выявлении факта совершения хищения денежных средств из устройств самообслуживания и с их использованием следователем возбуждается уголовное дело, о чем он выносит соответствующее постановление. Далее ему необходимо произвести первоначальные следственные действия, которые направлены на формирование более полной картины преступления, а также для установления обстоятельств, подлежащих доказыванию (ст. 73 УПК РФ).

Одним из первоначальных следственных действий, которое необходимо произвести следователю по факту хищения денежных средств из банкоматов и с их использованием, нередко является осмотр места происшествия. Качество данного следственного действия имеет ключевое значение для установления всех обстоятельств совершенного деяния, а также для выявления лиц, которые совершили данное преступление.

Перед проведением осмотра места происшествия необходимо произвести следующее:

- Установить круг лиц, необходимых для проведения данного следственного действия.
- Определить задачи и последовательность их выполнения для каждого члена СОГ, которая выехала на осмотр места происшествия.
- При необходимости пригласить соответствующих специалистов, заранее их предупредить о важности

использования специального технического оборудования и материалов.

- Перед началом следственного действия разъяснить участникам их задачи, права и обязанности в соответствии с УПК РФ.

В ходе первоначального осмотра места происшествия необходимо детально осмотреть само устройство самообслуживания и прилегающую к нему территорию. При этом следует осмотреть не только сам банкомат или терминал, но и предметы, которые находятся в непосредственной близости к нему. В случае если имеются основания полагать, что осматриваемый банкомат или банковский терминал оборудован таким внештатным оборудованием, как скимминговое устройство, следует обратить внимание на наличие внештатной видеокамеры, считывателя магнитной полосы, накладки на клавиатуру. Необходимо выявить на устройстве самообслуживания наличие следов ранее установленного оборудования, такие как остатки клея на клавиатуре устройства, следы установки видеокамеры и т. д. В том случае, если нарушена целостность устройства и денежные средства похищены из его сейфа путем его взлома (взрыва), то следует детально описать повреждения, которые имеются.

Таким образом, основными аспектами, на которые необходимо обратить внимание при проведении осмотра места хищения из устройства самообслуживания, являются:

- Осмотр места введения карты, в том числе с выяснением возможности использования специального оборудования или следов его использования. В первую очередь следует обратить внимание на возможное наличие скиммеров, микрокамер, «ливанские петли» и т. д.

- Осмотру подлежит верхняя часть банкомата, в том числе место над банкоматом, место над монитором и под ним.
- Исследуется клавиатура для введения ПИН-кода в целях поиска накладок или их следов, микрокамер и т. д.

При осмотре места происшествия необходимо тщательно проверить устройство самообслуживания и помещение, в котором он установлен, на наличие следов пальцев рук, потожирового вещества, иных следов человека. Данная процедура на практике не всегда является эффективной, так как количество лиц, которые пользовались данным банкоматом до и после установления на него внештатного оборудования или при ином преступлении, установить сложно, соответственно, идентифицировать следы этих лиц зачастую не представляется возможным.

Все следы преступления, которые будут обнаружены при осмотре места преступления, в том числе обнаруженное внештатное оборудование, фиксируются в протоколе осмотра места происшествия и изымаются. Также необходимо изъять образцы вещества или предметов, с помощью которых осуществлялось крепление внештатного оборудования к банкомату.

Следует учитывать, что при первичном осмотре места происшествия следователю затруднительно без соответствующего запроса изъять документы из автоматизированных охранных систем наблюдения. Кроме того, данные затруднения нередко связаны с отсутствием необходимого специалиста при осмотре или отсутствием представителя банка, которому принадлежит терминал[26].

Следователю необходимо изъять видеодокументы из охранных систем наблюдения, расположенных при входе

в помещение, где установлен банкомат, а также на соседних зданиях. В дальнейшем может помочь следователю в установлении соучастников преступления, путей отхода, характеристик транспортного средства, на котором прибыл преступник к месту совершения преступления.

Таким образом, своевременный, полный, тщательно спланированный осмотр места происшествия при расследовании хищения денежных средств из банкоматов или с их использованием, а также тактически правильный порядок его проведения позволят следователю спланировать дальнейший ход расследования.

После осмотра места происшествия целесообразно назначить соответствующие судебные экспертизы.

Дактилоскопическая экспертиза проводится в том случае, если были обнаружены следы пальцев рук на банкомате (банковском терминале) или прилегающей территории и имеются основания полагать, что данные следы мог оставить преступник.

Химическая экспертиза назначается в целях установления происхождения, идентификации, сравнения веществ, использовавшихся при монтировании на банкоматы (банковские терминалы) внештатного оборудования.

Примерные вопросы, задаваемые при назначении химической экспертизы:

- Какое именно вещество, представленное на экспертизу, обнаружено в ходе осмотра места происшествия (банкомата / банковского терминала)?
- Однородны ли по своему химическому составу фрагменты вещества, изъятые в ходе осмотра места происшествия (банкомата / банковского терминала), с клейким веществом во флаконе из полимерного материала, изъятым

в ходе осмотра места происшествия – парковки, расположенной по адресу при осмотре автомашины?

- Однородны ли по своему химическому составу фрагменты вещества, изъятые в ходе осмотра места происшествия (банкомата / банковского терминала), с клеем, изъятым в ходе личного досмотра задержанного?

Портретная экспертиза назначается в том случае, если имеется видеозапись с видеокамеры, установленной на устройстве самообслуживания, а также с видеокамер помещения, где он располагается, на которой запечатлено лицо, совершившее преступление. Портретная экспертиза назначается для идентификации лиц, изображенных на видеозаписях с камер видеонаблюдения. Для производства экспертизы эксперту необходимо предоставить носитель с записями, а также фотоизображения лиц, относительно которых проводится экспертиза.

Примерные вопросы, задаваемые при назначении портретной экспертизы:

- Имеются ли на видеозаписи с камеры в период времени с... по... ?
- Имеются ли изображения внешности подозреваемых?
- Одно и то же или разные лица изображены на фрагменте видеозаписи с камеры с показателями числового и временного маркеров с... по... и на изображениях подозреваемого?

Механоскопическая экспертиза необходима в том случае, если денежные средства были похищены из банкомата путем взлома сейфа банкомата. Устанавливается, каким именно способом и какими орудиями было совершено действие.

Молекулярно-генетическая экспертиза назначается при необходимости идентификации биологических следов, обнаруженных на месте происшествия, с ДНК-профилем заподозренного лица.

Радиотехническая экспертиза проводится в целях установления объективных фактов использования радиоэлектронных средств в качестве орудий подготовки, совершения или сокрытия совершенного преступления. Объектами радиотехнического экспертного исследования при раскрытии и расследовании преступлений, связанных с хищением денежных средств из устройств самообслуживания, чаще всего являются скимминговые устройства, «блэк-боксы», программаторы, энкодеры и постановщики заградительных радиопомех.

Примерные вопросы, решаемые в рамках радиотехнических экспертиз:

- Какова функциональная принадлежность представленного на исследование средства (каково его функциональное назначение)?
- Каков способ изготовления представленного средства?
- Возможно ли при помощи представленного устройства осуществить... (дать перечень действий)?
- Соответствует ли представленное устройство категории специальных технических средств, предназначенных для негласного получения информации?

Компьютерная (компьютерно-техническая) экспертиза проводится в том случае, если на банкомат была совершена компьютерная атака, в ходе которой и были похищены денежные средства.

Экспертиза материалов, веществ и изделий назначается в случае необходимости исследовать какие-либо вещества,

например следы материи от перчаток, оставленных преступником на скимминговом оборудовании.

Типичным видом процессуальной формы взаимодействия в этом случае является поручение следователя сотрудникам органа дознания о производстве отдельных следственных действий и оперативно-разыскных мероприятий.

Если уголовное дело возбуждается по заявлению потерпевшего, необходимо допросить его. Согласно ст. 190 УПК РФ ход и результат допроса отражаются в протоколе, составленном в соответствии со ст.ст. 166 и 167 УПК РФ.

В ходе допроса следователю необходимо соблюдать установленный законодательством порядок. Выяснение фактов у потерпевшего зависит от характера и способа совершения хищения денежных средств. В том случае, если в отношении лица было совершено ограбление в момент снятия или внесения денежных средств на свой счет в банке с помощью банкомата, тогда необходимо выяснить данные, которые потерпевший запомнил о лице, совершившем ограбление, а именно: рост, отличительные черты внешности, во что был одет преступник иные особые и броские приметы. В том случае, если преступные посягательства направлены на банковскую карту потерпевшего, то на допросе уточняется сумма материального вреда, причиненного преступлением.

§ 3.3. Особенности назначения компьютерных (компьютерно-технических) судебных экспертиз

Раскрытие и расследование преступлений, совершенных с использованием банковских устройств самообслуживания, невозможно без производства судебных компьютерных (компьютерно-технических) экспертиз. В ходе проведения такого рода исследований может быть получена информация о связи между злоумышленниками, внешнем облике участников преступной деятельности, причастности лиц к совершаемым правонарушениям. Часто материалы, обнаруженные экспертами, позволяют установить организаторов, объединить уголовные дела в одно производство, выделить организованную преступную группу.

В экспертной практике регулярно встречаются дела, в которых информационно-телекоммуникационные технологии и средства вычислительной техники используются на всех стадиях совершения правонарушения. В большей степени это обусловлено возможностью достичь анонимности, которая существенно затрудняет раскрытие и расследование.

Для решения задач, связанных с экспертно-криминалистическим сопровождением преступлений, совершенных в целях хищения денежных средств из устройств самообслуживания, в экспертно-криминалистических подразделениях (ЭКП) системы МВД России организовано производство компьютерных судебных экспертиз. Их главное отличие от компьютерно-технических экспертиз, проводимых в большинстве ведомственных экспертных учреждений правоохранительных органов, состоит в объекте исследования – исключительно компьютерной информации. Эксперты МВД России не в праве отвечать за техническое состояние средств

вычислительной техники, работоспособность и исправность (эти задачи решаются в рамках радиотехнических экспертиз, проводимых в ЭКП), а также проводить исследования, объектами которых будет являться динамическое (изменяемое) информационное пространство. При этом в ЭКП также могут назначаться компьютерные экспертизы, объектами в которых будет сетевое оборудование.

Применяемые государственными экспертными учреждениями методы исследований в основном позволяют решать задачи, поставленные органами предварительного расследования. Имеющиеся в рассматриваемой сфере методики являются общими и дают возможность отвечать на вопросы, выносимые при расследовании преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, в том числе в области дистанционного банковского обслуживания.

Для назначения судебных компьютерных и компьютерно-технических экспертиз следователю необходимо обладать элементарными знаниями об устройстве банкомата (банковского терминала) и основных принципах его функционирования (рис. 23).

В состав банкоматов входят: компьютер с установленным на нем программным обеспечением; специальные устройства, которые считывают данные, позволяющие идентифицировать клиента; оборудование, отвечающее за прием, хранение, и выдачу денежных средств. Все больше устройств самообслуживания оснащают дополнительным оборудованием, повышающим его безопасность. К таким устройствам можно отнести антискимминговые приборы и приспособления, охранные сигнализации, средства полу-

чения и хранения видеоинформации (камеры и видеорегистраторы). Производители устройств самообслуживания поставляют в комплекте с ними специальное программное обеспечение – библиотеку базовых программных модулей для формирования прикладной системы или для непосредственного использования в аппаратах.

Рис. 23. Банкомат, представленный
на судебную компьютерную экспертизу

Идентификация клиента в банковских устройствах самообслуживания осуществляется с помощью информации с платежной карты (магнитной полосы, микроконтроллера или NFC-метки), специальным кодом, вводимым на клавиатуре (пользовательским кодом и ПИН-кодом), сигналом, генерируемым смартфоном, или биометрическими данными. При успешной авторизации банкомат разрешает допуск пользователя к банковским сервисам и тем самым проводит операции, которые необходимы пользователю. Одним из самых распространенных действий является выдача наличных денежных средств.

Предназначенные для выдачи наличные денежные средства хранятся в специально оборудованных для этого кассетах, которые находятся в сейфовом отсеке банкомата. Как правило, сейфовая часть защищена более надежно по сравнению с аппаратной. Купюры, которые были забыты клиентом или отбракованы банкоматом, попадают в специальную, так называемую возвратную, кассету.

Основная цель судебной компьютерной экспертизы (СКЭ) состоит в изучении закономерностей функционирования информации в средствах вычислительной техники (СВТ).

Выявление, фиксация, изъятие и исследование криминалистически значимой компьютерной информации, представленной в памяти устройств и на электронных носителях, в том числе удаленной, зашифрованной или скрытой, является основной задачей судебной компьютерной экспертизы.

К задачам СКЭ относятся:

1) установление фактических обстоятельств на основе изучения закономерностей функционирования информации в СВТ;

2) поиск на машинном носителе (в СВТ) информации, созданной с помощью прикладных программ, сведений о действиях пользователя (процессах обработки файлов, ведении баз данных, работе в сетях передачи данных и др.);

3) определение свойств программ и программных продуктов, принадлежности программ и данных к конкретным классам;

4) установление материальных объектов по компьютерной информации (проводится в комплексе с другими видами экспертиз);

5) определение возможности совершения каких-либо действий с помощью СВТ;

6) установление фактических обстоятельств совершения преступления (проводится при наличии информации, полученной из различных источников).

Объект СКЭ – компьютерная информация, имеющаяся на электронных носителях, отдельных технических средствах и функциональных устройствах систем обработки информации и в системах обработки информации в целом.

Предметом экспертного исследования являются фактические данные (сведения) о содержимом памяти устройств, модулей идентификации абонента (SIM-карт), встроенных и съемных накопителей информации различного типа, а также о данных, находящихся в оперативной (временной) памяти компьютеров и компьютерных устройств различного назначения, исследуемые и устанавливаемые на основе специальных знаний в области информатики и вычислительной техники, информационной и компьютерной безопасности, радиотехники, автоматизации, систем управления и связи.

Знание особенностей исследования мобильных устройств и электронных носителей информации как объектов судебной компьютерной экспертизы зависит от понимания характеристик аппаратного и программного обеспечения компьютерных систем. Способность разбираться в структуре хранения информации поможет решить проблемы, возникающие при экспертном исследовании. Сведения из электронной почты, социальных сетей, программ персональной связи через информационно-телекоммуникационную сеть Интернет также важны для расследования, поскольку информация о контактах, переписке и т. п. содержится именно там.

При раскрытии и расследовании преступлений, связанных с хищением денежных средств из устройств самообслуживания, часто изымаются мобильные телефоны. Они могут использоваться злоумышленниками как для коммуникации с другими участниками преступных групп, так и непосредственно для совершения хищений, например для управления вредоносным программным обеспечением, внедряемым в банкомат.

Современные мобильные устройства способны выполнять ряд функций – от обычного цифрового органайзера до персонального компьютера. Они содержат микропроцессор, постоянное запоминающее устройство, оперативное запоминающее устройство, аналого-цифровой преобразователь, микрофон и громкоговоритель, ряд аппаратных ключей и интерфейсов, жидкокристаллический дисплей. Операционная система (ОС) находится в постоянном запоминающем устройстве, которое с помощью специальных средств обычно может быть стерто и перепрограммировано. Пользовательские данные, хранящиеся в оперативном запоминающем устройстве, поддерживаются с помощью источника

электрического питания, отключение которого приводит к потере данных.

Существующая классификация мобильных устройств условна, тем не менее при разделении по типу используемой ОС возможно выделение двух основных групп устройств: Apple iOS и Android. По типу исполнения устройств возможно их разделение на мобильные компьютеры и мобильные средства коммуникации.

Доступ к информации, как правило, зависит от состояния (включено, выключено, заблокировано или нет), в котором находится устройство, и от наличия кода блокировки.

Исследование некоторых видов объектов, поступающих с постановлениями о назначении компьютерных экспертиз, требует их включения. При проведении исследования мобильных устройств путем включения возможно внесение изменений в содержимое памяти по причинам, не зависящим от эксперта. Вместе с тем в соответствии с п. 4 ст. 57 УПК РФ эксперт не вправе: проводить без разрешения дознавателя, следователя, суда исследования, могущие повлечь полное или частичное уничтожение объектов либо изменение их внешнего вида или основных свойств. Кроме того, для исследования некоторых типов мобильных устройств требуется их частичная разборка. Если следователь согласен с внесением изменений в содержимое памяти исследуемых объектов, а также применением при проведении экспертизы разрушающих методов исследования (при наличии такой необходимости), ему следует дать на это согласие в постановлении.

Наиболее часто встречающееся средство хранения информации в компьютере – накопитель на жестких магнит-

ных дисках (НЖМД). Современные НЖМД отличаются высокими показателями емкости, скорости, надежности, а также самой низкой стоимостью за мегабайт сохраняемой информации. На них обычно хранится ОС, прикладные программы и обрабатываемые данные.

Вместе с тем в современных компьютерах все чаще вместо НЖМД устанавливаются твердотельные накопители – немеханические запоминающие устройства на основе микросхем памяти. Наиболее распространенный вид твердотельных накопителей используется для хранения информации флеш-памяти типа NAND. Посредством команды TRIM контроллеру SSD-накопителя передается массив адресов блоков, которые должны быть очищены. С этого момента начинается фоновый процесс удаления данных из блоков, который не зависит от действий пользователя или ОС: алгоритмы контроллера начнут очистку ненужных блоков и продолжат ее, даже если извлечь SSD из компьютера и установить его в другой компьютер. Не поможет и специализированное устройство для блокировки записи, которое используется для снятия образа дисков. Для запуска процесса очистки будет достаточно подать питание. Таким образом, SSD-накопители могут удалять информацию совершенно самостоятельно и независимо от действий или бездействия специалиста по извлечению данных. Применение в SSD-накопителях механизма очистки содержимого блоков памяти с помощью команды TRIM осложняет или делает невозможным доступ к удаленной информации.

Небольшие твердотельные накопители могут встраиваться в один корпус с магнитными дисками, образуя гибридные диски. Флеш-память в них может использоваться в качестве буфера (кеша) небольшого объема. Подобное

объединение позволяет воспользоваться частью преимуществ флеш-памяти (быстрый произвольный доступ) при сохранении небольшой стоимости хранения больших объемов данных. Стоит отметить, что гибридные накопители не получили широкого распространения.

Общий подход к производству экспертных исследований таких носителей информации остается неизменным. В целях исключения внесения изменений на исследуемом объекте необходимо использовать аппаратные, аппаратно-программные или программные блокираторы записи. Рекомендуется создание посекторной копии информации на накопителе эксперта, при этом в исключительных случаях допустимо прямое включение исследуемого объекта, о чем делается соответствующая запись в заключении эксперта.

Нередки случаи, когда операторы устройств самообслуживания предоставляют следователю образы носителей информации. Такое часто встречается, когда невозможно изъять сам объект без утраты значимой информации. Например, портативные ОС, программы-шифровальщики, мессенджеры, не сохраняющие историю сообщений, и др. Как правило, после отключения компьютерной техники от сети электрического питания получить указанную информацию не представляется возможным.

Для раскрытия и расследования преступлений данной категории в некоторых случаях целесообразно создание копии интересующей информации, а также копии (дампа) оперативной памяти компьютера. Содержание оперативной памяти необходимо для изучения предыдущих действий с компьютером, поиска ключей шифрования от криптоконтейнеров. В случаях применения портативных операционных систем для сокрытия преступной деятельности (например, Tails

или Whonix) дамп оперативной памяти может являться единственным источником доказательной информации.

Образ носителя информации должен быть представлен на экспертное исследование на электронном носителе информации. В рамках производства экспертизы необходимо обеспечить сохранность первоначального состояния исследуемого образа. Это возможно также с использованием блокираторов и создания криминалистической копии информации.

Экспертное исследование образа накопителя информации не должно отличаться от традиционных подходов к экспертному исследованию электронных носителей информации, при этом в заключении эксперта необходимо отображать характеристики исследуемого образа, характеристики накопителя информации, на котором он предоставлен, а также возможность восстановления удаленной информации.

Как уже отмечалось, важным элементом достижения анонимности при совершении преступлений является бесконтактный способ оплаты услуг и сбыта средств, предназначенных для подготовки, совершения или сокрытия преступлений. Покупатель указывает счет, на который следует перевести денежные средства. После получения данных о зачислении денежных средств на указанный счет «сбытчик» предоставляет информацию о местонахождении тайников. Несмотря на то, что счета, платежные карты, электронные кошельки открываются и регистрируются, как правило, на подставных лиц, можно отследить цепочку перечислений денежных средств и в конечном итоге установить их реальных получателей. Последние могут либо самостоятельно снять данные денежные средства, либо оплатить ими услуги, кредиты, товары и т. п., что позволяет до-

казать их причастность к совершению преступления. Учитывая, что любое движение денежных средств фиксируется финансово-кредитными организациями, имеется возможность получить необходимые документы для использования их в качестве доказательств даже по истечении продолжительного времени после совершения преступления.

В рамках производства СКЭ возможно получить данные о совершении платежей, номерах счетов, виде криптовалюты и другую важную информацию. Указанные сведения могут отображаться в журналах работы банковских приложений, программ, управляющих электронными кошельками, а также в истории посещения интернет-ресурсов.

Для качественного анализа информации, содержащей указанные сведения, необходимо знать порядок формирования записей об операциях. В некоторых случаях целесообразно привлекать сторонних специалистов, имеющих специальные знания о работе конкретных приложений.

Оценка содержимого файлов, содержащих графические материалы, не входит в компетенцию эксперта по специальности «Компьютерная экспертиза», при этом эксперту при ответе на соответствующие вопросы не запрещается давать предположительную оценку, сформированную на основе личного опыта (личной компетенции). В соответствии с пп. 31 и 32 Инструкции по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, утвержденной приказом МВД России от 29 июня 2005 г. № 511, в исследовательской части заключения эксперта отражаются содержание и результаты исследований, в том числе выявленные экспертом по собственной инициативе существенные обстоятельства, по поводу которых ему не были поставлены

вопросы. Выводы эксперта должны содержать краткие, четкие, однозначные ответы на все поставленные вопросы и установленные им в порядке инициативы значимые по делу обстоятельства.

Примеры вариантов ответа на вопрос «Имеются ли на представленном объекте файлы, содержащие графические материалы, имеющие отношение к хищению денежных средств из банкомата?»:

- Оценка содержимого файлов не входит в компетенцию эксперта.
- Оценка содержимого файлов не входит в компетенцию эксперта. Вместе с тем эксперт считает необходимым приобщить файлы… (указать какие и куда скопированы), предположительно, представляющие интерес (имеющие отношение) для расследования уголовного дела.
- На представленном объекте… (указать наименование) имеются файлы, содержащие графические материалы, которые скопированы… (указать место), при этом оценка содержимого файлов не входит в компетенцию эксперта.

Для поиска файлов, содержащих графические материалы, рекомендуется использовать поиск по расширению, при этом стоит учитывать, что данный перечень не является исчерпывающим. Эксперт в соответствии с методикой самостоятельно определяет область и критерии поиска.

Примерный перечень расширений файлов, содержащих графические материалы:

- Изображения: *.arw; *.bmp; *.cr2; *.crw; *.cur; *.dng; *.eps; *.gif; *.j2k; *.jp2; *.jpg; *.jpe; *.jpeg; *.ico; *.mrw; *.nef; *.orf; *.pcx; *.pef; *.png; *.ppm; *.psd; *.raf; *.rw2; *.sr2; *.srf; *.tga; *.tif; *.tiff; *.wmf; *.x3f;*.heic.
- Графика: *.ani; *.cdr; *.clp; *.cgm; *.dib; *.drw; *.dxf; *.emf; *.icl; *.iff; *.img; *.lbm; *.ldf; *.lwf; *.pbm; *.pcd; *.pgm; *.pic; *.pct; *.psp; *.qtif; *.ras; *.rgb;*.rle;*.sfw;*.wpg.
- Видео: *.3g2; *.3gp2; *.3gp; *.3gpp; *.amr; *.amv; *.asf; *.avi; *.bik; *.divx; *.dpg; *.dvr-ms; *.evo; *.ifo; *.flv; *.k3g; *.m1v; *.m2v; *.m2t; *.m2ts; *.m4v; *.m4p; *.m4b; *.mkv; *.mov; *.mp4; *.mpeg; *.mpg; *.mpe; *.mpv2; *.mp2v; *.mts; *.mxf; *.nsr; *.nsv; *.ogm; *.ogv; *.rm; *.ram; *.rmvb; *.rpm; *.rv; *.qt; *.skm; *.swf; *.ts; *.tp; *.tpr; *.trp; *.vob; *.wm; *.wmp; *.wmv.

Для оптимизации сроков производства компьютерных экспертиз следователю необходимо уделять больше внимания процессам доэкспертной оценки материалов в целях тщательного отбора объектов, имеющих значение для процесса доказывания, а также представления достаточного объема материалов, направляемых для проведения экспертизы. При этом важно на этапе формулирования экспертного задания выносить на разрешение эксперта только те вопросы, решение которых имеет значение для доказывания в рамках конкретного уголовного дела.

В рамках предварительного осмотра с участием специалиста могут быть определены приоритетность и целесообразность назначения экспертного исследования. Формулировку вопросов и достаточность представляемых материалов рекомендуется согласовать с экспертом. В большинстве

случаев такой подход обеспечивает оперативность, качество и результативность применения специальных знаний при расследовании и раскрытии преступлений.

Объекты исследования должны быть представлены в работоспособном состоянии, позволяющем производить поиск и считывание хранящейся на них информации. Представление заведомо неисправных устройств допускается, если доподлинно известно, что объект содержит сведения, представляющие значительный интерес для следствия, при обязательной предварительной консультации с экспертом и в рамках назначения комплексной компьютерной и радиотехнической экспертизы, при этом необходимо учитывать особенности назначения таких экспертиз.

Объекты исследования, содержащие зашифрованную информацию или заблокированные какой-либо пользовательской защитой, представляются с ключом разблокировки (паролем, ПИН-кодом, графическим рисунком). В случае отсутствия необходимых сведений у инициатора экспертизы представление объектов на исследование без ключа разблокировки допускается после предварительного согласования с экспертом с указанием обстоятельств в постановлении о назначении экспертизы.

Количество объектов, представляемых на исследование в рамках одной экспертизы, должно быть минимизировано – допускается представление не более пяти объектов. Увеличение количества представляемых объектов возможно в исключительных случаях после предварительной консультации с экспертом.

Не должны представляться на СКЭ объекты, внешне схожие с носителями информации, средствами вычислительной техники, такие как переходники, разветвители, кабели,

зарядные устройства (отдельно), аппаратные ключи защиты. Посторонние объекты могут быть отсеяны в рамках осмотра.

Количество ключевых слов (фраз) для осуществления контекстного поиска должно быть оптимизировано, исключать возможность использования системными приложениями и не должно превышать 15 на одну экспертизу.

Сетевое оборудование (маршрутизаторы, модемы, сетевые карты) могут представляться только для ответов на вопросы в области информационно-телекоммуникационных технологий после обязательной предварительной консультации с экспертом.

Объекты исследования для СКЭ в области анализа программного обеспечения целесообразно представлять с материалами уголовного дела, содержащими информацию о преступлении (инциденте).

Упаковка объектов исследования должна исключать возможность физического доступа к ним. Целесообразно использовать картонные коробки, полимерные и бумажные пакеты, которые заклеиваются (завязываются), опечатываются и снабжаются пояснительными надписями. Все порты и разъемы персональных компьютеров и серверного оборудования оклеиваются и опечатываются. Мобильные телефоны упаковываются в непрозрачный материал в целях предотвращения доступа к дисплею.

Объекты необходимо хранить в сухом помещении при комнатной температуре, исключив влияние на них электромагнитных полей.

При постановке типовых вопросов, решаемых в рамках СКЭ, необходимо следовать фабуле уголовного дела и ограничиваться актуальными вопросами, решение которых способствует раскрытию преступления. Формулировки вопросов, отличающиеся от типовых, следует согласовывать с экспертом.

При производстве экспертизы компьютерной информации, представленной в виде файловых систем, могут быть заданы следующие вопросы:

- Имеются ли в памяти представленных на исследование электронных носителей информации... (перечислить) сведения об учетных записях (аккаунтах) и паролях пользователя?
- Имеются ли в памяти представленных на исследование электронных носителей информации... (перечислить) файлы, содержащие электронную переписку посредством электронной почты, сервисов мгновенных сообщений (мессенджеров) и социальных сетей?
- Имеются ли в памяти представленных на исследование электронных носителей информации... (перечислить) файлы, содержащие историю посещения интернет-ресурсов?
- Имеются ли в памяти представленных на исследование электронных носителей информации... (перечислить) файлы, содержащие следующие ключевые слова (и выражения): «...», «...» и «...» (перечислить)?
- Имеются ли в памяти представленных на исследование электронных носителей информации... (перечислить) созданные или полученные пользователем графические/текстовые/аудио-/видеофайлы?
- Имеются ли в памяти представленных на исследование электронных носителей информации...

(перечислить) сведения об установленном ПО (для чего / атрибутирующем себя как)?

При производстве экспертизы компьютерной информации, содержащейся на платежных картах, могут быть заданы следующие вопросы:

- Какая информация имеется на магнитной полосе пластиковой карты, представленной на исследование?
- Соответствует ли информация, записанная на магнитную полосу пластиковой карты, информации, имеющейся в элементах ее внешнего оформления?
- Может ли представленная на исследование пластиковая карта быть воспринята в технологии функционирования платежной системы в качестве платежной (при условии использования информации, записанной на магнитную полосу карты) (на определенную дату или период)?

Помимо вопросов, решаемых в рамках исследования компьютерной информации, представленной в виде файловых систем, при производстве экспертизы мобильных телефонов могут быть дополнительно заданы следующие:

- Имеется ли в представленном на экспертизу мобильном телефоне, установленных в нем SIM-карте и карте памяти информация, вводимая абонентом (номера телефонов, сообщения, аудио-, видео- и графические файлы и др.) или накопленная в процессе работы телефона в сети сотовой связи (последние набранные и полученные звонки, принятые сообщения и др.)? Если да, то какая?
- Каково значение IMEI (международного идентификатора мобильного оборудования),

представленного на исследование мобильного телефона?

- Имеются ли в памяти представленных на исследование объектов сведения об абонентских номерах, присвоенных SIM-картам, установленным в мобильном телефоне?

При производстве экспертизы компьютерной информации, содержащейся на накопителях видеорегистратора, может быть задан следующий вопрос:

- Содержатся ли в представленном на исследование видеорегистраторе видеозаписи за период с... по... ?

При производстве экспертизы в области исследования программного обеспечения (в том числе вредоносного) могут быть заданы следующие вопросы:

- Имеются ли на представленных носителях информации (средствах вычислительной техники) объекты компьютерной информации (ПО), с помощью которых возможно совершение описанных в постановлении о назначении экспертизы действий?
- Как атрибутируют себя обнаруженные (представленные) объекты компьютерной информации (ПО), их основные параметры?
- Совпадает ли следовая картина, образованная в результате исполнения кода представленного на исследование ПО, со следовой картиной конкретного инцидента при условии создания

аналогичных условий функционирования и схожего состава входящих информационных потоков?

- К каким ресурсам глобальных и локальных информационных сетей фиксируются обращения в результате исполнения кода представленного на исследование ПО?
- Какая информация передается и какая ожидается в результате обращения к ресурсам глобальных и локальных информационных сетей, исполнения кода представленного на исследование ПО, какие предусмотрены варианты реагирования на полученные команды?
- Доступ к каким информационным ресурсам заложен в алгоритме кода представленного на исследование ПО, какая компьютерная информация и как (копирование, изменение, удаление и пр.) при этом обрабатывается?

Вопросы определения представленного на исследование программного обеспечения «вредоносным» либо заведомо предназначенного для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, не могут быть решены в ходе производства СКЭ в области исследования ПО.

Указанные особенности проведения и назначения специализированных экспертиз позволят должным образом систематизировать работу правоохранительных органов на стадии предварительного расследования.

§ 3.4. Деятельность следователя по взаимодействию с сотрудниками финансово-кредитных организаций

Рассмотрение данного вопроса необходимо начать с того, что при расследовании хищений из устройств самообслуживания и с их использованием остается достаточно много неурегулированных вопросов, связанных со взаимодействием банковских учреждений с сотрудниками правоохранительных органов. Как правило, это и является одной из основных причин низкой эффективности расследования рассматриваемых хищений.

Многие финансово-кредитные учреждения с частным уставным капиталом являются относительно закрытыми для успешного взаимодействия с правоохранительными органами, в связи с чем при выявлении банковскими работниками противоправных операций руководители соответствующих банков не всегда обращаются за помощью в правоохранительные органы.

Такое положение вещей вполне обосновано, поскольку нормативные документы большинства банковских учреждений Российской Федерации закрепляют следующие обязанности служб банковской безопасности: выявление признаков подготавливаемых и совершенных преступлений, применение мер по их предупреждению и прекращению; подготовка материалов в правоохранительные органы для решения вопроса о возбуждении уголовного дела; участие в предварительном расследовании уголовных дел; направление правоохранительным органам информации, имеющей отношение к расследованию; применение в пределах компетенции мер по возмещению причиненного банку вреда.

Между тем взаимодействие банков с органами предварительного расследования могло бы значительно ускорить процесс расследования преступлений данного вида, сделать его более эффективным. Результаты опросов, проводимых некоторыми учеными, показали, что совместная деятельность сотрудников банковской безопасности и следователей целесообразна в случае:

1) предоставления службами безопасности правоохранительным органам материалов для решения вопроса о возбуждении уголовного дела;

2) доступа в помещения, к документам и техническим средствам банка, необходимым для проведения следственных действий и оказания помощи в их применении;

3) налаживания связей и получения информации от иных банков по вопросам незаконного перечисления средств;

4) сбора и предоставления фактических данных, имеющих отношение к процессу расследования, в целях получения новых доказательств;

5) участия в розыске лиц, посягавших на интересы банка или подозреваемых в их совершении, а также применения в пределах компетенции мер по возмещению причиненного ущерба.

В целях разрешения возникающих проблем взаимодействия правоохранительных органов с финансово-кредитными учреждениями следует установить исчерпывающий перечень органов государственной власти, имеющих право получения из банков сведений, составляющих банковскую тайну, а также сроки предоставления информации, предусмотрев возможность их увеличения по просьбе банков. Кроме того, в целях сокращения временных рамок исполне-

ния запросов правоохранительных органов, а также устранения необходимости наполнения уголовного дела лишней информацией целесообразно предоставить банкам возможность передавать сведения, составляющие банковскую тайну, на электронных носителях с заверением ее подлинности в сопроводительных письмах.

В 2021 г. отчитывающиеся операторы направили в Банк России информацию о 973 инцидентах, связанных с несанкционированным доступом к их информационной инфраструктуре, на общую сумму 103,8 млн ₽. Несанкционированный доступ работников или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры и автоматизированным банковским системам или информации о банковских счетах, стал причиной 877 инцидентов, связанных с переводом денежных средств оператора или его клиентов без их согласия.

Объем ущерба в результате таких хищений составил порядка 24,5 млн ₽. Хищений, произошедших в результате компьютерных атак или несанкционированного доступа к автоматизированным банковским системам (информации о банковских счетах), было зафиксировано в 15 раз меньше – 58 инцидентов, при этом объем хищений составил 23,2 млн ₽. Несанкционированный доступ работников или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, программно-аппаратному обеспечению банкоматов и электронных терминалов, стал причиной 14 хищений на сумму порядка 13,5 млн ₽, в то время как хищений в результате компьютерных атак и несанкционированного доступа было всего восемь (на сумму около 10,6 млн ₽).

В этом же году произошли 15 компьютерных атак и два случая несанкционированного доступа к программно-аппаратному обеспечению банкоматов, которые стали причиной несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах на сумму 32,2 и 0,9 млн ₽ соответственно[27].

В Красноярске суд рассмотрел уголовное дело в отношении двух бывших сотрудниц банка «Открытие», которые обвинялись в хищении. Обвиняемые занимали должности начальника кассовых операций и ведущего кассира одного из подразделений банка, среди прочего в их обязанности входила загрузка наличных в кассеты, помещаемые в банкомат. По версии следствия, кассиры недокладывали в кассеты по несколько купюр, в результате в период с мая 2018 по апрель 2019 г., по подсчетам следствия, они похитили у кредитной организации 2,2 млн ₽. Недостача вскрылась, когда банкомат был передан на обслуживание в другой филиал банка. Следственные органы возбудили уголовное дело по ч. 4 ст. 160 УК РФ (присвоение в особо крупном размере). В судебном заседании подсудимые полностью признали вину. Учитывая, что кассиры возместили ущерб, а представитель банка не настаивал на суровом наказании, суд назначил обвиняемым по три года условно[28]

В представленном примере при надлежащем уровне взаимодействия между банковскими служащими и правоохранительными органами подобной ситуации можно было бы избежать.

Таким образом, определение принципов и форм взаимодействия правоохранительных органов со службами безопасности банков, разработка и внедрение электронного документооборота, разработка соответствующих методик документирования и изобличения преступников, а также проведение совместных семинаров и тренингов для сотрудников практических подразделений при участии специалистов из банковской сферы и сферы информационных технологий позволят надлежащим образом организовать противодействие хищениям денежных средств из банкоматов и с их использованием. Вместе с тем сотрудникам, расследующим дела о хищениях денежных средств из банкоматов или с их использованием, следует учитывать некоторые особенности человеческого фактора, в случаях когда сами работники банков являются преступниками, совершившими хищение, или оказывают помощь и содействие третьим лицам.

Говоря о сотрудничестве правоохранительных органов и банковских служащих, следует также отметить, что их помощь является в некотором роде основополагающей при расследовании уголовных дел о кражах из банкоматов или электронных средств платежа, поскольку сотрудники, занимающиеся расследованием данного преступления, в обязательном порядке будут вынуждены сделать запрос на предоставление данных о движении денежных средств, направляемый в банк.

З., состоящая в должности руководителя дополнительного офиса Якутского отделения филиала ПАО «Сбербанк России», совершила два умышленных тяжких преступления против собственности – присвоение, т. е. хищение чужого имущества, вверенного виновному, совершенное с использованием своего служебного положения, в крупном размере. З. в ходе выполнения своих должностных обязанностей умышленно, из внезапно возникших корыстных побуждений, в целях извлечения материальной выгоды и зная, что кассеты с денежными средствами не опломбированы, пользуясь тем, что за ней никто и не наблюдает, подошла к устройству самообслуживания №... (банкомату), открыла сейф данного устройства посредством введения кодовых комбинаций, откуда вынула кассеты с наличными денежными средствами и путем присвоения похитила принадлежащие ПАО «Сбербанк России» денежные средства[29]

Вместе с тем, как уже указывалось ранее, следователю необходимо запросить записи с камер видеонаблюдения, расположенных в помещении банка или в ином помещении, в котором находился банкомат, поскольку только таким образом можно получить доступ к данным, позволяющим проводить надлежащее расследование.

В настоящее время вопросам повышения взаимодействия с кредитно-финансовыми организациями уделяется особое внимание, как и мерам повышения эффективности такого взаимодействия. В частности, это расширение возможностей информационного обмена в рамках сервисов межведомственного взаимодействия, а именно заключение

соглашений о сотрудничестве и электронном документообороте с кредитно-финансовыми организациями, операторами сотовой связи и интернета.

Кроме того, для повышения взаимодействия полиции с кредитно-финансовыми организациями принимаются следующие меры:

1. Создание специализированных подразделений в составе полиции, которые занимаются взаимодействием. Эти подразделения имеют опыт работы в финансовой сфере и знают специфику деятельности банков и других финансовых организаций.

2. Организация регулярных встреч между представителями полиции и представителями кредитно-финансовых организаций. На этих встречах обсуждаются вопросы сотрудничества, проблемы, возникающие при проведении операций, а также возможности улучшения взаимодействия.

3. Внедрение новых технологий в работу полиции и кредитно-финансовых организаций. Например, использование систем анализа информации, баз данных и программного обеспечения для обмена информацией о преступниках и их действиях.

4. Обучение сотрудников полиции работе с финансовыми инструментами и технологиями. Это позволяет им лучше понимать специфику работы банков и других финансовых организаций, а также эффективнее проводить операции по выявлению и пресечению преступлений в этой сфере.

5. Установление более тесного контакта между сотрудниками полиции и представителями кредитно-финансовых организаций. Это достигается путем проведения совмест-

ных тренингов, семинаров и конференций, на которых обсуждаются вопросы безопасности и противодействия преступлениям.

Само по себе взаимодействие следователя и сотрудников финансовых и кредитных организаций позволяет осуществлять целый комплекс мероприятий. Прежде всего следует понимать, что цель у данных субъектов общая – поймать преступника и вернуть денежные средства. Таким образом, можно сделать вывод, что инициатором взаимодействия выступает именно следователь – именно он направляет соответствующие запросы и истребует необходимые данные. Поддержание хорошего взаимодействия между представителем правоохранительных органов и представителем финансово-кредитной организации позволяет в кратчайшие сроки установить преступника, задержать его и вернуть украденные денежные средства.

Вопросы для самоконтроля

1. Каков алгоритм первоначальных действий следственно-оперативной группы по прибытии на место происшествия по факту хищения, совершенного из устройства самообслуживания?

2. Перечислите мероприятия, проводимые следователем, оперуполномоченным полиции, участковым уполномоченным полиции и экспертом-криминалистом до возбуждения уголовного дела, указав их назначение.

3. Каков алгоритм действий следственно-оперативной группы при выявлении в ходе осмотра места происшествия внештатного оборудования?

4. Назовите формы взаимодействия сотрудников органов предварительного следствия и дознания с сотрудниками служб безопасности финансовых и кредитный организаций отразив их содержание.

5. Перечислите судебно-криминалистические экспертизы, назначаемые по факту хищения денежных средств из устройств самообслуживания и с их использованием с указанием следственных ситуаций.

6. Что относится к задачам судебной компьютерной экспертизы?

7. Назовите основные следственные действия, проводимые после возбуждения уголовного дела по факту хищения денежных средств из устройств самообслуживания и с их использованием, указав их назначение.

Заключение

Мы живем в эпоху информационного общества, и наша жизнь тесно связана с различными технологиями. Использование платежных систем является неотъемлемой ее частью, все больше появляется электронных ресурсов, исключающих прием денежных средств наличными. Однако каждый раз, взаимодействуя с компьютерными технологиями, мы подвергаем себя угрозе стать жертвой преступников. В связи с этим всестороннее изучение средств совершения дистанционных хищений позволяет разработать эффективные меры по предупреждению и расследованию киберпреступлений.

Само выявление данных преступлений на сегодняшний момент представляет проблему, поэтому прослеживается их высокая латентность.

Для большинства сотрудников органов предварительного расследования раскрытие и расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий, представляет сложность, которая связана с неэффективным взаимодействием и с тем, что при сборе доказательств и доказывании в таких делах необходимо изучение «виртуальных следов». При этом уровень специальной технической подготовки, которая нужна для расследования подобных дел, в органах юстиции очень низкий.

Кроме того, отсутствует обобщенный материал следственной практики, методический материал и рекомендации по расследованию данного вида преступлений. В связи с этим учебное пособие представляет особую актуальность в рамках построения плана расследования следователем, дачи правильной квалификации содеянному и успешному расследованию данных хищений.

Список использованной литературы

1 Банкоматы и банковские терминалы самообслуживания // URL: https://kiosks.ru/index.php/product-category/all-bank-kiosks/.

2 История банкоматов. Начало истории // URL: https://rbcard.com/hist ory/hist_atm.htm.

3 История банкоматов. Начало истории // URL: https://rbcard.com/hist ory/hist_atm.htm.

4 История банкоматов. Начало истории // URL: https://rbcard.com/hist ory/hist_atm.htm.

5 About Credit Card. URL: https://ruscreditcard.ru/kak-bankovskie-karty-zavoevali-planetu/.

6 Свободная энциклопедия «Википедия». URL: https://ru.wikipedia.org.

7 Habr Blockchain Publishing LTD. URL: https://habr.com/ru/post/394993/.

8 Habr Blockchain Publishing LTD. URL: https://habr.com/ru/post/394993/.

9 Кредитные истории // URL: https://kredit.temaretik.com/938178563056863704/kak-platezhnye-karty-zavoevali-planetu/.

10 Habr Blockchain Publishing LTD. URL: https://habr.com/ru/post/394993/.

11 История банкоматов. Начало истории // URL: https://rbcard.com/ history/hist_atm.htm.

12 About Credit Card. URL: https://ruscreditcard.ru/kak-bankovskie-karty-zavoevali-planetu/.

13 Шмонин А. В. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий : аналитический обзор. М. : Академия управления МВД России, 2015. С. 4.

[14] Приговор Октябрьского районного суда г. Самары от 18 сентября 2017 г. № 1-192/2017 // Судебные и нормативные акты РФ. URL: https://sudact.ru/.

[15] Постановление Мариинского городского суда Кемеровской области от 4 марта 2019 г. № 1-42/2019 // Судебные и нормативные акты РФ. URL: https://sudact.ru/.

[16] Карасева М. Ю. Криминологическая характеристика субъекта преступления // Экономика и право. XXI век. 2013. № 1. С. 85–92.

[17] Судебные и нормативные акты РФ. URL: https://sudact.ru/.

[18] Решение Новокуйбышевского городского суда г. Самары от 25 мая 2020 г. № 2-875/2020 // Судебные и нормативные акты РФ. URL: https://sudact.ru/.

[19] Информационно-аналитические материалы Следственного департамента МВД России за 2019 г.

[20] Современные системы безопасности // URL: https://www.mckrona.ru/-blog/okhrana-bankomatov-sovremennye-sredstva-zashchity/.

[21] Национальная экономическая энциклопедия. URL: https://vocable.ru/.

[22] Официальный новостной портал «Вести.Ru». URL: https://www.vesti.ru/article/2403213.

[23] Алгоритм работы следователя при рассмотрении сообщений о преступлениях / под общ. ред. А. М. Багмета. М. : Юрлитинформ, 2012. С. 4.

[24] Федеральный закон от 4 марта 2013 г. № 23-ФЗ «О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. 2013. № 9. Ст. 875.

[25] Официальный портал пресс-службы, новостной архив. URL: http://www.zrpress.ru/finance/primorje_22.03.2015_71481_moshenniki-opustoshili-bankovskie-karty-zhitelej-primorja.html.

[26] Имаева Ю. Б. Тактические приемы осмотра места происшествия, используемые для преодоления противодействия расследованию хищения с использованием кредитных и расчетных карт // Пробелы в российском законодательстве. 2011. Вып. 3. С. 238.

[27] Обзор операций, совершенных без согласия клиентов финансовых организаций за 2021 г., подготовленный Банком России // URL: https://cbr.ru/Content/Document/File/103609/Review_of_transactions_2021.pdf.

[28] Официальный новостной портал «Коммерсантъ». URL: https://www.kommersant.ru/doc/4164440.

[29] Судебные и нормативные акты РФ. URL: https://sudact.ru/.

Библиографический список

Нормативные акты

Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 04.09.2023).

Уголовный кодекс Российской Федерации : УК : Федеральный закон № 63-ФЗ : принят Государственной Думой 24 мая 1996 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 04.09.2023).

Уголовно-процессуальный кодекс Российской Федерации : УПК : Федеральный закон № 174-ФЗ : принят Государственной Думой 22 ноября 2001 г. // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 04.09.2023).

Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 04.09.2023).

Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно розыскной деятельности» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 04.09.2023).

Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 04.09.2023).

Федеральный закон от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_122329/ (дата обращения: 04.09.2023).

Паспорт национального проекта «Национальная программа „Цифровая экономика Российской Федерации”» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_328854/ (дата обращения: 04.09.2023).

Приказ МВД России от 4 января 1996 г. № 4 «О реализации Соглашения между МВД России и Ассоциацией российских банков» // Бюллетень текущего законодательства МВД России. – 1996. – Вып. 15. Ч. II.

Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2005. – № 35.

Приказ МВД России от 29 августа 2014 г. № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» // Российская газета. – 2014. – № 260.

Судебная практика

Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике

по делам о краже, грабеже и разбое» // Бюллетень Верховного Суда Российской Федерации. – 2003. – № 2.

Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 04.09.2023).

Учебная и научная литература

Алгоритм работы следователя при рассмотрении сообщений о преступлениях / под общ. ред. А. М. Багмета. – М. : Юрлитинформ, 2012.

Анапольская, А. И. Порядок взаимодействия правоохранительных органов с банковскими учреждениями при расследовании мошенничеств, совершаемых в сфере функционирования электронных расчетов / А. И. Анапольская // Вестник Тамбовского университета. – 2015. – С. 34–36.

Болсуновская, Л. М. Мошенничество в сфере компьютерной информации: анализ судебной практики / Л. М. Болсуновская // Уголовное право. – 2016. – № 2. – С. 12–16.

Воронин, А. С. Платежные карты. Бизнес-энциклопедия / А. С. Воронин. – 2-е изд. – М. : Кнорус, 2014.

Имаева, Ю. Б. Тактические приемы осмотра места происшествия, используемые для преодоления противодействия расследованию хищения с использованием кредитных и расчетных карт // Пробелы в российском законодательстве. Юридический журнал. – 2011. – Вып. 3.

Колдин, В. Я. Вещественные доказательства: Информационные технологии процессуального доказывания / В. Я. Колдин ; под общ. ред. В. Я. Колдина. – М. : Норма, 2002.

Методика исследования объектов радиотехнической экспертизы / [В. М. Щербак и др.]. – М. : ЭКЦ МВД России, 2019.

Михайленко, Н. В. Кибернетические угрозы, как проблема национальной безопасности // Актуальные проблемы международного сотрудничества в борьбе с преступностью : сборник статей по итогам Международной научно-практической конференции, приуроченной к 70-летию принятия Генеральной Ассамблеей Организация Объединенных Наций Всеобщей декларации прав человека 1948 г. / под общ. ред. Д. Д. Шалягина. – М. : Московский университет МВД России имени В.Я. Кикотя, 2019. – С. 101–105.

Михайленко, Н. В. Цифровое государственное управление. Современные проблемы и перспективы завтрашнего дня / Н. В. Михайленко // Государственная служба и кадры. – 2020. – № 2. – С. 171–175.

Мурадян, С. В. Факторы, обусловливающие рост числа преступлений, совершаемых с использованием криптовалют и способы их нивелирования в России / С. В. Мурадян // Актуальные вопросы современной криминологической и уголовно-исполнительной науки : сборник тезисов Международной научно-практической заочной конференции памяти доктора исторических наук, профессора А. В. Шаркова, 15 апреля 2021 г. – Минск : Академия МВД, 2021. – С. 208–210.

Россинская, Е. Р. Судебная экспертиза в гражданском, арбитражном и уголовном процессе / Е. Р. Россинская. – М., 1996.

Русскевич, Е. А. О содержании правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в контексте ст. 274 УК / Е. А. Русскевич // Библиотека уголовного права и криминологии. – 2017. – № 4. – С. 160–163.

Русскевич, Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е. А. Русскевич. – М. : Инфра-М, 2019.

Русскевич, Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учебное пособие / Е. А. Русскевич. – 2-е изд., доп. – М. : Инфра-М, 2019.

Саенко, Г. В. Типовая методика исследования компьютерной информации / Г. В. Саенко, О. В. Тушканова. – М. : ЭКЦ МВД России, 2010.

Турышев, А. А. Квалификация хищения с использованием банкоматов / А. А. Турышев // Законы России: опыт, анализ, практика. – 2016. – № 6. – С. 46–50.

Тушканова, О. В. Терминологический справочник судебной компьютерной экспертизы / О. В. Тушанкова. – М. : ЭКЦ МВД России, 2005.

Финагеев, В. А. Проблемы взаимодействия правоохранительных органов и подразделений банковской безопасности в выявлении и расследовании преступлений / В. А. Финагеев // Таможенное дело. – 2016. – № 2 (86). Ч. 2. – С. 264–270.

Чурин, Р. А. Особенности исследования сетевых хранилищ данных в рамках компьютерных экспертных исследований : методические рекомендации / Р. А. Чурин, В. А. Ращупкина, А. В. Перевощиков. – М. : ЭКЦ МВД России, 2022.

Чурин, Р. А. Современное состояние компьютерной судебной экспертизы в экспертно-криминалистических подразделениях МВД России / Р. А. Чурин, В. А. Ращупкина // Судебная экспертиза Беларуси. – 2022. – № 1 (16). – С. 59–63.

Шмонин, А. В. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий : аналитический обзор / А. В. Шмонин. – М. : Академия управления МВД России, 2015.

Учебное издание

Гончар Владимир Владимирович,
кандидат юридических наук, доцент

Полянская Елена Петровна

Михайленко Наталья Васильевна,
кандидат юридических наук, доцент

Мурадян Светлана Владимировна,
кандидат юридических наук

Чурин Роман Александрович

Расследование преступлений, связанных с хищениями денежных средств из устройств самообслуживания

Редактор *Васильевых Е. М.*
Корректор *Лосева О. С.*
Компьютерная верстка *Лосева О. С.*

Формат 60×84/16.
Усл. печ. л. 8,48.
Подписано в печать 18.10.2023. Заказ № 25.
Тираж 125 экз. 1-й завод 76 экз.

Отпечатано в Полиграфическом центре
Московского университета МВД России имени В.Я. Кикотя
https://мосу.мвд.рф, e-mail: support_mosu@mvd.ru