МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ

Н.Р. Шевко
А.М.Каримов

ДЕЙСТВИЯ ДЕЖУРНОГО ПРИ ПОСТУПЛЕНИИ СООБЩЕНИЯ О ПРЕСТУПЛЕНИИ, СОВЕРШЕННОМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Памятка

Казань 2018

ББК 32.81
Ш 31

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты:

Доктор экономических наук, профессор С.Г. Аксёнов
(Уфимский юридический институт МВД России)

Т.М. Уразманов (Отдел организации работы дежурных частей
ОВД ОУ МВД по РТ)

Шевко Н.Р.

Ш 31 Действия дежурного при поступлении сообщения о преступлении, совершенном с использованием информационных технологий: памятка / Н.Р. Шевко, А.М. Каримов. - Казань: КЮИ МВД России, 2018. – 28 с.

В памятке отражена специфика рассмотрения сообщений о преступлениях, совершенных с использованием информационных технологий, представлен алгоритм неотложных первоначальных действий дежурного.

Адресована преподавателям, курсантам и слушателям образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

ББК 32.81

Оглавление

ВВЕДЕНИЕ

В настоящее время широкий спектр преступлений может совершаться с использованием телекоммуникаций и компьютерной информации. Подавляющее большинство преступлений в данной сфере связано с различными видами хищений, такими, как мошенничество.

Средства телекоммуникаций и новые информационные технологии создают условия для подготовки, совершения и сокрытия хищений денежных средств с их использованием, к которым относятся: виртуальный характер дистанционных банковских операций; доступность открытых телекоммуникационных систем; высокая скорость выполнения транзакций; глобальный характер межсетевого операционного взаимодействия[1].

Если раньше специфика преступлений в сфере компьютерной информации была обусловлена использованием при их совершении высоких технологий и новейших достижений науки и техники, необходимостью обладания определенным уровнем специальных познаний, то в настоящее время в глобальной сети Интернет в практически свободном доступе находятся как программы, предназначенные для совершения несанкционированных действий с компьютерной информацией, так и инструкции по их применению.[2]

Для успешного раскрытия и расследования таких преступлений сотрудникам ОВД необходимо тесное взаимодействие с другими службами, в том числе и в иностранных государствах. Но первостепенную роль играют оперативные дежурные, которые могут грамотно объяснить потерпевшему, какие действия

[1] Ревенков П.В. Управление рисками в условиях электронного банкинга: автореф. дис. ... д-ра эконом. наук. СПб., 2013. С. 20.

[2] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России). Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

необходимо произвести в данной ситуации, а какие, наоборот, не следует в целях сохранения следов преступления и соответствующих улик.

Представляется, что настоящее учебное пособие будет способствовать выработке умений и навыков при прохождении первоначальной подготовки и переподготовки, а также повышению уровня профессиональной подготовки сотрудников дежурных частей при регистрации сообщений о преступлениях, совершаемых с использованием высоких технологий и телекоммуникаций.

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Преступление, совершенное с использованием информационных технологий - преступление, которое совершено в электронной среде.

Преступление, совершенное с использованием информационных технологий, в узком смысле —
любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных.

Преступление, совершенное с использованием информационных технологий, в широком смысле —любое противоправное деяние, совершаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, предложение или распространение информации посредством компьютерной системы или сети, в том числе и преступления, совершаемые с использованием высоких технологий и телекоммуникаций.

Компьютерная информация - информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию компьютерной техники, или передающаяся по каналам связи.[3]

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объек-

[3] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Доступ из СПС «Консультант плюс» (дата обращения 11.08.2017).

тов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.[4]

Компьютерный взлом - несанкционированное проникновение в компьютерную сеть с целью получения собственной выгоды, например, хищения денег на счетах в банках.[5]

Хищение денежных средств, совершаемое с использованием высоких технологий – это совершенное с корыстной целью противоправное безвозмездное изъятие и обращение чужих денежных средств, числящихся на банковских и иных счетах, в пользу лица, совершившего данное преступление, или других лиц путем применения средств хранения, обработки и (или) передачи компьютерной информации, причинившее ущерб их собственнику или иному владельцу. К ним можно отнести кражу (ст. 158 УК), мошенничество с использованием платежных карт (ст. 159.3 УК), мошенничество в сфере компьютерной информации (ст. 159.6 УК), присвоение и растрату (ст. 160 УК).

4 О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 N 187-ФЗ. Доступ из СПС «Консультант плюс» (дата обращения 12.08.2017).

5 Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б. Современный экономический словарь. 6-е изд., перераб. и доп. М.: ИНФРА-М, 2011.

ДЕЙСТВИЯ ДЕЖУРНОГО

ПРИ ПОЛУЧЕНИИ СООБЩЕНИЯ О ПРЕСТУПЛЕНИИ, СОВЕРШЕННОМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1. Зарегистрировать данные заявителя:
- ФИО,
- адрес,
- номер телефона

2. Зарегистрировать данные потерпевшего:
- ФИО,
- адрес,
- номер телефона

3. Уточнить:
- обстоятельства происшествия,
- время (период),
- место,
- способ совершения преступления

4. Уточнить сумму ущерба.

5. Выяснить возможных лиц, причастных к преступлению (возможность получения доступа к карте, номеру телефона и т.д.)

6. Проинструктировать заявителя о мерах предосторожности и дальнейших действиях в целях сохранения следов преступления и соответствующих улик

7. Доклад руководителю территориального органа

8. Доклад в вышестоящую дежурную часть

9. Направить на место происшествия следственно-оперативную группу (СОГ) с дополнительным привлечением необходимых специалистов

10. Запрос в вышестоящую дежурную часть номера ориентировки на предмет похищенного либо лиц, причастных к данному преступлению

11. Получение информации с места происшествия от руководителя СОГ

12. Направление оперативной информации в вышестоящую дежурную часть с полученным номером ориентировки

13. Ориентирование районов области ближайших регионов

АЛГОРИТМ ДЕЙСТВИЙ ДЕЖУРНОГО ПРИ ПОЛУЧЕНИИ СООБЩЕНИЯ О ПРЕСТУПЛЕНИИ, СОВЕРШЕННОМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

РАБОТА С ЗАЯВИТЕЛЕМ

1. **Зарегистрировать данные заявителя:**
ФИО, адрес, номер телефона

2. **Зарегистрировать данные потерпевшего:**
ФИО, адрес, номер телефона

3. **Уточнить:**
- обстоятельства происшествия,
- время (период), место, способ совершения преступления;
- сумму ущерба

4. **Выяснить возможных лиц, причастных к преступлению (возможность получения доступа к карте, номеру телефона и т.д.)**

5. **Проинструктировать заявителя о мерах предосторожности и дальнейших действиях в целях сохранения следов преступления и соответствующих улик**

АЛГОРИТМ ДЕЙСТВИЙ ДЕЖУРНОГО

1. Работа с заявителем.

⇩

2. Доклад руководителю территориального органа.

⇩

3. Доклад в вышестоящую дежурную часть.

⇩

4. Направление на место происшествия следственно-оперативной группы (СОГ) с дополнительным привлечением необходимых специалистов.

⇩

5. Запрос в вышестоящую дежурную часть номера ориентировки на предмет похищенного либо лиц, причастных к данному преступлению.

⇩

6. Получение информации с места происшествия от руководителя СОГ.

⇩

7. Направление оперативной информации в вышестоящую дежурную часть с полученным номером ориентировки.

⇩

8. Ориентирование районов области ближайших регионов.

В Книге учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (КУСП) отражаются следующие сведения:

порядковый номер, присвоенный зарегистрированному заявлению (сообщению) о преступлении, об административном правонарушении, о происшествии;

дата, время и форма поступления заявления (сообщения) о преступлении, об административном правонарушении, о происшествии;

данные о сотруднике органов внутренних дел, принявшем заявление (сообщение) о преступлении, об административном правонарушении, о происшествии;

данные о заявителе;

регистрационный номер талона-уведомления, выданного заявителю (в случае выдачи);

краткое содержание заявления (сообщения) о преступлении, об административном правонарушении, о происшествии;

данные о руководителе, которому доложено о заявлении (сообщении) о преступлении, об административном правонарушении, о происшествии;

результаты работы следственно-оперативной группы, дежурного наряда (сотрудника) на месте совершения преступления, административного правонарушения, месте происшествия;

данные о руководителе, поручившем проверку заявления (сообщения) о преступлении, об административном правонарушении, о происшествии;

данные о сотруднике органов внутренних дел, которому поручена проверка заявления (сообщения) о преступлении, об административном правонарушении, о происшествии, его подпись, дата и время получения;

срок проверки, установленный руководителем, и срок, в который рассмотрено заявление (сообщение) о преступлении, об административном правонарушении, о происшествии, данные о должностных лицах, продливших срок проверки;

результаты рассмотрения заявления (сообщения) о преступлении, об административном правонарушении, о происшествии.

ДЕЙСТВИЯ ПОТЕРПЕВШЕГО ПРИ ОБНАРУЖЕНИИ НЕСАНКЦИОНИРОВАННЫХ ТРАНЗАКЦИЙ

Как только потерпевший обнаружил в истории операций своей карты незнакомые переводы средств, ему необходимо:

1. **Незамедлительно заблокировать ее.**
   Это можно сделать при помощи интерфейса «Онлайн» и опции «Заблокировать карту», а также связавшись с оператором по номерам горячей линии.
   При обращении по телефону сотрудники банка попросят назвать кодовое слово регистрируемой при получении карты. Однако в случае необходимости данную операцию они могут произвести по другим данным, например серии, номера паспорта и т.д. Точно таким же образом в случае необходимости карту можно разблокировать.
2. **Прекратить какие-либо самостоятельные манипуляции с объектами,** использованными злоумышленниками для дистанционного банковского обслуживания (ДБО) (смартфонами, телефонами, планшетами, ноутбуками, ПК, POS-терминалами, банковскими картами).
3. Если на момент поступления сообщения данный объект выключен**, включать его нельзя.**
4. Если устройство включено для недопущения удаленного подключения, направленного на совершение повторных незаконных транзакций или на удаление следов инцидента, **устройство необходимо выключить и обязательно отключить сетевые подключения, источник питания.**
5. Во избежание утраты следов инцидента **ЗАПРЕЩЕНО:**
   - перезагружать устройство,
   - форматировать носители,
   - переустанавливать операционную систему,
   - проводить проверку антивирусными программами.

6. **Позвонить в полицию** и сообщить о случившемся.
7. Если выяснится, что деньги с карты были переведены на счет другого банка, потерпевшему **НЕОБХОДИМО В КРАТЧАЙШИЕ СРОКИ обратиться в свой банк с заявлением на блокировку счета, на который поступили денежные средства, и последующий возврат денег.** В течение 5 дней есть большая возможность ограничить операции по банковскому счёту, на который злоумышленниками были переведены денежные средства, и через какое-то время вернуть деньги.

ТИПИЧНЫЕ ПРИЗНАКИ ПОДГОТОВКИ, СОВЕРШЕНИЯ И СОКРЫТИЯ ПРЕСТУПЛЕНИЯ, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ:

- появление в системе ПК или их сети ложных данных (письма электронной почты от неизвестных и известных адресатов с прикрепленными файлами, не соответствующими описанию, и т.п.);

- несанкционированные изменения программного обеспечения и конфигурации ПК, системы ПК или их сети;

- частые сбои в работе аппаратуры;

- жалобы клиентов на предоставление некачественного доступа к ПК, системе ПК, их сети или компьютерной информации;

- нерегламентированный доступ к ПК, системе ПК, их сети и к компьютерной информации отдельных субъектов;

- нарушение правил работы с компьютерной информацией и несанкционированные манипуляции с ней;

- чрезмерный интерес отдельных субъектов (клиентов, сотрудников) к содержанию компьютерной информации определенной категории;

- применение на рабочем месте и вынос с работы личных носителей информации под различными предлогами;

- случаи утечки конфиденциальной информации либо обнаружение негласных устройств ее получения; нарушение установленных правил оформления документов при работе с ПК, системой ПК, их сетью или компьютерной информацией;

- создание копий определенной категории данных и компьютерной информации, не предусмотренных технологическим процессом;

- несоответствие данных, содержащихся в первичных (исходных) документах, иным более поздним по времени создания документам;

- подозрительно частое обращение одного и того же пользователя к данным и компьютерной информации определенной категории;

- появление в компьютере недостоверных данных;

- отсутствие обновления в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств.

ВИДЫ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, В ЗАВИСИМОСТИ ОТ СПОСОБА ИХ СОВЕРШЕНИЯ

Кардинг – название преступлений с банковскими картами – в них незаконно используются сами карты или информация о них:

- «кардинг-он-лайн» - применение скомпрометированных карт в интернет-магазинах,
- «кардинг-офф-лайн» – использование карт для расчета в традиционных торгово-сервисных предприятиях (ТСП),
- «кэшинг» – съем денег в банкомате (АТМ) по скомпрометированным картам.

Занимаясь кардингом, можно либо получить информацию о реальной карте, либо сгенерировать все эти данные. Интересующиеся могут свободно найти ссылки на сайты, которые открыто торгуют сведениями о банковских картах.

Подделка карты - изготовление карт, реквизиты которых полностью повторяют реквизиты реальных карт, выпущенных эмитентом. По поддельной карте можно совершать операции, выдавая ее за настоящую.

Скимминг (skimming) - незаметное для держателя реальной карты копирование данных с магнитной полосы с помощью специальных устройств на банкомате. Собираются данные клиентов банка, которые воспользовались данным банкоматом, после чего на специальную заготовку записывается дамп карты потерпевшего и снимаются деньги прямо в банкомате, т.к. скимер списывает данные с карты и записывает пин-код к ней.

Скимминговое оборудование - оборудование для несанкционированного считывания информации с банковских карт физических лиц и фиксации ПИН-кодов к ним.

Сниффинг (от англ. to sniff — нюхать) — перехват и анализ сетевого трафика с помощью сниффера (программы или устройства). Сниффер может анализировать только то, что проходит через его сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются всем машинам, из-за этого возможно перехватывать чужую информацию. Коммутация пакетов — форма передачи, при которой данные, разбитые на отдельные пакеты, могут пересылаться из исходного пункта в пункт назначения разными маршрутами. Так что если кто-то в другом сегменте посылает внутри него какие-либо пакеты, то в ваш сегмент коммутатор эти данные не отправит.

Снятие дампа карты (дамп - данные с магнитной ленты карты). Снятые данные записываются на заготовку карты, на которой принтером наносится изображение какого-либо банка и иногда эмбасируется номер карты и имя владельца, и в дальнейшем приобретаются какие-либо товарно-материальные ценности, так как не во всех терминалах нужен пин-код карты.

Фарминг — метод онлайнового мошенничества, заключающийся в изменении *DNS* (*Domain Name System*) адресов так, чтобы веб-страницы, которые посещает пользователь, были не оригинальными, а другими, специально созданными кибермошенниками для сбора конфиденциальной информации. Необходимая для инфицирования программа-вирус скрытно устанавливается на каждый компьютер бот-сети.

Фишинг (phishing – производное от phone –телефон и fishing - рыбалка) - преступление, в котором все персональные данные о картах и счетах клиента добываются злоупотреблением доверием (мошенничеством) - всю требуемую информацию владельцы карт передают преступникам добровольно. Часто фишинг осуществляется рассылкой по электронной почте официального письма якобы от имени представителя банка.

DDOS атаки. Бот-сети (botnets) – сети в Интернет зомбированных (инфицированных) компьютеров. Зараженный компью-

тер-бот в дальнейшем используется для рассылки спама, проведения «атак на отказ в обслуживании» (Distributed Denial of Service - DDoS), организации клик-фрода. Необходимая для инфицирования программа-вирус скрытно устанавливается на каждый компьютер бот-сети.

Криптолокинг – блокирование доступа к данным на персональном компьютере или ином устройстве, в облачном хранилище с последующими незаконными требованиями передачи денежных средств или ином вознаграждении за его разблокировку.

Платежное мошенничество: EMV (чип и PIN-код), геоблокировка и другие промышленные меры безопасности продолжают помогать в эффективной борьбе с карточным мошенничеством, но, тем не менее, растет и число атак, направленных против банкоматов. Организованные преступные группы начинают компрометировать платежи, связанные с использованием бесконтактных карт (NFC).

ОСОБЕННОСТИ ПЛАСТИКОВЫХ КАРТ

Пластиковая карта — обобщающий термин, который обозначает все виды карточек, различающихся по назначению, по набору оказываемых с их помощью услуг, по своим техническим возможностям и организациям, их выпускающим. Важнейшая особенность всех пластиковых карт, независимо от степени их совершенства, состоит в том, что на них хранится определенный набор информации, используемый в различных прикладных программах.

Под **банковской (платежной) картой** понимается средство для составления расчетных и иных документов, подлежащих оплате за счет клиента, т.е. физического или юридического лица, заключившего с кредитной организацией-эмитентом банковской карты договор, предусматривающий осуществление операций с ее использованием. Она представляет собой пластиковый прямо-

угольник со специальной магнитной полосой, в памяти которой хранится информация, необходимая для расчетов за товары (работы, услуги) либо для снятия наличных денег за счет имеющихся на карточном счете сумм.

Магнитная банковская карта - это только отражение банковского счета владельца: ее магнитный индикатор содержит лишь информацию об имени владельца и номере его счета в банке. Поэтому при расчетах с использованием этой карты каждый раз необходимо обращаться к центральному компьютеру для получения информации о наличии на счете необходимой для оплаты товаров (работ, услуг) суммы денег. При использовании магнитной карты следует пройти процедуру персонификации - уточнения того факта, что картой владеет именно ее предъявитель. Связь с системным кассовым терминалом нужна для дачи команды на списание определенной суммы денег, подлежащей оплате.

Чиповая карта содержит микропроцессор (чип) - маленький квадратик или овал на лицевой стороне, в памяти которого содержится вся информация о банковском счете ее владельца: о количестве денег на счете, максимальном размере суммы, которую можно снять со счета единовременно, об операциях, совершенных в течение дня. Чиповая карта - это одновременно и кошелек, и средство расчета, и банковский счет. И это все благодаря микропроцессору, главным достоинством которого является его высокая способность при постоянстве памяти надежно сохранять и использовать большие объемы информации. При этом чиповая карта не нуждается в процедуре идентификации и персонификации, а значит, способна работать в режиме off-line, что не требует обращения при каждом необходимом случае к банку или компании, где открыт счет владельца карты.

Список литературы

а) Нормативные правовые акты:

1. Преступления, связанные с использованием компьютерной сети / Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями // A / CONF.187/10. - Доступ из СПС «Консультант плюс» (дата обращения 13.03.2018).

2. 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: приказ МВД РФ от 29 августа 2014 г. № 736: в ред. приказа МВД России от 07.11.2016 № 708. - Доступ из СПС «Консультант плюс» (дата обращения 13.03.2018).

3. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. - Доступ из СПС «Консультант плюс» (дата обращения 13.03.2018).

4. Конституция Российской Федерации // Собрание законодательства РФ. - 2014. - № 9. - Ст. 851.

5. Уголовно-процессуальный кодекс Российской Федерации // Собрание законодательства РФ. - 2001.- № 52 (часть I). - Ст. 4921.

6. Уголовный кодекс Российской Федерации // Собрание законодательства РФ. - 1996. - № 25. - Ст. 2954.

7. О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ // Собрание законодательства Российской Федерации. - 2011. -№ 27. - Ст. 3872.

8. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации. - 2006. - № 31 (часть I). - Ст. 3451.

9. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ //

Собрание законодательства Российской Федерации. - 2006. - № 31 (часть I). - Ст. 3448.

10. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. - Доступ из СПС «Консультант плюс» (дата обращения 13.03.2018).

б) Основная литература:

1. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий / А.В. Шмонин и др. – М., 2016. - 189 с.

2. Баркалов Ю.М. Актуальные проблемы информационной безопасности: методические рекомендации для стран СНГ/ Ю.М. Баркалов. - Воронеж, 2015.

в) Дополнительная литература:

1. Ревенков П.В. Управление рисками в условиях электронного банкинга: автореф. дис. ... д-ра эконом. наук / П.В. Ревенков. - СПб., 2013.

2. Выборнов А. Устранение уязвимостей / А.Выборнов // BIS journal. - 2014. - № 4.

3. Яковлев А.Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: "электронная почта" / А.Н. Яковлев // Вестник Воронежского института МВД России. - 2014. - № 4. - С. 46.

4. Шевченко Е.С. Актуальные проблемы расследования киберпреступлений / Е.С. Шевченко // Эксперт-криминалист. - 2015. - № 3.

5. Бутенко О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия / О.С. Бутенко // Lex russica. - 2016. – № 4.

6. Чекунов И.Г. Современное состояние киберпреступности в Российской Федерации. / И.Г. Чекунов, Р.Н. Шумов // Российский следователь. - 2016. - № 10.

7. Хажевскас А. Актуальные проблемы проведения экспертизы информационных технологий / А. Хажевскас, К. Гражялис, А. Горбатков // Эксперт-криминалист. – 2013. - № 3.

г) Интернет - источники:

1. Греф: необходимо создать систему по борьбе с киберпреступниками. – URL: http://ria.ru/economy/20160412714092152 02.html (дата обращения: 13.03.2018).

2. Безопасность банковских карт: взгляд потребителя и активность игроков рынка. Отчет по результатам исследования. - М.: Национальное агентство финансовых исследований, 2017. - URL: http://nacfin.ru/wpcontent/uploads/2017/01/moshennichestvo_bankovskie_karty.pdf.

Приложение

ТЕЛЕФОНЫ ГОРЯЧИХ ЛИНИЙ БАНКОВ РТ

Банк	Телефон горячей линии
ПАО «Сбербанк»	**+7 (495) 500-55-50** **8 (800) 555-55-50** **короткий номер 900**
Россельхозбанк	**8(800) 200-02-90 8(800) 100-01-00**
ВТБ	8(800) 200-77-99
ВТБ -24 банк	8(800) 100-24-24
Абсолют Банк	8(800) 200-20-05
Авангард Банк	8(800) 333-98-98
Аверс Банк	8(800) 77-518-77
Агросоюз Банк	8(800) 555-00-91
Альфа-Банк	8(800) 200-00-00 8(800) 100-77-33
Ак Барс банк	8(800) 200-53-03
Автоградбанк	8(800) 510-35-10
Банк Казани	8(800) 77-518-77
БТА-Казань банк	8(800) 100-66-77
Банк жилищного финансирования	8(800) 555-00-26
Банк Интеза	8(800) 200-80-08
Банк Союз	8(800) 100-33-22
Бин Банк	8(800) 200-50-75 8(800) 555-55-75

Банк	Телефон горячей линии
Бинбанк Диджитал	8(800) 200-20-80
Бкс Банк	8(800) 500-70-65
Быстро Банк	8(800) 333-22-65
ВТБ Банк Москвы	8(800) 200-23-26
Газпром Банк	8(800) 100-07-01
Гута Банк	8(800) 100-47-00
Девон-Кредит банк	8(800) 200-92-22
Дельтакредит Банк	8(800) 200-07-07
Запсибкомбанк	8(800) 100-50-05
Камский коммерческий банк	8(800) 200-04-38
Киви Банк	8(800) 707-77-59
Кредит Европа банк	8(800) 700-77-57
Локо Банк	8(800) 250-50-50
МДМ Банк	8(800) 200-37-00
Модульбанк	8(800) 222-92-45
МТС Банк	8(800) 250-05-20
Национальный банк сбережений	8(800) 100-50-50
Опт Банк	8(800) 100-55-55
Открытие банк	8(800) 700-78-77
Почта Банк	8(800) 550-07-70

Банк	Телефон горячей линии
Плюс Банк	8(800) 200-23-72
Промсвязь Банк	8(800) 555-20-20 8(800) 700-50-33 8(800) 333-03-50
Райффайзенбанк	8(800) 700-91-00
Радиотехбанк	8(800) 200-58-59
Ренессанс кредит	8(800) 200-09-81
Росбанк	8(800) 200-54-34
Росгосстрах Банк	8(800) 700-40-40
Рост Банк	8(800) 200-50-75
Русский Стандарт	8(800) 200-62-00
Русфинанс Банк	8(800) 700-27-27
Связь Банк	8(800) 500-00-80
СКБ банк	8(800) 100-06-00
Совкомбанк	8(800) 200-66-96
Солид банк	8(800) 775-56-06
Сетелем Банк	8(800) 500-55-03
Тимер Банк	8(800) 100-66-77
Хоумкредит Банк	8(800) 700-80-06
Уралсиб Банк	8(800) 200-55-20
Уральский банк реконструкции и развития	8(800) 100-02-00
Юникредит Банк	8(800) 700-73-00 8(800) 700-10-20

Практическое издание

Шевко Наиля Рашидовна
Каримов Адель Миннурович

ДЕЙСТВИЯ ДЕЖУРНОГО ПРИ ПОСТУПЛЕНИИ СООБЩЕНИЯ О ПРЕСТУПЛЕНИИ, СОВЕРШЕННОМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Памятка

Компьютерный набор Н.Р. Шевко
Корректор Н.А. Климанова

Подписано в печать 12.11.2018
Усл. печ. л.1,8 Тираж 30 экз.

Типография КЮИ МВД России
420108 г. Казань, ул. Магистральная, 35