ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ПЕРВОНАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ И ИХ РЕКВИЗИТОВ

Учебное пособие

Уфа 2022

УДК 351.745.078(470)(075.8)
ББК 67.401.133.12-9(2Рос)я73-1
П26

Рекомендовано к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России

Рецензенты:
кандидат юридических наук, доцент В. Н. Чаплыгина
(Орловский юридический институт МВД России имени В. В. Лукьянова);
кандидат юридических наук Т. А. Бадзгарадзе
(Санкт-Петербургский университет МВД России)

Коллектив авторов:
Ю. Б. Имаева – кандидат юридических наук, доцент;
А. Ю. Самойлов – кандидат юридических наук, доцент;
Г. Х. Афзалетдинова – кандидат юридических наук, б/з;
Л. Н. Ермолаева – б/с; б/з

П26 **Первоначальный этап расследования хищений, совершенных с использованием банковских карт и их реквизитов** : учебное пособие / Ю. Б. Имаева [и др.]. – Уфа : Уфимский ЮИ МВД России, 2022. – 48 с. – Текст : непосредственный.

ISBN 978-5-7247-1110-4

В учебном пособии рассматриваются разнообразные способы хищений, совершенные с использованием банковских карт и их реквизитов, и актуальные проблемы и особенности производства отдельных следственных действий на первоначальном этапе расследования, предлагаются криминалистические рекомендации, направленные на совершенствование расследования хищений, совершенных с использованием банковских карт и их реквизитов.

Предназначено для обучающихся образовательных организаций МВД России.

УДК 351.745.078(470)(075.8)
ББК 67.401.133.12-9(2Рос)я73-1

ISBN 978-5-7247-1110-4

© Коллектив авторов, 2022
© Уфимский ЮИ МВД России, 2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Несколько последних лет ознаменовались динамичным развитием высоких технологий, являющихся закономерным проявлением формирующегося информационного общества. Быстрое становление, развитие и совершенствование информационных технологий, в том числе по предоставлению услуг в дистанционном формате, не могло не оставить в стороне такой аспект, как оборот денежных ресурсов, выступающих универсальным средством урегулирования различных обязательств возмездного характера. Нынешние условия констатируют тот факт, что электронные средства платежа[1] и системы постепенно даже вытесняют оборот с наличными денежными средствами. Согласно данным Банка России среди операций, совершаемых с помощью банковских карт, преобладают не снятие наличных денежных средств, а совершение иных операций безналичного характера, характеризующихся дальнейшей циркуляцией денежных средств с помощью соответствующих электронных систем. Всего же за 2021 год с использованием платежных карт, эмитированных банками, расположенными на территории Российской Федерации, было совершено 231,5 млн операций[2]. Новые способы оплаты не остались без внимания лиц, желающих незаконно обогатиться.

Так, официальная статистика МВД России свидетельствует, что в 2021 году число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 32,2 % по сравнению с прошлым годом, в том числе с использованием сети Интернет – на 51,3 %, при помощи средств мобильной связи – на 39 %, количество нераскрытых преступлений составило 388 607[3].

Приведенные статистические данные подтверждают потребность в глубоком и тщательном криминалистическом исследовании хищений, совершенных с использованием банковских карт и их реквизитов (электронных средств платежа), и в разработке методико-криминалистических ре-

---

[1] В соответствии со ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» электронное средство платежа – средство и (или) способ, позволяющие 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 // Официальный интернет-портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 01.02.2022).

[2] Статистика национальной платежной системы (2021) // Центральный Банк России. – URL: http://www.cbr.ru/statistics/nps/psrf/ (дата обращения: 01.02.2022).

[3] Краткая характеристика состояния преступности за январь–декабрь 2021 г. // Информационно-аналитический портал Министерства внутренних дел Российской Федерации. – URL: https://мвд.рф/reports/item/28021552/ (дата обращения: 01.02.2022).

комендаций, направленных на выявление, раскрытие и расследование этих деяний.

Федеральный закон Российской Федерации от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» (далее – УК РФ) модернизировал положения некоторых составов, касающихся преступлений против собственности, которые, применительно к рассматриваемым нами преступлениям, могут быть следующими: п. «г» ч. 3 ст. 158 УК РФ – кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ); ст. 159.3 УК РФ – мошенничество с использованием электронных средств платежа; п. «в» ч. 3 с. 159.6 УК РФ – мошенничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении электронных денежных средств; ст. 160 УК РФ (присвоение или растрата), ст. 161 УК РФ (грабеж), ст. 162 УК РФ (разбой). Отметим, что такие формы хищения, как разбой, грабеж и присвоение нельзя признать не заслуживающими внимания, так как анализ судебно-следственной практики выявил их отрицательную динамику; расследование данной категории дел вызывает не меньшее затруднение со стороны правоохранительных органов.

Раскрытие и расследование хищений, совершенных с использованием банковских карт и их реквизитов, остается довольно сложной задачей для большинства сотрудников органов предварительного расследования. Это отчасти обусловлено отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки следователей по соответствующей специализации.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ И ИХ РЕКВИЗИТОВ

§ 1. Криминалистически значимые сведения о способе и обстановке совершения хищений

Анализируя мнения различных авторов о структуре криминалистической характеристики, необходимо отметить, что количество криминалистически значимых признаков до настоящего времени не определено и, на наш взгляд, количество элементов должно определяться исходя из важности корреляционных связей между элементами, способствующих дальнейшему раскрытию и расследованию преступлений.

Изучив существующие мнения о криминалистической характеристике и ее элементах, базируясь на анализе судебно-следственной практики по делам о хищениях с использованием банковских карт и их реквизитов[1], характеристике форм хищений, а также необходимости нахождения элементов в такой взаимосвязи, чтобы как можно полнее раскрыть те значимые криминалистические данные, которые характеризуют все формы хищений, предлагаем отнести к элементам криминалистической характеристики:

1. Криминалистически значимые данные о способах подготовки, совершения и сокрытия преступлений.

2. Криминалистически значимые данные о предмете и обстановке совершения хищения.

3. Криминалистически значимые сведения о личности преступника и потерпевшего (держателя карты).

4. Криминалистически значимые данные о механизме следообразования.

Криминалистически значимые данные о способах подготовки, совершения и сокрытия преступлений. Совершение хищений с использованием банковских платежных карт невозможно без предварительной подготовки, изучения и оценки обстановки, создания необходимых условий, облегчающих доступ к чужой банковской карте или ее реквизитам, обеспечения возможности сокрытия хищения.

Все подготовительные действия можно разделить на три группы: действия, связанные с обеспечением доступа к самой банковской карте; действия, связанные с обеспечением доступа к реквизитам банковской карты (банковскому счету) или персональным данным держателя карты;

[1] Здесь и далее используется обзор судебно-следственной практики по уголовным делам, рассмотренным судами общей юрисдикции в 2017–2020 гг. – URL: http://www.sudact.ru (дата обращения: 03.02.2022).

действия, связанные с созданием (подбором) условий, облегчающим совершение преступления.

I. Подготовительные действия, направленные на завладение банковской картой могут быть следующими:

1. Правомерное получение карты, например, держатель карты сам передал субъекту преступления банковскую карту для совершения по его просьбе каких-либо действий.

2. Неправомерное завладение картой: обнаружение находящейся в свободном доступе чужой (утерянной, оставленной без присмотра) банковской карты; тайное хищение банковской карты свободным доступом при законном нахождении в жилом или ином помещении; тайное хищение банковской карты из одежды, носильных вещей и т. д., принадлежащих потерпевшему; открытое хищение банковской карты (путем грабежа, разбоя), в том числе вместе с сопутствующими предметами (кошельком, сумкой, одеждой и пр.); завладение картой путем обмана или введения в заблуждение потерпевшего; обнаружение чужой карты в слоте банкомата, в том числе в результате отмены незавершенной финансовой операции.

II. Действия, сопряженные с обеспечением доступа к реквизитам банковской карты (банковскому счету) или персональным данным держателя карты, могут быть следующими:

1. Завладение мобильным телефоном (смартфоном) или SIM-картой, подключенной к услуге «Мобильный банк». Преступники получают телефон или SIM-карту[1] в свое владение путем хищения (кражи, грабежа, разбоя, мошенничества), находки утерянного телефона или SIM-карты, покупки (согласно установленному порядку через шесть месяцев после отказа от телефонного номера оператор сотовой связи вправе передать (продать) абонентские номера другим пользователям).

2. Получение конфиденциальной информации о держателе карты и его счете, использующем дистанционное банковское обслуживание (далее – ДБО), например, потерпевший сам позволяет пользоваться интернет-банкингом третьим лицам; получение пароля доступа через Интернет; получение пароля доступа через SMS-уведомление якобы от банка.

III. Действия, связанные с созданием (подбором) условий, облегчающим совершение преступления:

1. Подбор соучастников, которые будут выполнять роль пособников в совершении преступления, например, обналичивать похищенные денежные средства. Сюда же можно отнести подбор лиц, которые не осведомлены о преступных замыслах преступника.

[1] SIM-карта (англ. Subscriber Identification Module− модуль идентификации абонента) − идентификационный модуль абонента, применяемый в мобильной связи. – URL: https://dic.academic.ru/dic.nsf/es (дата обращения: 03.02.2022).

2. Установление информации о держателях карт и наличии на принадлежащих им банковских счетах денежных средств в целях определения суммы хищения.

3. Выбор будущей жертвы – держателя карты и сбор сведений об имеющихся на карте денежных средствах.

4. Выбор места хищения карты и места хищения денежных средств.

5. Приискание SIM-карт, электронных устройств, предназначенных для дальнейшего общения с жертвой, приобретение «базы клиентов» банков, открытие счетов для зачисления денежных средств и т. д.

Применительно к рассматриваемой категории преступлений ученые предлагают различные классификации способов хищений, поэтому, в целях сравнительного анализа акцентируем внимание на нескольких вариантах видения этой проблемы в специальной литературе.

Для хищения денежных средств с использованием банковских карт и их реквизитов преступники используют следующие способы:

1. Проведение транзакции[1] с использованием похищенной карты и PIN-кода. В данном случае следует заметить, что хищение самой карточки еще не влечет возможности наступления общественно опасных последствий в виде причинения материального ущерба держателю карты, так как тайное хищение денежных средств в данном случае возможно только при наличии PIN-кода.

2. Проведение транзакции с использованием банковских карт утерянных или временно вышедших из владения потерпевшего, а также банковских карт, находящихся у виновных на законных основаниях.

Например, М., являясь главным бухгалтером краевого государственного казенного учреждения «Центр содействия семейному трудоустройству детей-сирот и детей, оставшихся без попечения родителей», обладала полномочиями по обналичиванию денежных средств с банковской карты ПАО «Сбербанк», привязанной к расчетному счету учреждения, открытому в Управлении федерального казначейства, используя свое служебное положение неоднократно, находясь в отделении ПАО «Сбербанк», снимала с указанной банковской карты наличные денежные средства, предназначенные для приобретения товаров воспитанникам. Впоследствии, с целью сокрытия хищения, М. вносила в авансовые отчеты сведения о приобретении имущества для нужд учреждения на сумму 152 430 рублей 85 копеек. Действия М. судом были квалифицированы как присвоение чужого имущества, вверенного виновному, совершенное лицом с использованием своего служебного положения[2].

---

[1] Транзакция – любая операция на банковской карте, связанная с изменением ее счета. – URL:https://dic.academic.ru/dic.nsf/fin_enc/30557 (дата обращения: 04.02.2022).

[2] Приговор по уголовному делу № 1-111/2020 // Арх. Чугуевского районного суду (Приморский край).

3. Хищение, сопряженное с несанкционированным внесением изменений в программы, обеспечивающие проведение расчетных операций с использованием банковских карт.

Например, К. в мессенджере «Telegram» посмотрела видеоролики о способе хищения денежных средств посредством устройств самообслуживания с банковских счетов ПАО «Сбербанк». После чего К. взяла на время у своей знакомой Ч. банковскую карту со счетом, открытым в ПАО «Сбербанк России» и пришла к банкомату, где зная PIN-код, выбрала операцию по внесению наличных денежных средств. Когда открылся шаттер для приема наличных денежных средств, К. стала удерживать его, инициируя сбой в программном обеспечении оборудования, в связи с чем на экране появилось сообщение об оформлении претензии ввиду незачисления на счет карты денежных средств. После этого К., используя клавиатуру устройства самообслуживания, оформила претензию на сумму 5000 рублей. На следующий день денежные средства в сумме 5000 рублей, принадлежащие ПАО «Сбербанк России», были списаны с банковского счета ПАО «Сбербанк» и зачислены на банковский счет карты на имя Ч. Поступившие денежные средства К. обратила в свою пользу[1].

4. Оформление путем обмана или злоупотребления доверием кредитов и займов с использованием реквизитов чужой банковской карты с последующим переводом виновным денежных средств на свой или подконтрольный ему счет.

5. Проведение транзакции путем перевода денежных средств потерпевшего на счет преступника или подконтрольный ему счет, оформленный на третьих лиц, при этом возможно понуждение потерпевшего путем психологического воздействия, когда он сообщает преступнику необходимые для доступа к банковскому счету реквизиты.

Например, неизвестный позвонил С. и, представившись, сотрудником ПАО «Сбербанк», сообщил, что на его имя оформлен кредитный договор на сумму 312 000 рублей, в том числе в нее входит страхование жизни, а сумма кредита – 275 000 рублей, и эта сумма ему переведена на карту. При этом С. не обращался с заявкой на оформление кредита и, соответственно, кредит не оформлял. «Сотрудник банка», выслушав пояснения С., предложил ему закрыть кредит и предложил перевести деньги по номеру телефона на счет ПАО «Сбербанк». Звонивший пояснил, что в отделение Банка обращаться нельзя, поскольку там могут находиться мошенники, «которые, возможно, и оформили на его имя этот кредит». Впоследствии С., следуя указаниям «сотрудника банка», сообщил звонившему цифры, которые написаны на оборотной стороне карты, и передавал ему коды, приходившие на номер его телефона. Таким образом, платежами по 50 000 рублей была переведена сумма 275 000 рублей. После

[1] Приговор по уголовному делу № 1-89/2020 // Арх. Курчатовского районного суда (Курская область).

перевода последней суммы «сотрудник банка» сообщил ему, что кредитная история закрыта. Спустя несколько минут после всех этих событий С. понял, что стал жертвой мошенника, и обратился в отдел полиции[1].

Данный способ хищений имеет несколько разновидностей, которые условно можно разделить на следующие:

5.1. «Ваша карта заблокирована».

Например, Ш., отбывая наказание в ФКУ ИК-28 ГУФСИН России по Самарской области, вступила в предварительный сговор с неустановленными лицами на завладение путем обмана имуществом граждан-держателей банковских карт. Согласно распределению ролей внутри группы Ш. была обязана общаться с держателями карт с использованием средств сотовой связи, убеждать их путем обмана выполнить перевод своих денежных средств с банковских карт на указанные Ш. платежные реквизиты. В дальнейшем Ш. и неустановленные лица действовали следующим образом: неустановленное лицо с использованием аппарата сотовой связи отправило на абонентский номер потерпевшего SMS-сообщение, где содержались заведомо ложные сведения о блокировании принадлежащей ему банковской карты. Потерпевший, получив сообщение о блокировке карты перезванивал на указанный в SMS-сообщении номер, который находился в пользовании осужденной Ш. В ходе разговора Ш., выдавая себя за сотрудника банка, сообщала потерпевшим, что их карта заблокирована, а для того, чтобы «сохранить» денежные средства, их необходимо перечислить на другой счет, который она укажет. Потерпевшие переводили денежные средства по указанным Ш. реквизитам, после чего они обналичивались и обращались виновными в свою пользу[2].

5.2. «Перевод денежных средств путем входа злоумышленником в личный кабинет мобильного банка», например, «СберБанк Онлайн».

Например, Л. попросил у своей знакомой А. банковскую карту, которой та в настоящее время не пользуется, для зачисления на нее денежных средств от работодателя. А. согласилась и передала Л. свою личную расчетную карту ПАО «Сбербанк» и PIN-код к ней. Впоследствии на мобильный телефон А. стали приходить сообщения о поступлении на карту денежных средств, о чем она сразу уведомляла Л. Через некоторое время Л. попросил у А. разрешение установить приложение «СберБанк Онлайн» на его телефон и привязать карту к его мобильному телефону, а также открыть дополнительные услуги, так как самому далеко ходить до банко-

[1] Решение № 2-216/2020 2-216/2020~М-181/2020 М-181/2020 от 7 сентября 2020 г. по делу № 2-216/2020 // Архив Островского районного суда (Костромская область).

[2] Приговор по уголовному делу № № 1-242/2019 // Арх. Волжского районного суда (Самарская область).

мата, на что А. также дала согласие. Спустя некоторое время А. получила в ПАО «Сбербанк» кредитную карту на свое имя, которую в пользование никому не передавала и сама данной картой не пользовалась. Через какое-то время А. стали приходить SMS-уведомления о списании денежных средств с банковской карты, однако сразу понять с какой карты происходит списание, с расчетной, которая находится у Л., или кредитной, она понять не могла, так как на ее телефоне приложение «СберБанк Онлайн» не установлено. Впоследствии А. выяснила, что Л., воспользовавшись мобильным приложением, получил доступ к ее кредитной карте, с которой переводил денежные средства на другие свои счета[1].

5.3. Использование работающих в сети Интернет электронных торговых площадок «Авито», «Юла», интернет-магазинов и т. д. или посредством использования социальных сетей («Одноклассники», «ВКонтакте», «Мой Мир» и др.).

Например, М. с использованием информационно-телекоммуникационной сети Интернет и сотового телефона нашел на сайте «Авито.ру» объявление о продаже мебели. Далее М, используя сотовый телефон и чужую SIM-карту сотового оператора ПАО «Вымпел-Коммуникации», под видом покупателя позвонил по номеру, указанному продавцом в объявлении, и под предлогом перевода денежных средств на счет банковской карты продавца в качестве оплаты за мебель убедил последнего сообщить конфиденциальную информацию по банковской карте ПАО «Сбербанк России», а именно номер банковской карты, срок ее действия, код безопасности и пароли, полученные SMS-сообщениями. М., воспользовавшись полученной информацией, перевел денежные средства с банковского счета потерпевшего на лицевой счет, находящийся в его пользовании[2].

Другой пример. Б. в составе группы лиц по предварительную сговору совершила несколько краж с банковских счетов при следующих обстоятельствах: Б. и неустановленное следствием лицо, используя средства мобильной связи со специальным программным обеспечением «KoronaPay», подыскивали в социальной сети «Одноклассники» объявления физических лиц о продаже товаров. Затем Б. звонила по указанному в объявлении номеру и сообщала продавцу свои намерения приобрести товар путем безналичного перевода денежных средств на счета, привязанные к банковским картам потерпевшего. В ходе разговора Б. убеждала держателя карты сообщить ей реквизиты карты, пароли и другие сведения, необходимые для перевода денежных средств. После получения дан-

[1] Приговор по уголовному дело № 1-269/2020 // Арх. Новочебоксарский городской суд (Чувашская Республика).

[2] Приговор по уголовному делу № 1-283/2020 // Арх. Новочебоксарский городской суд (Чувашская Республика).

ной информации Б., используя сотовый телефон, подключенный к информационно-телекоммуникационной сети Интернет с установленными приложениями «KoronaPay» для осуществления перевода денежных средств со счета банковской карты на подконтрольный электронный кошелек карты, создавала запрос о списании денежных средств со счета банковской карты потерпевшего, после чего вводила полученные от потерпевшего данные в форму запроса. После получения доступа к денежным средствам, находящимся на счете банковской карты потерпевшего, Б. и неустановленное лицо перечисляли деньги со счета банковской карты потерпевшего на подконтрольные им карты, распорядившись ими в последующем по своему усмотрению[1].

К способам скрытия хищений с использованием банковских карт и их реквизитов можно отнести:

– использование для перечисления похищенных денежных средств банковских счетов (в том числе транзитных) соответствующих им банковских карт, зарегистрированных на имя иных лиц;

– использование паспортных и иных персональных данных иных лиц;

– использование чужих технических средств (мобильных телефонов, смартфонов, компьютеров, ноутбуков и т. д.);

– использование аккаунтов, профилей, SIM-карт (контактных номеров) и т. п., зарегистрированных на имя других лиц, а равно относящихся к другим регионам по отношению к профилям (контактным номерам) потерпевших;

– использование программного обеспечения, позволяющего визуально изменить номер исходящего контакта;

– уничтожение банковских и SIM-карт;

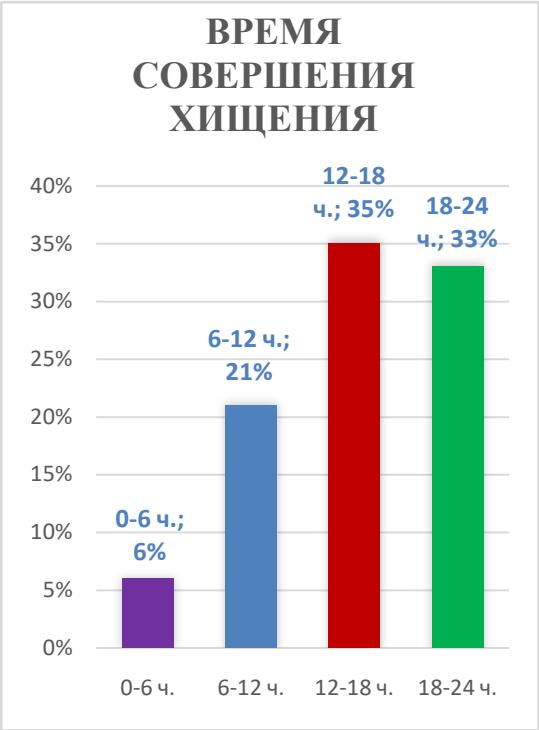
– уничтожение слипов, чеков, квитанций, полученных в результате проведения транзакции;

– маскировка внешности при использовании чужой банковской карты;

– осуществление мероприятий, позволяющих в момент попытки воздействия на жертву скрыть свое истинное местонахождение.

Обстановка совершения хищения. Выбор преступником способа действия зависит не только от наличия у него определенной профессиональной подготовки или наличия соучастников, но и от особенностей *места совершения преступления*, времени, наличия у преступника средств совершения преступления.

[1] Приговор по уголовному делу № 1-51/2020 // Арх. Топчихинский районный суд (Алтайский край).



Время совершения хищения напрямую связано не только с местом совершения хищения, но и с местом и временем завладения банковской картой. Так, в 41,13 % случаев хищения денежных средств совершались в течение трех часов после завладения картой и в 36,54 % − в течение первого часа. Это обусловлено тем, что преступник предполагает скорое обнаружение потерпевшим пропажи карты и последующую блокировку. В 12,41 % случаев преступник использует чужую банковскую карту, находящуюся в его владении, в течение продолжительного времени, будучи уверенным, что потерпевший длительно не обнаружит хищения денежных средств.

В случае совершения открытого хищения денежных средств и ряда краж завладение картой и денежными средствами происходит почти одновременно в присутствии потерпевшего 8,8 %.

Предмет хищения. Сами банковские карты (кредитные или расчетные) не являются предметом хищения, так как действия виновного направлены на противоправное завладение в итоге не ими, а денежными средствами, поэтому предметом хищения являются денежные средства, а банковская карта выполняет роль средства (орудия) совершения преступления.

В качестве предмета хищения, совершенного с использованием банковских карт и их реквизитов, следует признавать имущество в виде безналичных денег, то есть сумму, записанную на карточном счете держателя карточки, либо денежные средства участников осуществления системы безналичных расчетов с использованием банковских карт. Необходимо отметить, что в отличие от наличных денег, безналичные деньги находятся

не у держателя карты, а у третьего лица – банка, который не может ими распоряжаться.

Ошибочно считать, что при расследовании данной категории дел предметом являются лишь денежные средства. Действительно, если речь идет о таких формах хищений, как кража, грабеж, разбой, присвоение или растрата, предметом хищения могут быть только денежные средства. Однако при расследовании мошенничества с использованием банковских карт предметом преступного посягательства могут быть и различные товарно-материальные ценности, приобретенные с использованием банковской карты: бытовая техника, продукты питания, спиртные напитки.

§ 2. Криминалистически значимые сведения о личности преступника и потерпевшего

Эффективное расследование преступления с установлением всех обстоятельств совершенного деяния невозможно без установления и изучения *личности преступника*, так как «изучение личности обвиняемого является основной составной частью работы следователя по конкретному уголовному делу»[1]. Кроме того, как известно, данные о личности обвиняемого являются обязательным элементом предмета доказывания и криминалистической характеристики преступления. Полное, всестороннее и объективное расследование преступлений, обеспечение соблюдения законности на предварительном следствии зависят от знания следователем типичных личностных особенностей преступников, для чего необходимо их подробное изучение.

Проявлением характеристики личности преступника, по нашему мнению, является взаимосвязь свойств, связей личности, которые не только имеют значение для подготовки, совершения и сокрытия преступления, но и являются его содержанием как элемента криминалистической характеристики, который определяется конкретным набором признаков личности, специфичных для лиц, совершающих конкретный вид преступления.

Совершение данного вида преступления невозможно без наличия у преступника знаний об обороте пластиковых карт, к которым, на наш взгляд, вполне можно отнести: во-первых, знания о видах платежных карточек, механизме их использования, во-вторых, знания о сущест-

[1] Коршик М. Г., Степичев С. С. Изучение личности обвиняемого на предварительном следствии / под ред. проф. А. И. Винберга. – М., 1961. – С. 19.

вующей защите карточек, в-третьих (что немаловажно при использовании реквизитов банковских карт знания), о процессинге банковских карт[1].

Анализируя субъектов преступления, следует согласиться с мнением П. Б. Смагоринского о том, что «анализ хищений чужого имущества, совершенных с использованием пластиковых карт, показывает, что одному лицу достаточно сложно решить весь комплекс возникающих при этом проблем. Поэтому, нередко, на этапе подготовки к совершению преступления и на этапе его реализации действуют совершенно разные лица»[2].

Рассматривая криминалистическое значение информации о личности преступника при расследовании хищений с использованием банковских карт, следователю необходимо акцентировать внимание на значимости сведений о характерных свойствах личности субъекта преступления для эффективного выбора дальнейших тактических приемов и выдвижения следственных версий.

Проведенный нами анализ состояния, динамики и структуры хищений с использованием банковских карт, а также характеристики субъекта преступления позволил нам обнаружить следующие закономерности: наиболее многочисленную группу составляют лица в возрасте от 25 до 31 года – 37,73 %, 18–25 лет – 31,6 %, 30–35 лет – 17,92 %, 35–40 лет – 11,32 %, несовершеннолетние составляют 0,47 %, и 0,94 % составляют лица в возрасте старше 40 лет. По нашему мнению, то, что число лиц в возрасте от 40 лет, совершивших подобные хищения, невелико, объясняется тем, что данная категория лиц не обладает достаточными знаниями о механизме использования банковских карт.

Изучение данных видов хищений показало, что распределение лиц по полу имеет определенные особенности:

– грабежи и разбои на открытой местности совершаются лицами мужского пола, которые применяют насилие для завладения картой и получения PIN-кода к ней от потерпевших;

– значительное число мошенничества совершается лицами мужского пола, обладающими определенными знаниями в сфере электронного оборота денежных средств;

– доля лиц женского пола заметно выше в категории мошенников и расхитителей, которые являются банковскими работниками – 65,4 %;

---

[1] Процессинг – это общая совокупность всех операций, которые выполняются при проведении платежей и зачислении денежных средств на счет получателя. Проведение заявленных операций возможно благодаря высоким ресурсным и программным мощностям электронного банкинга. – URL: https://dic.academic.ru/contents.nsf/business/ (дата обращения: 03.02.2022).

[2] Смагоринский П. Б. Криминалистическая характеристика хищений чужого имущества, совершенных с использованием пластиковых карт и ее применение в следственной практике : автореф. дис. … канд. юрид. наук (12.00.09) / Смагоринский Павел Борисович; Волгоградский гос. ун-т. – Волгоград, 2020. – С. 15.

– лица, обладающие обывательскими знаниями в области использования банковских карт, совершают в основном кражи – 55,06 %.

Образовательный уровень лиц, совершающих преступления с банковскими картами и их реквизитами, распределяется следующим образом:

– нигде не работали – 58,96 %,

– имеют постоянный источник дохода – 34,43 %;

– ранее судимые за совершение корыстных преступлений – 29 %;

– ранее судимые за совершение преступлений против личности – 8 %;

– против общественной нравственности и здоровья населения – 2 %;

– ранее не судимы – 61 %;

– в составе группы лиц совершается 83,57 % мошенничества, 5,45 % краж, 37,14 % грабежей (и разбойных нападений) и 64,23 % присвоений.

Таким образом, при совершении преступлений с использованием банковских карт способ совершения позволяет существенно охарактеризовать отдельные личностные данные преступника. Так, хищения путем мошенничества совершают так называемые профессиональные «компьютерные» преступники с выраженными корыстными целями, в качестве соучастников или непосредственно исполнителей выступают сотрудники эмитента, мерчанта, эквайера, т. е. лица, также имеющие определенную профессиональную подготовку и имеющие доступ к оформлению расчетных операций с использованием платежно-расчетных карт. Сотрудники банков, совершающие хищения с использованием банковских карт, имеют доступ к персональным данным лица, обращавшегося в банк по какому-либо вопросу. И, напротив, при совершении тайного хищения денежных средств с использованием банковских карт, например, при хищении карты и PIN-кода преступник может не обладать никакими специальными знаниями, кроме как умением пользоваться банкоматом.

Выявленные основные социально-демографические признаки лиц рассматриваемой группы преступлений тесно связаны с их нравственно-психологическими качествами, знание которых необходимо для выбора тактики производства следственных действий, так как они определяют поведение преступника на предварительном следствии.

Необходимо отметить, что качественные характеристики того или иного субъекта преступления могут отличаться в зависимости от способа совершения преступления. Предложенная нами характеристика свойств преступника может помочь сотрудникам правоохранительных сузить круг лиц, которое могут быть причастны к совершению преступления, определить очередность, а также тактику производства следственных действий, в некоторых случаях выявить и преодолеть оказываемое субъектами преступления противодействие.

Криминалистические значимые сведения о личности потерпевшего. По мнению И. И. Рубцова, «от того, насколько полно изучена личность потерпевшего, нередко зависит решение таких вопросов, как обоснованность возбуждения уголовного дела, правильная квалификация преступления, продуманное выдвижение следственных версий, установление подлинных мотивов преступления, избрание наиболее эффективной тактики следственных действий, выявление конкретных причин и условий, способствовавших совершению преступления»[1].

Анализ юридической литературы показывает, что криминалисты, обратившие внимание на личность потерпевшего как на элемент криминалистической характеристики, приводят различные критерии их классификаций. Анализируя судебно-следственную практику, можно сделать вывод о взаимосвязи преступника и потерпевшего: отмечается что почти все потерпевшие сами создают благоприятные условия для совершения преступления, а именно: пренебрежительно относятся к хранению банковской карты и ее PIN-кода; совершают неосмотрительные действия с картой в присутствии будущего преступника, что создает благоприятные условия для совершения хищения и во многом провоцирует совершение противоправных действий (хранят PIN-код рядом с картой; сообщали PIN-код посторонним лицам, сообщали посторонним место хранения карты, позволяли пользоваться своим смартфоном с установленным приложением «Мобильный банк» и т. д.).

Пол, профессия, место работы, семейное положение и другие качества потерпевшего не играют существенной роли в механизме завладения картой и последующего ее преступного использования. Исключение составляет возраст потерпевшего, например, люди пожилого возраста, получающие пенсионные или другие социальные выплаты на банковскую кар-

[1] Рубцов И. И. Криминалистическая характеристика преступлений как элемент частных методик расследования : дис. … канд. юрид. наук : 12.00.09 : защищена 21.03.2000 : утв. 14.09.2000 / Рубцов Илья Ильич. – СПб, 2001. – 225 с.

ту, в основном передают карту своим родственникам или близким знакомым для получения денежных средств в банкомате, поскольку сами не хотят или не умеют пользоваться банкоматом (не хотят учиться, имеют плохое зрение, не разбираются в порядке использования карты, по состоянию здоровья не могут дойти до банкомата и т. д.). Впоследствии лица, которым была передана карта, злоупотребляют оказанным им доверием и совершают хищения.

В случаях, когда хищение денежных средств с использованием банковской карты совершается лицами, подготовившими преступление, в выборе им личности держателя карты можно проследить некоторые закономерности, а по поведению держателя карты определить дальнейшие действия преступника.

В подавляющей части случаев преступник заранее знает о количестве денежных средств на карте и о том, каким образом он может их похитить. Чаще всего это присуще банковским служащим, совершающим хищение путем мошенничества или присвоения, а также при совершении мошенничества с использованием поддельных карт, а также хищений денежных средств с использованием банковских карт своих знакомых и родственников.

Таким образом, мы считаем обоснованным исследование личности потерпевшего как элемента криминалистической характеристики рассматриваемых хищений, поскольку, как показало исследование, его поведение до совершения преступления в большинстве является немаловажным обстоятельством в принятии преступником решения о совершении преступления. Анализ личности преступника и потерпевшего играет существенную роль для установления закономерностей в определении круга виновных лиц, что позволяет правоохранительным органам более результативно проводить разыскные мероприятия.

§ 3. Криминалистически значимые данные о механизме следообразования и обстоятельствах, способствовавших совершению преступления

Как и все преступления, хищения с использованием банковских карт оставляют определенные характерные следы, знание которых помогает как выявить преступление, так и выбрать тактику проведения следственных действий, субъекту расследования получить необходимую информацию о способе совершения хищения, лице, его совершившем.

Так, при расследовании хищений, сопряженных с использованием реквизитов подлинных банковских карт и SIM-карт мобильного оператора связи, зарегистрированных на держателя карты с подключенной услугой «Мобильный банк», а также банковской карты с предоставлением ДБО к

материальным следам, а также источникам получения информации по данным следам, относятся:

– мобильный телефон и (или) SIM-карта, используемые держателем карты и (или) преступником;

– детализация счета принятия/отправки SMS, предоставленная оператором мобильной связи;

– договор на оказание услуг связи, хранящийся в офисе оператора мобильной связи, а также у потерпевшего и (или) преступника;

– сведения о местонахождении мобильного устройства в момент совершения преступления, предоставленные оператором мобильной связи;

– компьютер (другое мобильное устройство с выходом в сеть Интернет), с которого держатель карты постоянно или в последний раз пользовался услугами интернет-банкинга;

– компьютер (другое мобильное устройство), который использовался преступником для использования дистанционного банковского обслуживания (далее – ДБО) с чужими паролями доступа;

– слипы с постоянным и разовыми паролями доступа к системе интернет-банкинга; выписка по банковскому счету держателя карты, предоставленная банком;

– выписка по банковскому счету, который использовался для зачисления похищенных с банковской карты денежных средств;

– анкета-заявление на получение банковских карт и договор банковского обслуживания по счету, который использовался для зачисления денежных средств;

– выписка по банковскому счету, который использовался для дальнейшего движения похищенных денежных средств;

– видеозапись с камеры наблюдения, установленной в месте обналичивания денежных средств;

– следы пальцев рук на слипах, чеках, SIM-карте, мобильном телефоне;

– банковская карта, используемая преступником для обналичивания денежных средств;

– материальные ценности, приобретенные преступником с использованием банковской карты;

– схема, содержащая сведения о структурированной кабельной системе здания (помещения) с указанием внешних подключений, выходящих за контролируемую зону;

– протоколы работы пользователей в сети Интернет с указанием подключений, материалы проверки заявления держателя карты о несанкционированном списании денежных средств со счета банковской карты, проведенной службой безопасности банка;

– документы, подтверждающие использование лицензионного программного обеспечения, а также использования лицензионных антивирусных программ;

– документ, регламентирующий политику информационной безопасности юридического лица, содержащий сведения об ознакомлении с ней конкретных сотрудников;

– информационные системы, информация о входящем и исходящем трафике конкретного IP-адреса, хранящиеся у интернет-провайдера или системного администратора;

– документы, содержащие сведения об IP-адресах, с которых происходила авторизация с использованием похищенных учетных данных, хранящиеся в банках;

– видеозаписи с камер наблюдения, установленных в местах, где держатель карты пользовался интернет-банкингом (например, торговые центры, аэропорт и другие общественные места);

– черновые записи с паролями, используемые для доступа в ДБО;

– поддельные паспорта и иные документы, используемые преступником для регистрации юридического лица и (или) открытия банковского счета на подставное лицо для последующего обналичивания похищенных денежных средств.

При совершении хищений с использованием банковских карт могут оставаться также и идеальные следы, к носителям которых мы относим: держателя карты, сотрудников мерчанта или банка, в том числе коллег потерпевшего или преступника, сотрудников службы безопасности банка или торгово-сервисной организации, сотрудников салонов мобильной связи, родственников и знакомых держателя карты. С учетом этого к типичным идеальным следам указанного вида хищений можно отнести: сведения о внешнем виде, особенностях поведения лица, причастного к совершению хищения; сведения об общем количестве преступников; сведения о предмете хищения; сведения об обстоятельствах знакомства и взаимоотношений потерпевшего с преступником, отношениях после совершения преступления.

По мнению Е. Н. Дерябиной-Чистяковой: «Недооценка следов всегда отрицательно сказывается на ходе расследования, поэтому в криминалистике им уделяется большое внимание. Следы только тогда способны с той или иной стороны характеризовать совершенное преступление, когда принимается во внимание их совокупность и взаимосвязь, когда не остается без анализа ни один вид следов»[1].

[1] Дерябина-Чистякова Е. Н. Методика расследования мошенничества в сфере денежного обращения, кредита и банковской деятельности : дис. ... канд. юрид. наук : 12.00.09 : защищена 25.10.2006 : утв. 24.01.2007 / Дерябина-Чистякова Елена Николаевна. – М., 2006. – С. 32.

В зависимости от формы и способа хищения количество идеальных следов индивидуально. Так, мошенничество или присвоение характеризуются большим количеством идеальных следов, так как их совершение зачастую невозможно без хотя бы кратковременного контакта с другими лицами.

Анализируя указанные элементы криминалистической характеристики, мы можем резюмировать, что выбор способа хищения напрямую зависит от знаний преступниками правил банковских операций с использованием банковских карт, наличия специальных знаний в области изготовления банковских карт, занимаемой должности в кредитной организации. Наше исследование показало, что лица, намеревающиеся длительное время совершать хищения в целях получения значительного дохода, тщательно готовятся к совершению преступления: изучают дополнительную литературу, компьютерные программы и т. д., и стараются оставить как можно меньше следов. И, напротив, более тривиальные способы совершения хищений выбирают преступники, не имеющие никакой профессиональной подготовки, а их подготовка к совершению преступления занимает минимальное время непосредственно перед самим хищением. Наличие судимости влияет лишь на выбор способов подготовки к преступлению, а на выбор способа хищения влияния не оказывает.

ГЛАВА 2. ОСОБЕННОСТИ ТАКТИКИ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ, ПРОВОДИМЫХ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ И ИХ РЕКВИЗИТОВ

§ 1. Типичные ситуации расследования хищений, совершенных с использованием банковских карт и их реквизитов

Хищения денежных средств с банковских счетов граждан, совершенных с использованием банковских карт и их реквизитов целесообразно разделить на две основные группы:

1) бесконтактные, т. е. совершаемые без контакта злоумышленника с потенциальным потерпевшим;

2) контактные, т. е. совершаемые посредством установления контакта злоумышленника с потенциальным потерпевшим (например, путем телефонного звонка или SMS-сообщения)[1].

С учетом наработанного криминалистического научного инструментария и проанализированных материалов уголовных дел о преступлениях указанной категории можно сформулировать следующие типичные следственные ситуации первоначального этапа хищений, совершенных с использованием электронных средств платежа.

Рассмотрим направления деятельности следователя (дознавателя) с учетом обозначенных выше типичных следственных ситуаций первоначального этапа расследования.

Ситуация 1. Установлено хищение денежных средств, совершенное с использованием электронных средств платежа, единовременно или серийно, в отношении потерпевшего, утратившего контроль за принадлежащей ему банковской картой, реквизитами счета, контактным номером, иными средствами защиты банковского счета. Имеются отдельные данные в отношении лица (лиц), причастных к совершению преступления, а также особенностей их действий.

Данная ситуация характерна для так называемого бытового хищения, спровоцированного виктимными действиями потерпевшего (утеря банковской карты, оставление ее в общедоступном месте, передача другому лицу карты или реквизитов счета и т. п.). В распоряжении потерпевшего имеются некоторые данные относительно обстоятельств совершения деяния – SMS-сообщения о списании денежных средств с его карты/счета (снятии, перечислении, покупках товаров или услуг), что позволяет установить тот или иной объем первичной информации: от места расположения торговой, финансовой или иной организации, платежного терминала, где совершена

[1] Антонова Е. Ю., Клименко А. К. Классификация хищений денежных средств с использованием средств связи // Российский следователь. – 2019. – № 1. – С. 38–41.

операция с использованием банковской карты/счета потерпевшего, до данных о счете/карты и Ф.И.О. лица, на имя которого перечислены денежные средства со счета/карты потерпевшего. С учетом этого производится допрос потерпевшего, осмотр имеющихся у него документов, в том числе в электронной форме, а равно осмотр находящихся в его распоряжении электронных средств связи, отражающих данные относительно несанкционированной финансовой операции. Осуществляется допрос уполномоченных сотрудников торговых, финансовых или иных организаций, присутствовавших на месте происшествия в момент совершения финансовой операции, производится осмотр места происшествия, в ходе которого, наряду с уяснением общей обстановки совершения преступления, технических особенностей платежного терминала, в том числе терминала эквайринга и т. п., производится обследование и изъятие информации с электронных средств наблюдения.

Производится выемка документов из финансовых учреждений (либо направляются запросы относительно предоставления необходимой информации) относительно состояния счетов потерпевшего и лица, на счет которого были переведены денежные средства (если имел место перевод). Устанавливается причастность к деянию конкретных лиц и их местонахождение, в том числе с использованием данных относительно нахождения принадлежащих им технических средств. Допрашивается лицо, на имя которого переведены денежные средства, в зависимости от конкретных действий – в качестве свидетеля или подозреваемого, если нет оснований подозревать данное лицо в совершении преступления, отрабатываются его связи, включая, по необходимости, средства негласного контроля информации, передаваемой с помощью телекоммуникационных технологий. По мере установления лица, совершившего преступление, производится его задержание, допрос, обыск по месту жительства или месту пребывания, выемка. Назначаются необходимые экспертизы[1].

Ситуация 2. Установлено хищение денежных средств, совершенное с использованием электронных средств платежа, единовременно или неоднократно, в отношении потерпевшего, утратившего контроль за принадлежащей ему банковской картой, реквизитами счета, контактным номером, иными средствами защиты банковского счета, лицом, находящимся с потерпевшим в социально значимых отношениях.

Данная ситуация более благоприятна, поскольку изначально присутствует информация о конкретных лицах, имевших, помимо потерпевшего, доступ к данной карте и/или реквизитам банковского счета.

[1] Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.]. – М. : Юрайт, 2021. – С. 94 // ЭБС Юрайт. – URL: https://urait.ru/bcode/467208 (дата обращения: 30.01.2022).

Потерпевший подлежит допросу, после чего у него изымаются необходимые для установления обстоятельств деяния документы (касающиеся наличия и состояния банковского счета, обслуживаемого с помощью конкретной банковской карты, несанкционированных операций, проведенных с помощью его банковской карты/банковского счета), а также предметы – средства связи, благодаря которым ему стало известно о несанкционированных операциях (мобильный телефон, ноутбук, планшетный компьютер и пр.), иные предметы, указывающие напричастность к совершенному деянию конкретного лица (вплоть до оставшихся на месте личных вещей подозреваемого, несущих на себе следовую информацию).

Производится осмотр места происшествия (при необходимости) - места, где потерпевшим был утрачен контроль за картой, с целью выявления следовой информации о пребывании на месте происшествия в момент совершения деяния определенных лиц. Изъятые предметы, документы подлежат осмотру в рамках самостоятельных следственных действий.

Планируется и производится задержание подозреваемого (либо, в условиях очевидного характера деяния, лицо обязывается явкой в правоохранительные органы), подозреваемый допрашивается, путем выемки или обыска у него изымаются документы и предметы, значимые для установления обстоятельств преступления.

Допрашиваются свидетели из числа окружения потерпевшего и подозреваемого, а также лица, наблюдавшие несанкционированные финансовые операции с банковской картой/счетом потерпевшего. При наличии противоречий в показаниях проводятся очные ставки. Назначаются необходимые судебные экспертизы.

Ситуация 3. Установлено серийное хищение денежных средств, совершенное с использованием электронных средств платежа с применением методов социальной инженерии, компьютерных технологий, иных способов целенаправленного воздействия на потерпевшего и/или принадлежащие ему электронные устройства. Задержан один или некоторые соучастники группы лиц или организованной группы, совершившей данное деяние.

Приведенная ситуация являет собой (как тенденцию) причастность к деянию группы лиц или организованной группы, специализирующейся на данном виде криминальной деятельности. Методы социальной инженерии проявляются в виде телефонных обзвонов жертв, рассылки SMS-сообщений, писем в социальных сетях, по электронной почте и т. д.; вступление с жертвой в вербальный контакт (через живое общение или переписку) побуждает ее под тем или иным предлогом сообщить информацию относительно данных банковского счета/карты, контрольных данных либо лично перечислить денежные средства со счета. Вариантом также является дистанционное внедрение в электронное устройство жертвы вредоносных

программ, способствующих автоматическому перечислению денежных средств со счета потерпевшего на подконтрольные счета.

Серийный характер такой противоправной деятельности обусловливает ее многоэпизодный характер, массовые обращения потерпевших по факту преступного посягательства, в том числе в правоохранительные органы, дислоцированные на территории различных регионов России.

Необходимо допросить пропевших и провести выемку имеющихся у них документов, предметов, отражающих следовую информацию относительно обстоятельств деяния, изъять и подвергнуть обследованию в направлении поиска единого источника.

Проводятся выемки в финансовых организациях, по месту нахождения которых открыт банковский счет, в организациях, предоставляющих услуги мобильной связи и т. д.

По изъятым у потерпевших средствам связи в случае необходимости назначается компьютерная экспертиза. Установленные номинальные держатели подконтрольных банковских карт/счетов, используемых в качестве средств преступлений, а также задержанный участник группы (например, при попытке обналичивания) подлежат допросу, по месту их жительства или пребывания проводится выемка (обыск), производится контроль телефонных переговоров, получение информации с технических каналов связи, иные следственные действия.

Параллельно проводятся оперативно-розыскные мероприятия по установлению местонахождения иных лиц, совершивших деяния; связанные с негласным контролем информации, передаваемой с помощью технических каналов связи; планируется задержание с поличным соучастников в момент попытки обналичивания, во время их встреч, совершения иных действий, обусловливающих наличие доказательственной информации.

Задержанные подлежат допросу, по месту их жительства или постоянного пребывания проводятся обыски, выполняются следственные действия, связанные с негласным получением информации, передаваемой с технических каналов связи. В случае необходимости в отношении подозреваемых, а также изъятых у них объектов назначаются экспертизы: фоноскопические, трасологические, технико-криминалистические исследования документов, компьютерная экспертиза и пр. Осуществляется оперативное наблюдение, а также иные мероприятия за остальными соучастниками, оставшимися вне поля зрения уголовного судопроизводства.

Ситуация 4. Установлено серийное хищение денежных средств, совершенное с использованием электронных средств платежа с применением методов социальной инженерии, компьютерных технологий, иных способов целенаправленного воздействия на потерпевшего и/или принадлежащие ему электронные устройства. Имеются отдельные незначительные сведения в отношении лиц, причастных к совершению указанного посягательства, недостаточные для их индивидуализации.

Формированию данной ситуации также предшествует массовое обращение потерпевших, нередко проживающих в различных регионах России, в правоохранительные органы с заявлениями о фактах хищения денежных средств с помощью электронных средств платежа.

Потерпевшие подлежат подробному допросу, в ходе которого акцентируется внимание на аспектах, позволяющих сформировать психолого-криминалистический портрет субъектов преступления, обнаружить их характерные индивидуальные особенности и установить их вероятное местонахождение и иную криминалистически значимую информацию.

В отношении находящихся в распоряжении потерпевших предметов и документов, изъятых путем выемки, проводятся обследования в форме осмотра, при необходимости – судебных экспертиз.

Проводятся оперативно-розыскные мероприятия, а также обращения к потенциалу криминалистической регистрации с целью установления личности и местонахождения субъектов, причастных к данному деянию, выявления обстоятельств, указывающих на организованный характер преступной деятельности, а также данных, указывающих на совершение многоэпизодных деяний одними и теми же лицами.

Планируется задержание с поличным, затем – допросы подозреваемых, обыски и выемки по месту жительства, месту пребывания, обследование изъятых документов, средств электронной техники и иных актуальных для расследования предметов. Изъятые носители электронной информации и иные значимые объекты подлежат экспертному исследованию.

Важной особенностью механизма следообразования по кражам и мошенничествам, совершенным с использованием банковских карт и их реквизитов, является одновременное возникновение следов преступления в нескольких местах. Они возникают в рамках системы оборота банковских карт и их реквизитов, элементами которой являются: платежные системы, банки-эмитенты, банки-эквайреры, процессинговые центры, расчетные банки, торгово-сервисные предприятия, держатели карт, оборудование и коммуникации, связывающие финансовые организации между собой и с пунктами обслуживания карт. Во время проведения операций между участниками оборота банковских карт в автоматическом режиме осуществляется обмен информацией о проводимых транзакциях, что влечет за собой изменения на машинных носителях информации[1].

На стадии возбуждения уголовного дела при проверке сообщения о краже и мошенничестве рассматриваемого вида необходимо устанавливать следующие обстоятельства:

[1] Филиппов М. Н. Методика расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов // Ведомости УИС. – 2015. – № 5 (156). – URL: https://cyberleninka.ru/article/n/metodika-rassledovaniya-krazh-i-moshennichestv-sovershennyh-s-ispolzovaniem-bankovskih-kart-i-ih-rekvizitov (дата обращения: 27.01.2022).

1) факт проведения транзакции и ее характеристика (время, место совершения транзакции, способ и др.);

2) наличие и характеристику ущерба;

3) сведения о пострадавшем лице;

4) характеристику банковской карты и ее связь с пострадавшим лицом;

5) сведения о возможном совершении держателем конкретной операции с использованием банковской карты; о ее передаче другому лицу; о поручении держателем другому лицу провести транзакцию с использованием банковской карты или ее реквизитов.

Основными методами проверки сообщений о хищениях, совершенных с использованием банковских карт и их реквизитов, являются:

1) запросы в банки-эмитенты, банки-эквайреры, платежные системы с целью получения документов, отражающих факты совершения транзакций;

2) объяснения, полученные от держателей и лиц, совместно проживающих с ними;

3) осмотры мест происшествий;

4) осмотры предметов и документов: банковских карт, копий заявлений держателей об опротестовании конкретных транзакций, копий анкет держателей, копий договоров о кредитовании и выдаче банковских карт, копий выписок по карточным счетам за определенный период, копий электронных журналов банкоматов, POS-терминалов;

5) криминалистические и компьютерные исследования.

На первоначальном этапе расследования, в зависимости от места совершения хищения, возникают следующие типичные ситуации:

1) имеются сведения о совершении хищения в месте, оборудованном банкоматом;

2) имеются сведения о совершении хищения в месте, где используется POS-терминал;

3) имеются сведения о совершении хищения с использованием сети Интернет.

Общими для разрешения данных следственных ситуаций будут являться следующие действия:

1) осмотр места совершения транзакции с целью собирания и исследования следов совершения преступления;

2) допрос держателя банковской карты об обстоятельствах оспоренной транзакции;

3) допрос лиц, совместно проживающих с держателем карты, об обстоятельствах оспоренной транзакции;

4) допрос представителей банка об особенностях проведения транзакций, а также о факте совершения преступления;

5) выемка банковской карты у держателя и последующий ее осмотр с целью фиксации ее реквизитов и обнаружения на ней следов преступления[1];

6) выемка документов, подтверждающих договорные отношения между банком и держателем банковской карты, а также факт опротестования конкретных транзакций.

К тактическим особенностям осмотра места происшествия по делам о хищениях указанного вида относятся:

1) необходимость привлечения специалистов в области бухгалтерского учета и компьютерных технологий;

2) избирательность в применении тактических приемов;

3) наличие у понятых опыта использования банковских карт.

§ 2. Особенности организации первоначального этапа расследования хищений, совершенных с использованием банковских карт и их реквизитов

Для упорядочения и единообразия действий сотрудников правоохранительных органов при возбуждении и расследовании рассматриваемых видов хищений предлагаем следующий алгоритм действий.

I. При бесконтактных хищениях денежных средств при помощи дистанционного доступа к мобильным устройствам, а также персональной компьютерной техники, «зараженных» вредоносным программным обеспечением сотрудникам нужно произвести следующие действия:

1. Допросить заявителя по факту произошедшего, в допросе отразить:

− какие платежные средства использовались на компьютерной технике (мобильном устройстве сотовой связи);

− с каких платежных средств произошло хищение средств;

− когда и при каких обстоятельствах обнаружен факт хищения;

− дату и точное время платежных операций, посредством которых проведено хищение средств;

− обстоятельства работы данной техники (наличие сбоев, следов посторонних действий и т. п.)

− осуществлялось ли использование компьютерной техники (мобильного устройства сотовой связи) после обнаружения факта хищения, проводились ли ремонтные, профилактические работы.

2. В обязательном порядке разъяснить потерпевшему необходимость сохранения компьютерной техники (мобильного устройства сотовой связи)

[1] Бураева Л. А. К вопросу о классификации типичных следственных ситуаций по преступлениям, совершаемым с использованием банковских платежных карт // Проблемы экономики и юридической практики. – 2015. – № 1. – С. 108–110.

в неизменном виде (исключить использование, удаление самостоятельно вредоносного программного обеспечения).

3. Провести выемку у потерпевшего компьютерной техники в комплексе (системный блок, смартфон) либо накопителя информации (на жестких магнитных дисках (далее – НЖМД)) и т. п.

4. По изъятой компьютерной технике, мобильному устройству сотовой связи назначить компьютерную экспертизу с целью установления:

− наличия на компьютерной технике (мобильном устройстве сотовой связи) следов вредоносного программного обеспечения;

− обстоятельств установки на компьютерную технику (мобильного устройства сотовой связи) вредоносного программного обеспечения;

− следов деятельности и образцов вредоносного программного обеспечения. При формулировании вопросов для экспертного исследования целесообразно обратиться за консультацией к эксперту в соответствующей области знаний.

5. Направить запрос в банк (электронную платежную систему (далее – ЭПС), оператору связи), на счет которого перечислены похищенные денежные средства с целью установления:

− сведений о владельце банковской карты, счета (клиента ЭПС, оператора связи);

− сведений о дальнейшем движении поступивших средств до момента обналичивания либо вывода их из системы;

− IP-адресов, даты и времени доступа пользователя к системе (для электронных платежных систем).

6. Направить поручение в оперативно-разыскное подразделение с целью установления географического местоположения лица по абонентскому номеру (с которого поступали звонки потерпевшему), детализации входящих и исходящих звонков с указанием информации об абонентах (необходимо судебное решение).

7. При получении запрошенных сведений от операторов связи, электронных платежных систем, банков, операторов сотовой связи проанализировать полученные сведения, в результате чего направить материал проверки по территориальности если:

− установлено место обналичивания средств потерпевшего;

− установлен оператор связи, посредством которого осуществлялся доступ преступника к социальной сети, велась электронная переписка;

− установлено географическое положение абонентских номеров, посредством которых преступник взаимодействовал с потерпевшим.

Провести иные следственно-оперативные мероприятия направленные на раскрытие преступления.

II. При контактных, т. е. совершаемых посредством установления контакта злоумышленника с потенциальным потерпевшим (например, пу-

тем телефонного звонка или SMS-сообщения) хищениях, сотрудникам нужно произвести следующие действия.

Дополнительно, при совершении хищения, описанного как «Ваша карта заблокирована» сотрудникам правоохранительных органов необходимо:

1. Допросить потерпевшего и очевидцев, установив, на какие номера (расчетные счета) заявитель перевел денежные средства.

2. Провести выемку у потерпевшего или в банке, где открыт его банковский счет, выписки о детализации входящих и исходящих звонков по его абонентскому номеру.

3. В случае, если денежные средства были переведены на телефонные номера, необходимо направить запросы операторам сотовой связи с целью установления:

− владельцев SIM-карт;

− IMEI *(англ. International Mobile Equipment Identity* – международный идентификатор мобильного оборудования) соответствующих телефонов;

− движения денежных средств по счету абонентских номеров, на которые было осуществлено зачисление денежных средств потерпевшего и на номер, с которого звонил преступник.

4. Направить поручение в оперативно-розыскное подразделение с целью установления географического местоположения лица по абонентскому номеру (с которого поступали звонки потерпевшему), детализации входящих и исходящих звонков с указанием информации об абонентах (необходимо судебное решение).

5. В случае если денежные средства были переведены на расчетные счета других банковских карт (банковские счета), необходимо направить запрос в банк, где обслуживается заявитель, с целью получения информации о расчетном счете (счете б/карты) преступника.

6. При получении ответов от операторов сотовых компаний необходимо осуществить анализ данной информации и установить:

− место регистрации и местонахождение абонента во время перевода денежных средств, в этом случае, если:

− абонентский номер зарегистрирован не на обслуживаемой территории и абонент не находился там в момент совершения преступления, то материал проверки следует направить по территориальности;

− абонентский номер зарегистрирован на обслуживаемой территории, но в момент совершения преступления абонент находился не на обслуживаемой территории, то направить материал по территориальности в ОВД, руководствуясь географическим положением абонента в момент совершения преступления;

− абонентский номер зарегистрирован на обслуживаемой территории и в момент совершения преступления абонент находился на обслужи-

ваемой территории, то принять решение о возбуждении уголовного дела (далее – ВУД).

7. Установить наличие Управления Федеральной службы исполнения наказаний (далее – УФСИН) рядом с местом, указанным в географическом положении (далее – ГП) абонентского номера, с которого звонил преступник в момент совершения преступления;

− проанализировать детализацию с целью установления лица, совершившего преступление;

− установить номер счета (абонентский номер), на который были перечислены денежные средства, и установить дальнейшее движение денежных средств с этого номера (если деньги обналичивались, то установить место (банкомат, отделение связи, интернет ресурсы), где была совершена данная денежная операция, и осуществить направление необходимых запросов в организации, осуществляющие денежные переводы, для установления лица, осуществившего снятие денежных средств);

− при установлении исправительного учреждения организовать мероприятия при взаимодействии с сотрудниками УФСИН с целью установления изъятия SIM-карт, телефонных аппаратов с указанными идентификационными номерами.

Провести иные следственно-оперативные мероприятия направленные на раскрытие уголовного дела.

С целью своевременного получения необходимых сведений при сборе информации при расследовании хищений денежных средств с банковских счетов граждан, совершенных с использованием систем дистанционного банковского обслуживания, следует руководствоваться следующими рекомендациями:

− соблюдать общие правила делопроизводства (проставлять в запросе дату, исходящий номер, указывать обратный адрес для ответа, номер телефона конкретного исполнителя и т. п.);

− указывать основания истребования сведений: соответствующие статьи законодательства, номер материала проверки по КУСП (книге учета сообщений о проишествиях), номер уголовного дела и т. п.

− запрашивать сведения, которые возможно получить в рамках запроса в разумные сроки, не запрашивать сведений, в которых нет объективной необходимости, поскольку это увеличивает сроки исполнения запросов.

− соблюдать общую терминологию, формулировки.

Запросы операторам мобильной связи

При направлении запросов операторам мобильной связи необходимо помнить, что для абонентов сотовой связи возможно также запрашивать сведения:

− о движении денежных средств по лицевому счету абонентского номера, в том числе информацию, с какого банковского счета проходила оплата услуг связи;

− о IMEI-идентификаторах абонентских устройств сотовой связи, с которыми использовался данный абонентский номер;

− о номерах сотовой связи, использованных с определенными по IMEI идентификатору устройствами сотовой связи;

− о предоставлении копии договора об оказании услуг связи, месте заключения договора;

− о возможном обращении пользователя на «горячую линию» и сохранности фонограммы с записью разговора.

Бóльшая часть данных сведений (исключая копию договора об оказании услуг связи) может быть получена в рамках доследственной проверки.

Сведения о местоположении абонентского номера либо устройства сотовой связи согласно ст. 23 Конституции Российской Федерации и ст. 63 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» предоставляются оператором связи только на основании судебного решения. В этом случае в адрес оператора направляется заверенная копия соответствующего постановления.

Запросы официальным представителям социальных сетей

В сети Интернет действует значительное количество социальных сетей, как правило, в большинстве случаев используются самые распространенные: «ВКонтакте», «Одноклассники» и др. При запросе сведений у оператора социальной сети необходимо указывать в запросе идентификатор учетной записи либо ссылку на страницу интересующего пользователя[1].

Недопустимо указывать в запросах общее описание учетной записи (имя, фамилия, возраст, город и т. п.).

Операторы социальных сетей сохраняют у себя следующую информацию:

− сведения о регистрации учетной записи: указанные пользователем анкетные данные, дату и время регистрации, IP-адрес доступа к сети Интернет при регистрации, а также абонентский номер сотовой связи, использованный для подтверждения регистрации;

− сведения о доступе пользователя к своей учетной записи в виде зафиксированных даты и времени с соответствующим IP-адресом;

− сведения о платежных операциях, проведенных пользователем;

− электронную переписку пользователя, в случае, если она не была удалена владельцем.

Исключением является момент регистрации пользователя, сведения о котором хранятся постоянно.

---

[1] Бураева Л. А. Указ. соч. – С. 108–110.

Запросы операторам электронной почты

Операторы электронной почты сохраняют сведения о регистрации пользователей и сеансах последнего доступа за различный период времени. Также сохраняется содержимое электронной переписки, если пользователь не удалял свою корреспонденцию самостоятельно.

В основном возможно получить сведения от операторов связи, действующих на территории Российской Федерации (Mail.ru, Rambler.ru, Yandex.ru).

Запросы официальным представителям платежных систем, действующих на территории Российской Федерации

Операторы платежных систем сохраняют у себя следующую информацию:

– сведения о регистрации учетной записи: указанные пользователем анкетные данные, дату и время регистрации, IP-адрес доступа к сети Интернет при регистрации, как правило, также абонентский номер сотовой связи, использованный для подтверждения регистрации;

– сведения о доступе пользователя к своей учетной записи в виде зафиксированных моментов даты и времени с соответствующим IP-адресом. Сведения о доступе хранятся, как правило, за последние 2–3 месяца;

– сведения о платежных операциях, проведенных пользователем[1].

Ниже приведен алгоритм действий сотрудников следственных подразделений органов МВД России на стадии расследования уголовного дела, связанного с хищением, совершенным с использованием систем дистанционного банковского обслуживания.

Полагаем целесообразным в ходе проведения предварительного расследования по возбужденному уголовному делу в порядке, предусмотренном ст. 186.1 УПК РФ, истребовать информацию (если это не было сделано на стадии проверки сообщения о преступлении):

1) о входящих и исходящих соединениях абонента с телефонного номера, по которому звонили потерпевшему (детализацию вызовов), с целью установления лиц (организаций), с указанием данных о личности, адресов, на которых зарегистрирован указанный абонентский номер на день совершения преступления. Это связано с тем, что зачастую после совершения преступления владелец SIM-карты, с целью сокрытия следов преступления, производит замену абонентского номера, в результате чего первоначальный телефонный номер может быть оформлен на нового владельца, не имеющего никакого отношения к расследуемому уголовному делу;

[1] Новоселов Н. Г., Чиненов А. В. О некоторых вопросах раскрытия мошенничеств, совершаемых с использованием банковских карт // Вестник БелЮИ МВД России. – 2019. – № 3. – URL: https: //cyberleninka.ru/article/n/o-nekotoryh-voprosah-raskrytiya-moshennichestv-sovershaemyh-s-ispolzovaniem-bankovskih-art (дата обращения: 05.02.2022).

2) о базовой станции, в радиусе действия которой находился абонент, азимутах покрытия данных станций;

3) о номерах «IMEI» телефонов, в которых была активирована SIM-карта с вышеуказанным абонентским номером;

4) о поступлении денежных средств на счет абонентского номера (пополнение баланса, снятие денежные средств, перевод денежных средств другим абонентам);

5) о входящих и исходящих звонках с вышеуказанного абонентского номера с целью установления персональных данных абонентов, на телефонные номера которых поступали вызовы с телефона мошенника в день совершения преступления для установления их причастности (непричастности) к совершению преступления.

Анализ информации, полученной от операторов сотовой связи, позволит определить местонахождение абонента, осуществляющего звонок, выявить неизвестных следствию лиц, причастных к совершению преступления, потерпевших и свидетелей. С целью получения дополнительной информации о лицах, причастных к совершению преступления, следователю, руководствуясь положениями ст. 186 УПК РФ, необходимо вынести ходатайство о производстве контроля и записи их телефонных и иных переговоров.

Допрос потерпевшего

В отношении лица, пострадавшего от преступления в рамках производства следственных действий, необходимо признание его потерпевшим, допрос последнего с постановкой следующих вопросов: в какое время поступил звонок; с какого номера ему звонили; кем представился преступник, о чем он говорил, что предлагал сделать; какую сумму и за оказание каких услуг мошенник требовал к передаче;каким способом были переданы денежные средства (блиц-переводом, нарочным, помещением на счет определенного номера мобильного телефона и др.); звонил ли повторно потерпевший преступнику; сможет ли описать голос преступника и опознать его по голосу; если денежные средства передавались посреднику, попросить описать внешность данного лица, составить его субъективный портрет, выяснить, сможет ли потерпевший опознать данное лицо.

В случае если денежные средства были переведены блиц-переводом необходимо установить:

− когда и каким способом потерпевший сообщил свои персональные данные и код перевода, необходимые для получения отправленных денежных средств мошеннику. Произвести выемку документов о совершенном блиц-переводе у потерпевшего, осмотреть и приобщить их в качестве иных документов, определив место хранения последних;

− запросить в банке информацию о денежных переводах, полученных фигурантом уголовного дела; название и адрес филиала, где они были получены. При необходимости произвести выемку в отделении банка до-

кументов, на основании которых были получены денежные средства, а также изъятие видеозаписей с камер видеонаблюдения, установленных в отделениях банка, в случае снятия потерпевшим денежных средств со сберегательной книжки или в банкомате;

− в случае установления получателя денежных средств, собрать на него характеризующий материал, допросить данного гражданина об обстоятельствах получения им денежных переводов. В случае необходимости изъять образцы голоса и предъявить их для опознания потерпевшему, провести психофизиологическое исследование;

− установить родственников данного гражданина и круг его общения с целью получения информации о наличии среди них лиц, ранее судимых за аналогичные преступления, и лиц, отбывающих наказание в исправительных учреждениях; в случае положительного результата направить соответствующее поручение в оперативные подразделения, осуществляющие сопровождение по уголовному делу;

− направить поручение оперативным подразделениям с целью установления причастности подозреваемого к ранее совершенным аналогичным преступлениям и проведения в отношении указанного лица оперативных и технических мероприятий, направленных на изобличение лиц, совершивших данное преступление.

При получении результатов выемки у оператора сотовой связи необходимо провести анализ данной информации, в том числе путем составления схем, в которых наглядно будет отражен весь процесс перераспределения похищенных денежных средств, место нахождения абонентов с указанием базовых станций, и установить, не находится ли пенитенциарное учреждение недалеко от места, определенного географического положения абонентского номера, с которого звонил преступник в момент совершения преступления. В случае подтверждения данной информации, организовать взаимодействие с оперативным отделом данного исправительного учреждения с целью установления лиц, причастных к факту мошенничества. В случае установления искомых лиц, допросить последних об обстоятельствах совершенного преступления, о месте и времени регистрации SIM-карты (банковской карты), о факте получения денежных средств в соответствии и на основаниях, установленных УПК РФ.

Кроме того, после выемки информации (документов), полученных из сотовой компании, следователю необходимо допросить лицо, на которого была оформлена SIM-карта, посредством которой был произведен звонок потерпевшему. В случае если лицо, на которое оформлена SIM-карта, свидетельствует о своей непричастности к оформлению последней необходимо произвести выемку документов из компании сотовой связи и назначить почерковедческую экспертизу.

Если денежные средства были зачислены на счет банковской карты, абонентского номера или электронный кошелек (Webmoney, «Яндекс

Деньги» и др.), необходимо направить запрос в банк (платежную систему, оператору связи), на счет клиента которого потерпевший перечислил денежные средства, с целью установления: сведений о владельце банковской карты, счета (клиента электронной платежной системы, оператора связи); сведений о дальнейшем движении поступивших средств до момента обналичивания либо вывода их из системы; IP-адресов, даты и времени доступа пользователя к системе (для электронных платежных систем); географического местоположения, детализации с указанием информации об абонентах для перевода на счет абонентского номера.

Тактическими средствами разрешения задач, присущих первоначальному этапу расследования, служат следственные действия, призванные обнаружить, зафиксировать, изъять следы преступления и иную доказательственную информацию, а также объекты-носители данной информации, в отношении которых существует риск их утраты, исчезновения, уничтожения, фальсификации и т. п.

Допрос лиц, проходящих по уголовным делам о преступлениях названной категории, осуществляется в целом, в соответствии с рекомендациями, разработанными для этого следственного действия, с акцентированием внимания на всестороннем установлении обстоятельств, во-первых, образующих общий предмет доказывания согласно ст. 73 УПК РФ; во-вторых, определяющих специфику указанных деяний, проявляющихся в конструкции их состава[1].

С учетом проанализированных ранее факторов виктимности следователю необходимо строить тактику допроса потерпевших, выражая максимальную доброжелательность и вежливость к лицам, проявившим недостаточную правовую, финансовую или техническую компетентность, а равно подвергнувшимся психологическому воздействию злоумышленников. Тем более, что нередко потерпевшими от данных деяний, в особенности совершенных с помощью методов социальной инженерии (иными словами, совершенных лицами, специализирующимися на систематическом хищении денежных средств с помощью электронных средств платежа), выступают лица старших возрастных групп, которые в силу естественных психофизиологических процессов являются максимально уязвимыми.

По мере установления психологического контакта необходимо, побудив допрашиваемого к свободному рассказу, а также направляя его мысли путем постановки детализирующих и конкретизирующих вопросов, установить следующую совокупность обстоятельств:

1) обстоятельства, связанные с открытием банковского счета и оформлением в данной связи банковской карты (иного электронного сред-

[1] Маилян А. В. Криминалистические аспекты изучения хищений, совершенных с использованием электронных средств платежа // Вестник УЮИ. – 2020. – № 3 (89). – URL: https://cyberleninka.ru /article/n/kriminalisticheskie-aspekty-izucheniya-hischeniy-sovershennyh-s-ispolzovaniem-elektronnyh-sredstv-platezha (дата обращения: 28.01.2022).

ства платежа), а также с техническим обеспечением использования данного счета:

− дата, место, цель открытия банковского счета, наименование и подразделение банка, выдавшего карту, либо оформившего иное электронное средство платежа, условия и особенности банковского обслуживания;

− вид, номер, наименование банковского счета, а также соответствующей ему банковской карты (дебетовая, кредитная, карта рассрочки, накопительная, социальная); внешняя форма карты: пластиковая или виртуальная и т. д.; наименование электронного кошелька, иные реквизиты счета (карты);

− наименование оператора мобильной связи и номер мобильного телефона, привязанный к банковскому счету / банковской карте, электронному кошельку; на имя какого лица зарегистрирован данный контакт, в каких отношениях это лицо находится с потерпевшим;

− наименование, модель, марка и иные характеристики мобильного устройства (мобильного телефона, смартфона, планшетного устройства и т. д.), к которому подключена SIM-карта, привязанная к банковскому счету; наименование и криминалистически значимые характеристики иного электронного устройства, на которое установлено программное обеспечение для совершения финансовых операций в дистанционном формате;

− программное обеспечение для совершения финансовых операций, установленное на мобильном телефоне и / или ином электронном устройстве – кем и когда оно установлено; наименование и технические особенности данного программного обеспечения, значимые с точки зрения способов совершения и сокрытия преступлений и т. п.;

2) обстоятельства, связанные с текущим использованием банковского счета и соответствующей ему банковской карты (пластиковой, виртуальной), электронного кошелька, предшествующие совершению деяния:

− каким образом, с какой периодичностью, с применением каких электронных средств платежа использовались счет и / или карта потерпевшим;

− круг лиц, имеющих доступ, а также право и/или возможность систематически совершать операции по данной карте; на каких условиях, в каких пределах и / или лимите;

− имели ли место обстоятельства, в результате которых иные лица (помимо тех, кому потерпевший лично доверял использование своей карты/счета) могли получить возможность узнать реквизиты счета/карты, носящие конфиденциальный характер и т. п.;

− из каких источников сформировалась (поступила) сумма денежных средств, находившаяся на банковском счете потерпевшего, до момента незаконного доступа к банковскому счету и хищению;

3) обстоятельства, связанные с полной ли частичной утратой доступа к банковскому счету либо контроля за хранящимися на нем денежными средствами:

− где, когда, каким образом потерпевшему стало известно о неправомерном доступе иных лиц к его банковскому счету;

− действовали ли эти лица путем непосредственного вербального контакта либо с помощью средств связи; знакомы ли потерпевшему эти лица, если знакомы, то в каких отношениях находились;

− каково было последовательное содержание действий этих лиц и корреспондирующих им действий потерпевшего; какого характера персональную информацию субъекты преступления называли или сообщали в SMS, письме на электронную почту и т. д. (каким образом обращались к потерпевшему, какие данные относительно счета, карты, обслуживающего банка, а равно якобы попытки совершения несанкционированной финансовой операции иными лицами они указывали, какие меры предлагали осуществить потерпевшему);

− какими действиями и иными мерами потерпевший отреагировал (например, какие посетил сайты, скачал (из каких источников) или открыл электронные приложения, ссылки, мессенджеры и т. д.), какую именно персональную информацию и каким образом он сообщил злоумышленникам;

− что побудило допрашиваемого вступить с ними в вербальный контакт или электронную переписку, отнестись с доверием к сообщенной ими информации, выполнить определенные действия по их просьбе или требованию, а равно по собственной инициативе под воздействием навязанной ему легенды;

− каков итог взаимодействия потерпевшего с данными лицами;

− каковы приметы и иные характеризующие особенности этих лиц, а также использованные ими средства связи (контактные данные);

− какой вред причинен потерпевшему в результате совершения преступления, из каких слагаемых он состоит.

Как видно, в ходе допроса потерпевшего нередко излагается большой объем информации, касающийся:

− юридически значимых событий (оформления банковской карты, обслуживающей счет, имеющий те или иные реквизиты, оформления определенного телекоммуникационного контакта, имеющего особенности в обслуживании, приобретения средства связи, электронной техники, электронного приложения и т. д.);

− информации относительно определенных дат и присущих им событий;

− информации относительно сумм денежных средств: находящихся на счете, похищенных тем или иным образом и т. д.

Представляется, что в ходе допроса потерпевшего им сообщается большой объем знаковой информации (номер банковской карты и/или счета, сумма денежных средств, находившаяся до или после контакта, а равно иных действий злоумышленника, сумма несанкционированно списанных денежных средств и пр.). Очевидно, что запомнить всю подобную значимую информацию и воспроизвести ее хронологически и фактически безупречно для большинства лиц невозможно. В связи с этим на этапе, предшествующем допросу, потерпевшему необходимо разъяснить, что при допросе он может использовать банковские данные о наличии у него определенного банковского счета, обслуживаемого с помощью соответствующе карты и пр., в виде справок из банка, а также выписки из банковского счета за определенный временной период. Это прямо вытекает из ч. 3 ст. 189 УПК РФ, согласно которой допрашиваемые лица вправе пользоваться документами и записями.

С другой стороны, следователь не должен рассчитывать на сознательность потерпевших. Если допрашиваемый потерпевший не дает четких, развернутых, непротиворечивых показаний, путается в датах и/или событиях, следователю целесообразно предъявить данному лицу в качестве доказательства выписку (справку) из банковского счета, имеющуюся в материалах дела. По мере изложения потерпевшим того или итого эпизода следователь может предъявить соответствующий фрагмент выписки из движения денежных средств по счету (либо иной аналогичного содержания документ), предложив потерпевшему дать развернутый комментарий относительно события, значимого для установления обстоятельств деяния, отраженного в выписке.

Допрос свидетелей

Осуществляется с учетом разработанных в криминалистике рекомендаций по получению полных и правдивых показаний от этих лиц. В содержательном плане допрос свидетелей различается в зависимости от специфики обстоятельств, которые воспринимались непосредственно данным лицом, что требует рассмотреть наиболее типичные категории свидетелей по делам о данной категории преступлений:

− сотрудники финансовых организаций, организаций, оказывающих услуги связи, в период выполнения служебных обязанностей которыми подозреваемый или иное лицо совершали определенные юридически значимые действия: оформляли банковскую карту, кредит, счет (на свое имя либо имя других лиц), приобретали SIM-карту (восстанавливали якобы утерянную или поврежденную SIM-карту, карту с использованием паспортных данных других лиц и т. п.);

− сотрудники, обнаружившие в картоприемнике или ином узле банкоматов электронное оборудование по несанкционированному копированию (считыванию, перехвату) информации;

− сотрудники торговых или иных организаций, непосредственно воспринимавшие действия по распоряжению подозреваемым или обвиняемым чужими денежными средствами, находящимися на банковской карте потерпевшего;

− номинальные держатели банковской карты/SIM-карты (лица, на которых оформлена банковская карта по просьбе своих знакомых, знакомых своих знакомых и пр., передавшие карту в распоряжение другим лицам, не осведомленные о преступном умысле и истинных причинах использования карты);

− сотрудники правоохранительных органов, участвующие в задержании лиц, осуществлявших противоправные манипуляции с чужими банковскими картами/счетами;

− родственники или близкие лица потерпевшего, в том числе имеющие на законных основаниях доступ к банковской карте потерпевшего, либо у которых эта карта находилась в фактическом пользовании, а равно использующие на законных основаниях электронные инструменты, позволяющие совершать финансовые операции в дистанционном режиме;

− родственники или близкие лица потерпевшего, не имеющие доступа к банковской карте или иным источникам информации о банковском счете, но наблюдавшие те или иные обстоятельства деяния (например, момент посещения их места жительства злоумышленниками, факт и содержание телефонного разговора злоумышленника и потерпевшего и иные взаимосвязанные обстоятельства: момент обнаружения исчезновения банковской карты и/или мобильного телефона с номером, привязанным к банковской карте, момент поступления SMS-сообщения о списании денежных средств и пр.);

− родственники или близкие лица подозреваемого или обвиняемого, осведомленные об отдельных действиях этих лиц в связи с совершением преступления;

− иные лица.

По общему правилу, свидетелями считаются лица, не имеющие собственного интереса к результатам расследования, им не причинен вред в результате преступления, а потому их показания считаются наиболее объективными. Однако на практике это общее положение является весьма условным, в том числе применительно к расследуемой группе деяний.

Свидетели, являющиеся родственниками или близкими лицами подозреваемых (обвиняемых), нередко могут давать показания, свидетельствующие в пользу этих лиц, а обстоятельства, свидетельствующие против них, излагать в более нейтральной форме. Свидетели из числа сотрудников организаций, которые своими действиями неосознанно способствовали совершению преступления (например, по невнимательности, легкомыслию, нерадивости обслужили лицо, предъявившее чужие документы, удостоверяющие личность (либо их копии, а равно заполнившие необходимые дан-

ные со слов посетителя, продав ему SIM-карту или оформив банковскую карту, кредит и т. д.), могут давать неполные или нейтральные показания («не помню», «возможно» и т. п.), испытывая чувство стыда, опасаясь за свою деловую репутацию, а также перспектив привлечения их к ответственности и наказанию (хотя бы в рамках дисциплинарных отношений). Следовательно, общение с такими свидетелями требует, в рамках установления психологического контакта, убеждения их в даче правдивых показаний, бессмысленности запирательства, а также наиболее тщательного разъяснения последствий сообщения недостоверных (ложных) сведений.

На наш взгляд, представляет интерес допрос номинальных владельцев (держателей) банковских карт. Эти лица оформляют на свое имя банковские карты по просьбе или предложению (на определенных условиях, в том числе возмездного характера) других лиц, после чего предоставляют данные карты в пользование заинтересованным лицам. В зависимости от степени их осведомленности относительно дальнейшего использования карт они могут проходить по уголовным делам и в качестве подозреваемого (обвиняемого), например, если совершали действия по дальнейшему транзиту похищенных финансов либо знали, каким образом используется их банковская карта. В связи с чем допрос этих лиц должен быть весьма тщательным в плане выявления обстоятельств, указывающих на возможную (в том числе латентную) причастность этих лиц к организованной преступной деятельности.

Если показания лица о неосведомленности относительно намерений и действий заинтересованных лиц с картой представляются достоверными и подтверждаются объективно, то эти лица проходят по уголовным делам в качестве свидетелей. Допрос этих лиц позволяет, помимо установления реквизитов банковского счета / карты, обстоятельств оформления карты и передачи ее заинтересованным лицам, определить дальнейшие звенья в преступной цепочке – лиц, заинтересованных в приобретении чужих банковских карт.

Следственный осмотр

К числу следственных действий, в ходе которых можно выявить криминалистически значимую информацию, можно отнести и осмотры, объединяющие в себе группу следственных действий (осмотр места происшествия, местности, жилища, иного помещения, предметов и документов), сущностью которых выступает обследование окружающего пространства и находящихся в нем объектов в их взаимосвязи, осуществляемое следователем визуально (с помощью органов чувств и технико-криминалистических средств), а также с участием специалиста и иных лиц[1].

[1] Маилян А. В. Указ. соч. – С. 111.

В соответствии с ч. 1 ст. 178 УПК РФ целями осмотра (как собирательного понятия, объединяющего группу следственных действий) выступает: обнаружение следов преступления; выяснение других обстоятельств, имеющих значение для уголовного дела. Кроме того, ч. 2 ст. 178 УПК РФ допускает проведение осмотра места происшествия, документов и предметов до возбуждения уголовного дела.

С учетом изложенных уголовно-процессуальных условий и в соответствии с общими тактическими рекомендациями осуществляются различные виды осмотра по делам о хищениях, совершенных с использованием электронных средств платежа.

Наиболее распространенным видом осмотра применительно к расследованию указанных деяний выступает осмотр документов, прежде всего документов, подтверждающих наличие банковских счетов/банковских карт у определенного лица (потерпевшего, свидетелей (номинальных владельцев транзитных банковских счетов)), подозреваемых, обвиняемых, а также состояние данных счетов, характеризующих совершенные по ним финансовые операции.

Объектом осмотра документов являются:

– справки из банковских учреждений о наличии у определенного лица (потерпевшего, подозреваемого/обвиняемого, свидетеля – владельца счета, используемого в качестве транзитного, не осведомленного о преступном умысле лиц, фактически пользующихся счетом) банковских счетов с указанием реквизитов счетов, условий обслуживания счетов и т. д.;

– выписки из конкретного банковского счета о финансовых операциях за определенный период времени (отчетов о движении денежных средств по банковскому счету/карте);

– копии (скриншотов, распечаток) информации, отражающей действия с банковским счетом / картой, поступившей в виде SMS на мобильный телефон, сообщений на электронную почту, индивидуальную страничку пользователя в социальных сетях, на сайтах бесплатных объявлений, мессенджерах, push-уведомлений и т. д.

Таким образом, рассмотренные организации первоначального этапа расследования с учетом специфического предмета и средств преступного посягательства должны способствовать формированию доказательственной базы по уголовным делам о хищениях, совершенных с использованием банковских карт и их реквизитов.

ЗАКЛЮЧЕНИЕ

Безналичная система расчетов на основе использования кредитных и расчетных карт продолжает активно внедряться в кредитно-финансовую сферу нашей страны. Расширение спектра предоставляемых банками услуг с использованием электронных средств платежа неизбежно приводит к изменениям в структуре преступности, а причиненный этими преступлениями материальный ущерб в конечном итоге наносит существенный вред не только отдельным гражданам – держателям карт, но и урон экономике страны в целом.

Каждое раскрытое и расследованное хищение, совершенное с использованием банковских крат и их реквизитов, – это опровержение мнения о возможности безнаказанного обогащения посредством противозаконного использования банковских операций.

Однако расследование названных преступлений предполагает систему соответствующих методических рекомендаций, следование которым может гарантировать достижение успеха. Для этого необходимо иметь конкретное представление о способах совершения и сокрытия преступления, обстановки совершения и специфичности предмета хищения. При рассмотрении криминалистического значения информации о личности преступника при расследовании данного вида преступлений существенными являются сведения о характерных свойствах личности субъекта преступления, определение которых влияют на эффективность выбора дальнейших тактических приемов и выдвижения следственных версий. Кроме того, надлежит отметить, что качественные характеристики субъекта преступления могут отличаться в зависимости от способа совершения преступления, что может помочь сотрудникам правоохранительных органов сузить круг лиц, которые могут быть причастны к совершению преступления, в некоторых случаях выявить и преодолеть оказываемое субъектами преступления противодействие.

С учетом проанализированных материалов уголовных дел о преступлениях указанной категории и в последующем приостановленных производством из выделенных нами в данной работе типичных следственных ситуаций, встречающихся на первоначальном этапе расследования, отмечается серийное хищение денежных средств, совершенное с использованием электронных средств платежа с применением методов социальной инженерии, компьютерных технологий, иных способов целенаправленного воздействия на потерпевшего и/или принадлежащие ему электронные устройства. Имеются отдельные незначительные сведения в отношении лиц, причастных к совершению указанного посягательства, недостаточные для их индивидуализации.

Для всестороннего и объективного расследования преступлений данного вида в зависимости от сложившейся следственной ситуации

предлагается определенный набор следственных действий с преследованием конечной цели – привлечения виновного лица к уголовной ответственности и возмещению вреда, причиненного совершением преступления.

Рассмотренные особенности организации первоначального этапа расследования с учетом специфичности предмета и средств преступного посягательства помогут формированию доказательственной базы по уголовным делам рассматриваемой категории.

С целью решения выделенных проблем и повышения эффективности расследования хищений, совершенных с использованием банковских карт и их реквизитов, необходимо повысить уровень мониторинга данного вида преступлений; разработать программы повышения квалификации следователей (дознавателей) по расследованию данной категории дел; улучшить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий; увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования хищений, совершенных с использованием банковских карт и их реквизитов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Нормативные правовые акты и иные официальные документы

1. **Российская Федерация. Законы.** Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 5 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ, от 14 марта 2020 г. № 1-ФКЗ) // Официальный интернет-портал правовой информации. – URL: http// http//www.pravo.gov.ru (дата обращения: 04.02.2022). – Текст : электронный.

2. **Российская Федерация. Законы.** Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63–ФЗ // Официальный интернет-портал правовой информации. – URL: http// http//www.pravo.gov.ru (дата обращения: 03.02.2022). – Текст : электронный.

3. **Российская Федерация. Законы.** О национальной платежной системе : Федеральный закон от 27 июня 2011 г. № 161- ФЗ // Официальный интернет-портал правовой информации. – URL: http// http//www.pravo.gov.ru (дата обращения: 03.02.2022). – Текст : электронный.

4. **Российская Федерация. Законы.** О банках и банковской деятельности : Федеральный закон от 2 декабря 1990 г. № 395-1 // Официальный интернет-портал правовой информации. – URL: http// http//www.pravo.gov.ru (дата обращения: 01.02.2022). – Текст : электронный.

5. Об эмиссии платежных карт и об операциях, совершаемых с их использованием : Положение Банка России от 24 декабря 2004 г. № 266-П // Доступ из справ.-правовой системы «КонсультантПлюс». – URL: http//www.consultant.ru (дата обращения: 03.02.2022). – Текст : электронный.

II. Учебная, научная литература и иные материалы

1. **Вехов, В. Б.** Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов : монография / Б. В. Вехов; Министерство внутренних дел Российской Федерации. – Волгоград : Волгоградская академия МВД России, 2005. – 276 с. – ISBN 5-7899-0300-2. – Российская государственная библиотека. – URL: https://search.rsl.ru/ru/record/01002888885 (дата обращения: 03.02.2022). – Текст : электронный.

2. **Смагоринский, П. Б.** Криминалистическая характеристика хищений чужого имущества, совершенных с использованием пластиковых карт и ее применение в следственной практике : автореф. дис. … канд. юрид. наук

(12.00.09) / Смагоринский Павел Борисович; Волгоградский государственный универститет. – Волгоград, 2020. – 18 с. – Текст : непосредственный.

3. **Абдурагимова, Т. И.** Раскрытие и расследование изготовления, сбыта и использования поддельных кредитных и расчетных пластиковых карт : дис. … канд. юрид. наук : 12.00.09 : защищена 18.11.2001 : утв. 15.02.2002 / Абдурагимова Татьяна Иосифовна. – Москва, 2001. – 201 с. – Текст : непосредственный.

4. **Рубцов, И. И.** Криминалистическая характеристика преступлений как элемент частных методик расследования : дис. … канд. юрид. наук : 12.00.09 : защищена 28.09.2001 : утв. 15.02.2002 / Рубцов Илья Ильич. – Санкт-Петербург, 2001. – 225 с. – Текст : непосредственный.

5. **Дерябина-Чистякова, Е. Н.** Методика расследования мошенничества в сфере денежного обращения, кредита и банковской деятельности : дис. … канд. юрид. наук : 12.00.09 : защищена 25.10.2006 : утв. 24.01.2007 / Дерябина-Чистякова Елена Николаевна. – Москва, 2006. – 225 с. – Текст : непосредственный.

6. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.]. – Москва : Юрайт, 2021. – 243 с. – (Высшее образование). – ISBN 978-5-534-13898-6 // ЭБС Юрайт. – URL: https://urait.ru/bcode/467208 (дата обращения: 27.01.2022). – Текст : электронный.

III. Статьи из журналов

1. **Антонова, Е. Ю., Клименко, А. К.** Классификация хищений денежных средств с использованием средств связи // Российский следователь. – 2019. – № 1. – С. 38–41. – ISSN 1812-3783. – Текст : непосредственный.

2. **Вехов, В. Б.** О понятии, механизме образования и классификации электронноцифровых, оптических и магнитных следов // Криминалистика в системе правоприменения : материалы конференции, 27–28 октября 2008 г., Москва, МГУ им. М. В. Ломоносова. – Москва : МАКС Пресс, 2008. – С. 107–110. – Текст: непосредственный.

3. **Русанова, Д. Ю**. Цифровая криминалистика : возможности и перспективы развития / Д. Ю. Русанова // Intenational Journal of Humanities and Natural Sciences. – 2019. – № 124 (39) – С. 143. – ISSN 2500-1000. – Текст : непосредственный.

4. **Стельмах, В. Ю.** Современные проблемы фиксации хода и результатов производства следственных действий и возможные пути их решения / В. Ю. Стельмах // Актуальные проблемы российского права. – 2016. – № 7. – С. 152–159. – ISSN 19941471. – Текст : непосредственный.

5. **Филиппов, М. Н.** Методика расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов // Ведомо-

сти УИС. – 2015. – № 5 (156). – С. 26–30. – ISSN 2307-0382. – URL: https://cyberleninka.ru/article/n/metodika-rassledovaniya-krazh-i-moshennichestv-sovershennyh-s-ispolzovaniem-bankovskih-kart-i-ih-rekvizitov (дата обращения: 28.01.2022). – Текст : электронный.

6. **Бураева, Л. А.** К вопросу о классификации типичных следственных ситуаций по преступлениям, совершаемым с использованием банковских платежных карт / Л. А. Бураева // Проблемы экономики и юридической практики. – 2015. – № 1. – С. 108–110. – Текст : непосредственный.

7. **Новоселов, Н. Г., Чиненов, А. В**. О некоторых вопросах раскрытия мошенничеств, совершаемых с использованием банковских карт // Вестник БелЮИ МВД России. – 2019. – № 3. – ISSN 2313-5646. – URL: https://cyberleninka.ru/article/n/o-nekotoryh-voprosah-raskrytiya-moshennichestv-sovershaemyh-s-ispolzovaniem-bankovskih-kart (дата обращения: 29.01.2022). – Текст : электронный.

8. **Маилян, А. В.** Криминалистические аспекты изучения хищений, совершенных с использованием электронных средств платежа // Вестник УЮИ. – 2020. – № 3 (89). – ISSN 1729-9187. – URL: https://cyberleninka.ru/article/n/kriminalisticheskie-aspekty-izucheniya-hischeniy-sovershennyh-s-ispolzovaniem-elektronnyh-sredstv-platezha (дата обращения: 31.01.2022). – Текст : электронный.

IV. Эмпирические материалы

1. Приговор по уголовному делу № 1-111/2020 // Арх. Чугуевского районного суда (Приморский край). − URL: http://www.sudact.ru. (дата обращения: 01.02.2022). – Текст : электронный.

2. Приговор по уголовному делу № 1-89/2020 // Арх. Курчатовского суда (Курская область). − URL: http://www.sudact.ru. (дата обращения: 01.02.2022). – Текст : электронный.

3. Приговор по уголовному делу № 1-242/2019// Арх. Волжского районного суда (Самарская область). − URL: http://www.sudact.ru. (дата обращения: 29.01.2022). – Текст : электронный.

4. Приговор по уголовному делу № 1-269/2020 // Арх. Новочебоксарский городской суд (Чувашская Республика). − URL: http://www.sudact.ru. (дата обращения: 03.02.2022). – Текст : электронный.

5. Решение по уголовному делу № 2-216/2020 // Арх. Островского районного суда Костромская области. − URL: http://www.sudact.ru. (дата обращения: 30.01.2022). – Текст : электронный.

Учебное издание

Имаева Юлия Борисовна
(кандидат юридических наук, доцент)
Самойлов Александр Юрьевич
(кандидат юридических наук, доцент)
Афзалетдинова Гульнара Хасановна
(кандидат юридических наук)
и др.

ПЕРВОНАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ И ИХ РЕКВИЗИТОВ

Учебное пособие

Редактор Р. Р. Гафарова

Подписано в печать 15.03.2022	Выход в свет 28.03.2022
Гарнитура Times	Формат 60x84 1/16
Уч.изд. л. 2,8	Усл. печ. л. 3
Тираж 60 экз.	Заказ № 7

Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2

Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2