

АССОЦИАЦИЯ РОССИЙСКИХ БАНКОВ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ О ПОРЯДКЕ ДЕЙСТВИЙ В СЛУЧАЕ ВЫЯВЛЕНИЯ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ, ИСПОЛЬЗУЮЩИХ ЭЛЕКТРОННЫЕ УСТРОЙСТВА КЛИЕНТА

Настоящие рекомендации разработаны Рабочей группой Ассоциации российских банков и НП "Национальный платежный совет" по предотвращению мошенничества в платежных системах (далее - Рабочая группа) с учетом Письма Бюро специальных технических мероприятий Министерства внутренних дел Российской Федерации (далее - БСТМ МВД России) от 17 января 2012 г. N 10/257 с целью разъяснения порядка действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания <1> (далее - ДБО), использующих электронные устройства (далее - ЭУ): персональный компьютер, ноутбук, планшетный компьютер и т.п. в качестве удаленного рабочего места для целей дистанционного управления денежными средствами клиента.

<1> Под "системами дистанционного банковского обслуживания" для целей настоящих Рекомендаций понимаются системы "клиент-банк" и интернет-банкинг.

В целях оперативной организации эффективного взаимодействия и принятия процессуальных решений по фактам совершения хищения денежных средств в системах ДБО (далее - факт хищения денежных средств), а также исполнения требований [Положения](#) Банка России от 09.06.2012 N 382-П и [Указания](#) Банка России от 09.06.2012 N 2831-У, кредитным организациям и операторам платежных систем (далее совместно - банки) рекомендуется:

- соблюдать нижеизложенный порядок сбора и хранения необходимой доказательной базы по фактам хищений денежных средств;
- обеспечивать регистрацию и хранение информации, относящейся к работе клиентов в системах ДБО ([Приложение N 15](#) к настоящим Рекомендациям), не менее трех лет с момента последнего использования клиентом системы ДБО;
- соблюдать нижеизложенный порядок информирования и взаимодействия с правоохранительными органами;
- размещать и регулярно обновлять контактную информацию для оперативной связи с сотрудниками, ответственными за расследование фактов хищения денежных средств и противодействие мошенничеству в системах ДБО, на специальном закрытом разделе сайта Некоммерческого партнерства "Национальный платежный совет" (www.platsovetrf.ru);
- регулярно информировать своих клиентов о возможных рисках использования ДБО и рекомендованных мерах по их минимизации, которые должны осуществляться на постоянной основе;
- регулярно уведомлять клиентов о рекомендованном порядке действий в случае выявления хищения денежных средств.

1. Клиенту (пострадавшему) - юридическому лицу, индивидуальному предпринимателю или физическому лицу, занимающемуся в установленном законодательством порядке частной практикой необходимо:

1.1. В случае выявления хищения денежных средств в системе ДБО немедленно прекратить любые действия с ЭУ, подключенным к системе ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.) или перевести в режим гибернации ("спящий" режим).

При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и за протоколировать указанный факт.

1.2. При наличии технической возможности отозвать перевод с использованием иного ЭУ, после чего принять меры к блокировке системы ДБО.

1.3. При отсутствии технической возможности отозвать перевод по системе ДБО немедленно обратиться в банк плательщика по телефону с заявлением о блокировке системы ДБО, приостановке исполнения платежа и возврате средств.

1.4. Произвести фотосъемку ЭУ (с подключенными кабелями и иными периферийными устройствами), рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину. При необходимости ведения хозяйственной деятельности - задействовать другое ЭУ.

1.5. Дополнительно к [п. 1.2](#), [1.3](#) обратиться в банк плательщика с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе ДБО ([Приложение N 1](#) к настоящим Рекомендациям), а также о компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в банк плательщика незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в банк плательщика течение одного дня.

1.6. Проинформировать все банки, с которыми клиент имеет договорные отношения, предусматривающие использование ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

1.7. При наличии необходимой информации обратиться в банк получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении платежа и возврате денежных средств ([Приложение N 2](#) к настоящим Рекомендациям).

1.8. Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

1.9. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонент клиентского приложения системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, используемых для управления денежными средствами через систему ДБО банка, устройств, которые могут использоваться для удаленного управления указанными ЭУ.

1.10. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи ([Приложение N 3](#) к настоящим Рекомендациям) для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его локальной вычислительной сети (далее - ЛВС) как минимум за три месяца, предшествовавшие факту хищения денежных средств.

1.11. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.

1.12. Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенным к системе ДБО, предшествовавшие факту хищения денежных средств, подготовить объяснения клиента (работников клиента) об использовании ЭУ в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

1.13. Все действия, указанные в [пп. 1.1, 1.4, 1.8, 1.9, 1.12](#) настоящего раздела, производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъемки.

При невозможности осуществления коллегиальных действий (для индивидуальных предпринимателей или физических лиц, занимающихся частной практикой) отдельно зафиксировать данный факт.

1.14. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств ([глава 21](#) УК РФ) ([Приложение N 4](#) к настоящим Рекомендациям).

1.15. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами ([глава 60](#) ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона, содержащего порядковый номер из книги учета сообщений о преступлениях (далее - КУСП) содержащую отметку правоохранительного органа о его приеме.

1.16. Копии вышеуказанных документов по перечню, установленному банком плательщика, направить в банк плательщика с приложением Справки по факту инцидента информационной безопасности в системе ДБО ([Приложение N 5](#) к настоящим Рекомендациям), а также подтверждающих документов ([Приложение N 6](#) к настоящим Рекомендациям) <1>.

<1> Форму Справки и перечень подлежащих представлению в случае хищения денежных средств документов целесообразно закрепить в договоре между банком и клиентом.

2. Клиенту (пострадавшему) - физическому лицу необходимо:

2.1. В случае выявления хищения денежных средств в системе ДБО немедленно прекратить любые действия с ЭУ, подключенным к системе ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по USB, Wi-Fi и др.) или перевести в режим гибернации.

При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

2.2. Отозвать перевод денежных средств, обратившись в банк плательщика, следующими способами: при наличии технической возможности отозвать перевод - с использованием иного ЭУ, после чего заблокировать систему ДБО. При отсутствии технической возможности отозвать перевод по системе ДБО немедленно обратиться в банк плательщика по телефону с заявлением о приостановке исполнения платежа и возврате средств.

Оперативно обратиться в банк плательщика с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе ДБО ([Приложение N 1](#) к настоящим Рекомендациям), а также о компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в банк плательщика незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в банк плательщика как можно оперативнее.

2.3. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и опечатать горловину.

2.4. Проинформировать все банки, с которыми клиент имеет договорные отношения, предусматривающие использование ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

2.5. По возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру ([Приложение N 3](#) к настоящим Рекомендациям) для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его ЛВС как минимум за три месяца, предшествовавшие факту хищения денежных средств.

2.6. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.

2.7. Подготовить объяснения о значимых действиях и событиях, в том числе действия с ЭУ, подключенным к системе ДБО, предшествовавшим факту хищения денежных средств об использовании ЭУ в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

2.8. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств ([глава 21](#) УК РФ) ([Приложение N 4](#) к настоящим Рекомендациям).

2.9. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами ([глава 60](#) ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона КУСП, содержащую отметку правоохранительного органа о его приеме.

2.10. Копии документов по перечню, установленному банком плательщика, направить в банк плательщика с приложением Справки по факту инцидента информационной безопасности в системе ДБО ([приложение N 5](#) к настоящим Рекомендациям).

3. Банку плательщика необходимо:

3.1. При получении телефонного обращения плательщика о приостановке исполнения платежа немедленно предпринять разумно возможные и достаточные действия для идентификации плательщика, в том числе, посредством использования контактной информации, указанной в договоре банковского счета. При наличии возможности использовать дополнительные каналы для подтверждения обращения (SMS-уведомление, сообщение по электронной почте).

3.2. При подтверждении обращения незамедлительно принять меры к приостановке дальнейшей обработки платежа. При невозможности аутентификации клиента, зафиксировать данный факт, и продолжить обработку платежа, если нет иных оснований для приостановки дальнейшей обработки платежа.

3.3. В случае завершения обработки платежа незамедлительно в любой доступной форме направить в службу безопасности банка получателя информацию о факте хищения денежных средств с просьбой о приостановке обработки платежа.

3.4. Оперативно направить с использованием сервисов расчетной системы Банка России или по системе SWIFT в банк получателя сообщение с просьбой о приостановлении платежа и возврате средств ([Приложение N 7](#) к настоящим Рекомендациям).

3.5. С целью обеспечения сохранности доказательств исключить доставку в банк и/или техническое обслуживание ЭУ клиента, консультации, проверки ЭУ клиента, а равно совершение сотрудниками банка иных действий, которые могут привести к нарушению сохранности доказательств.

3.6. Оперативно направить письмо в банк получателя или к оператору платежной системы по факту хищения денежных средств ([Приложение N 8](#) к настоящим Рекомендациям) с просьбой о прекращении обработки платежа, блокировке ДБО и платежных карт клиента - получателя, применении к получателю платежа мер контроля в рамках системы ПОД/ФТ <1> и возврате средств.

<1> В соответствии с Федеральным [законом](#) от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма":

1) организации, осуществляющие операции с денежными средствами или иным имуществом, приостанавливают такие операции, за исключением операций по зачислению денежных средств, поступивших на счет физического лица, юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой, на два рабочих дня с даты, когда распоряжения клиентов об их осуществлении должны быть выполнены, и не позднее рабочего дня, следующего за днем приостановления операции, представляют информацию о них в уполномоченный орган в случае, если хотя бы одной из сторон является организация или физическое лицо, в отношении которых имеются полученные в установленном порядке сведения об их участии в террористической деятельности, либо юридическое лицо, прямо или косвенно находящееся в собственности или под контролем таких организации или лица, либо физическое или юридическое лицо (индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством порядке частной практикой), действующее от имени или по указанию таких организации или лица ([п. 10 ст. 7](#));

2) организации, осуществляющие операции с денежными средствами или иным имуществом, вправе отказать в выполнении распоряжения клиента о совершении операции, за исключением операций по зачислению денежных средств, поступивших на счет физического или юридического лица (индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой), по которой не представлены документы, необходимые для фиксирования информации в соответствии с положениями настоящего Федерального закона;

3) в случае, если у работников организации, осуществляющей операции с денежными средствами или иным имуществом, на основании реализации правил внутреннего контроля возникают подозрения, что какие-либо операции осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, эта организация не позднее трех рабочих дней, следующих за днем выявления таких операций, обязана направлять в уполномоченный орган сведения о таких операциях независимо от того, относятся или не относятся они к операциям, подлежащим обязательному контролю ([п. 3 ст. 7](#)).

Истребовать у плательщика подтверждение о подаче плательщиком заявления в правоохранительные органы и получить его копию в течение не более 2 рабочих дней со дня получения обращения плательщика в банк о факте хищения денежных средств.

3.7. Подготовить документы, указанные в [приложениях N 11](#) (в отношении юридического лица, индивидуального предпринимателя, физического лица, занимающегося в

установленном законодательством порядке частной практикой) и/или [N 12](#) (в отношении физического лица) к настоящим Рекомендациям.

3.8. Осуществить силами подразделения информационной безопасности банка, иных уполномоченных сотрудников либо с привлечением организаций, предоставляющих квалифицированные услуги по расследованию инцидентов информационной безопасности, по меньшей мере, следующие действия:

3.8.1. Провести мероприятия, определенные договорными отношениями с клиентом, в отношении проверки легитимности электронной подписи оспоренного платежного документа. При необходимости - провести мероприятия по факту компрометации ключей электронной подписи.

3.8.2. Получить от ответственных сотрудников банка, обслуживающих системы ДБО, администраторов сети, систем криптографической защиты и т.д. экспертные заключения в рамках их компетенции по корректности ЭП в составе платежного документа, ее целостности и авторства.

3.8.3. Провести анализ собранной информации с целью выявления источника осуществления хищения денежных средств и возможной причастности сотрудников банка. Результаты проверки оформить документально.

3.8.4. При необходимости - провести технические мероприятия, направленные на предотвращение сокрытия следов, уничтожения информации и т.д., для чего задействовать используемые в банке средства и методы защиты информации.

3.8.5. Обеспечить хранение собранной информации в неизменном виде для передачи правоохранительным органам по запросу.

3.9. При необходимости провести, документально зафиксировав полученные результаты, следующие проверочные мероприятия в целях формирования необходимой доказательной базы по факту хищения денежных средств:

3.9.1. Найти оспоренный Клиентом платежный документ в базе данных системы ДБО банка и в базе данных автоматизированной банковской системы (далее - АБС) банка.

3.9.2. Если платежный документ не найден в базе данных ДБО банка, но имеется в базе данных АБС банка:

3.9.2.1. По журналам систем ДБО и АБС установить присутствовал ли платежный документ в системе ДБО ранее.

3.9.2.2. В свойствах платежного документа установить его авторство, дату, время и способ его создания.

3.9.2.3. Получить объяснения от своих работников, уполномоченных на оформление и проверку платежных документов, администраторов ДБО и АБС банка, администраторов безопасности ДБО и АБС банка.

3.9.2.4. Провести сбор записей с межсетевых экранов, систем обнаружения вторжений и антивирусной защиты, серверов баз данных, систем авторизации пользователей (AD, NDS

и т.д.), рабочих станций сотрудников, штатно допущенных к управлению системами ДБО банка, и средств удаленного управления указанными рабочими станциями.

3.9.2.5. Получить записи систем видеонаблюдения, управления доступом в помещения и т.д.

3.9.2.6. Оценить возможность продолжения эксплуатации системы ДБО Банка.

3.9.3. Если платежный документ найден в базе данных ДБО банка, проверить подлинность оспариваемого платежного документа. <1>

<1> Подлинность платежного документа для целей настоящих Рекомендаций означает наличие у платежного документа всех необходимых реквизитов и атрибутов для возникновения обязанности банка плательщика принять платежный документ к исполнению.

3.9.3.1. Если подлинность платежного документа не установлена:

3.9.3.1.1. Получить объяснения от работников банка, уполномоченных на оформление и проверку платежных документов, поступивших по системе ДБО, администраторов ДБО и АБС банка, администраторов безопасности ДБО и АБС банка (другого уполномоченного лица).

3.9.3.1.2. По журналам систем ДБО установить, была ли подлинность платежного документа утрачена в процессе эксплуатации системы ДБО, а также оценить возможность продолжения эксплуатации системы ДБО банка.

3.9.3.2. Если подлинность платежного документа установлена:

3.9.3.2.1. Реализовать неотложные действия при компрометации закрытого ключа плательщика непосредственно после обращения клиента.

3.9.3.2.2. Получить от уполномоченного работника банка журналы работы системы ДБО и проанализировать их на предмет наличия записей, содержащих признаки несанкционированного доступа посторонних лиц.

3.9.3.2.3. Сохранить на съемном носителе журналы работы плательщика в системе ДБО.

3.9.3.2.4. Провести мероприятия, направленные на обеспечение целостности носителя.

3.9.4. Провести анализ информации с целью выявления возможной причастности к хищению денежных средств сотрудников банка. Результаты проверки оформить документально. При необходимости провести технические мероприятия, направленные на предотвращение сокрытия следов хищения.

3.10. Получить от плательщика Справку по факту инцидента информационной безопасности в системе ДБО ([Приложение N 5](#) к настоящим Рекомендациям).

3.11. На основании собранной информации оформить и передать в правоохранительный орган, осуществляющий расследование по факту хищения денежных средств, объяснение

по факту хищения денежных средств ([Приложение N 9](#) к настоящим Рекомендациям). В случае отказа клиента от обращения в правоохранительные органы оформить обращение по факту хищения денежных средств в региональное подразделение МВД от имени банка по форме, приведенной в [Приложении N 9](#) к настоящим Рекомендациям.

3.12. Обратиться в БСТМ МВД России либо его региональное отделение с заявлением об оказании содействия в расследовании факта хищения денежных средств с подробным описанием обстоятельств его совершения ([Приложение N 10](#) к настоящим Рекомендациям) и по запросу БСТМ МВД России направить документы, указанные в [приложениях N 11](#) (в отношении юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой) и/или [N 12](#) (в отношении физического лица) к настоящим Рекомендациям.

3.13. В случае хищения денежных средств плательщика, по счетам которого зафиксированы поступления средств бюджета любого уровня, также направить информационное письмо на имя руководителя ФСБ России о факте хищения денежных средств с подробным описанием обстоятельств его совершения ([Приложение N 13](#) к настоящим Рекомендациям) и по запросу ФСБ России направить документы, указанные в [Приложении N 9](#) (в отношении юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой) и/или [Приложении N 10](#) (в отношении физического лица) к настоящим Рекомендациям.

3.14. Направить в банк получателя полученную от плательщика копию заявления в правоохранительный орган по факту хищения денежных средств и номер КУСП (в случае обращения в правоохранительные органы).

3.15. При наличии в банке электронного документа с подлинной электронной подписью и при оспаривании подлинности электронной подписи в составе электронного документа, подтверждающего поручение плательщика банку выполнить оспоренный перевод, направить плательщику письмо о готовности участия в работе экспертной комиссии с целью проверки подлинности электронной подписи ([Приложение N 14](#) к настоящим Рекомендациям).

4. Банку получателя необходимо:

4.1. В рамках действующего законодательства Российской Федерации оказывать любое возможное содействие банку плательщика и плательщику в целях предотвращения хищения денежных средств, а при невозможности его предотвращения - в целях максимально оперативного расследования факта хищения денежных средств и возврата неосновательно полученных сумм, в том числе в части направления банку плательщика и плательщику имеющейся информации о получателе платежа на основании [статьи 19](#) Конституции Российской Федерации, [пункта 1.7 статьи 6](#) Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", [статей 6 и 131](#) ГПК РФ, а также [статьи 7](#) Федерального конституционного закона от 31.12.1996 N 1-ФКЗ "О судебной системе Российской Федерации" для предъявления иска к получателю о возврате неосновательного обогащения в соответствии с [главой 60](#) ГК РФ.

4.2. При получении обращения банка плательщика о приостановке исполнения платежа подтвердить достоверность и правомочность данного обращения.

4.3. На основании полученной от банка плательщика информации зачислить указанную в сообщении сумму на счет 47416 "Суммы, поступившие на корреспондентские счета до выяснения" и осуществить мероприятия в порядке, предусмотренном [Положением](#) Банка России "О Правилах ведения бухгалтерского учета в кредитных организациях, расположенных на территории Российской Федерации".

4.4. В случае, если похищенные денежные средства были сняты со счетов, открытых в банке получателя, необходимо подготовить технический носитель информации, содержащий записи видеокамер банкомата и других видеокамер, имеющих отношение к хищению денежных средств (до процессуального изъятия оригинала технического носителя информации следует обеспечить сохранность записи видеокамер банкомата и других видеокамер).

4.5. Подготовить и по запросу банка плательщика, правоохранительного органа, в который подано заявление по факту хищения денежных средств, БСТМ МВД России и/или ФСБ России направить в отношении получателя похищенных денежных средств документы, указанные в [Приложении N 11](#) (в отношении юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законом порядке частной практикой) и/или в [Приложении N 12](#) (в отношении физического лица) к настоящим Рекомендациям.

4.6. В случае, если похищенные денежные средства со счетов, открытых в банке получателя, были переведены на счет (счета) в ином банке (иных банках), банку получателя необходимо, в свою очередь, выполнить рекомендации, указанные в [Разделе 3](#) настоящих Рекомендаций, в том числе незамедлительно направить в этот банк (банки) информацию о факте хищения денежных средств и копии материалов, полученных от банка плательщика. В таком случае в своем обращении в БСТМ МВД России необходимо указать ссылку на первоначальное обращение банка плательщика.

4.7. Одновременно с мероприятиями по возврату похищенных средств необходимо провести полный анализ движений по всем счетам дроппера <1> (включая уже выявленный счет):

<1> Дроппер - (от англ. to drop - бросать) подставное физическое или юридическое лицо, используемое в мошеннических схемах обналичивания финансовых средств.

4.7.1. При наличии других поступлений денежных средств на счета дроппера необходимо повести проверку законности осуществленных переводов денежных средств, запросив соответствующую информацию у банков соответствующих плательщиков. В случае подтверждения незаконного характера переводов денежных средств необходимо провести совместно с банками выявленных пострадавших плательщиков мероприятия, предусмотренные [разделами 3 и 4](#) настоящих Рекомендаций.

4.7.2. При выявлении связей дроппера с другими дропперами необходимо провести проверку движений денежных средств по счетам этих дропперов и провести мероприятия по выявлению и блокированию их счетов, а также возврату похищенных денежных средств в соответствии с [разделами 3 и 4](#) настоящих Рекомендаций.