УТВЕРЖДЕНО

Советом директоров
Некоммерческого партнерства
«Национальный платежный совет»
(Протокол № 10 от 12 декабря 2012 года)

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. № 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.

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 № 382-П и Указания Банка России от 09.06.2012 № 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 № 15 к настоящим Рекомендациям), не менее трех лет с момента последнего использования клиентом системы ДБО;

[1] Под «системами дистанционного банковского обслуживания» для целей настоящих Рекомендаций понимаются системы «клиент-банк» и интернет-банкинг.

– 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.

– 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 запротоколировать 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 фотосъёмку 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 № 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 № 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 удалённого управления указанными ЭУ.

1.10. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи (Приложение № 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 фотосъёмки.

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 № 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 № 5 к

настоящим Рекомендациям), а также подтверждающих документов (Приложение № 6 к настоящим Рекомендациям)[2].

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 № 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] Форму Справки и перечень подлежащих представлению в случае хищения денежных средств документов целесообразно закрепить в договоре между банком и клиентом.

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 № 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, предшествовавших 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 № 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 № 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 № 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 № 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[3] и возврате средств.

[3] В соответствии с Федеральным законом от 07.08.2001 № 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

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 № 11 (в отношении юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой) и/или № 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, определённые договорными отношениями с клиентом, в отношении проверки легитимности электронной подписи оспоренного платёжного 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

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).

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 удалённого управления указанными рабочими станциями.

3.9.2.5. Получить записи систем видео-наблюдения, 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.[4]

3.9.3.1. Если подлинность платежного документа не установлена:

[4] **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.

3.9.3.1.1. 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 № 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 № 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 № 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 № 10 к настоящим Рекомендациям) и по запросу БСТМ МВД России направить документы, указанные в приложениях № 11 (в отношении юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой) и/или № 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 № 13 к настоящим Рекомендациям) и по запросу ФСБ России направить документы, указанные в Приложении № 9 (в отношении юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой) и/или Приложении № 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 № 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 №152-ФЗ «О персональных данных», статей 6 и 131 ГПК РФ, а также статьи 7 Федерального

конституционного закона от 31.12.1996 №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 № 11 (в отношении юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законом порядке частной практикой) и/или в Приложении № 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[5] (включая уже выявленный счет):

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 дропера с другими дроперами необходимо провести проверку движений денежных средств по счетам этих дроперов и провести мероприятия по выявлению и блокированию их счетов, а также возврату похищенных денежных средств в соответствии с разделами 3 и 4 настоящих Рекомендаций.

Приложения:

1. Форма заявления плательщика в банк плательщика об отзыве платежа, возврате денежных средств и блокировании доступа к системе ДБО.

2. Форма заявления плательщика в банк получателя или к оператору платежной системы о приостановлении платежа и возврате денежных средств.

3. Форма письма интернет провайдеру о предоставлении журналов соединений (логов).

4. Форма заявления плательщика (потерпевшего) в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.

5. Форма справки по факту инцидента информационной безопасности в системе ДБО.

6. Примерный перечень документов, которые могут быть истребованы у плательщика в случае выявления хищения денежных средств.

[5] Дроппер – (от англ. to drop – бросать) подставное физическое или юридическое лицо, используемое в мошеннических схемах обналичивания финансовых средств.

7. Форма сообщения в банк получателя по системе SWIFT о приостановлении платежа и возврате денежных средств.

8. Форма письма банка плательщика в банк получателя или к оператору платежной системы по факту хищения денежных средств.

9. Форма объяснения банка плательщика по факту хищения денежных средств.

10. Форма заявления банка плательщика в МВД России об оказании содействия в расследовании факта хищения денежных средств.

11. Перечень документов в отношении потерпевшего юридического лица (индивидуального предпринимателя, физического лица. занимающегося в установленном законодательством порядке частной практикой) и (или) юридического лица (индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой), на счет которого неправомерно зачислены денежные средства.

12. Перечень документов в отношении потерпевшего физического лица и (или) физического лица, на счет которого неправомерно зачислены денежные средства.

13. Образец информационного письма банка плательщика в ФСБ России о факте хищения денежных средств.

14. Форма письма о создании экспертной комиссии по проверке подлинности электронной подписи.

Приложение № 1
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА В БАНК ПЛАТЕЛЬЩИКА ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ ДБО

_____
должность руководителя

_____
наименование банка

_____
Фамилия И.О.

Уважаемый (ая) _____
имя, отчество руководителя

«___» _____ 201__ года с нашего банковского счета, открытого в Вашем банке, по системе дистанционного банковского обслуживания были похищены денежные средства, которые, по имеющейся информации были переведены со следующими реквизитами платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[6]

Прошу Вас заблокировать нашу учетную запись в системе ДБО, провести процедуру компрометации всех ключей ЭП и оказать содействие в возврате денежных средств.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

[6] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

Приложение № 2
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА В БАНК ПОЛУЧАТЕЛЯ ИЛИ К ОПЕРАТОРУ ПЛАТЕЖНОЙ СИСТЕМЫ О ПРИОСТАНОВЛЕНИИ ПЛАТЕЖА И ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ

_____
должность руководителя

_____
наименование организации

_____
Фамилия И.О.

Уважаемый (ая) _____
имя, отчество руководителя

«____» _____ 20___ года с нашего банковского счета были похищены денежные средства, которые, по информации, полученной из банка, были переведены со следующим реквизитам платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[7]

Прошу Вас оказать содействие в приостановлении прохождения платежа и возврате денежных средств.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

[7] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

Приложение № 3
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА ПИСЬМА ИНТЕРНЕТ ПРОВАЙДЕРУ О ПРЕДОСТАВЛЕНИИ ЖУРНАЛОВ СОЕДИНЕНИЙ (ЛОГОВ)

_____
должность руководителя

_____
наименование организации

_____
ФИО

от _____
должность, ФИО заявителя

проживающего: _____
адрес места жительства

паспорт: _____
номер паспорта, дата выдачи, кем и когда выдан

контактный телефон: _____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

Уважаемый (ая) _____
имя, отчество руководителя

«____» _____ 20___ года в ___:___ по московскому времени со счета _____ по системе дистанционного банковского обслуживания (ДБО) был осуществлен несанкционированный перевод денежных средств. Компьютер, с которого осуществляется подключение к системе ДБО, располагается по адресу _____ и использует IP-адрес ___.___.___.___.

Вероятной причиной несанкционированного перевода могло послужить заражение компьютера вредоносным программным обеспечением, кража логина, пароля и секретных ключей системы ДБО.

«____» _____ 20__ года между _____ и вами был заключен договор № _____ об оказании _____ услуг.

Для выявления обстоятельств несанкционированного перевода прошу предоставить информацию из журналов (логов) о входящем и исходящем трафике за период с «____» _____ 20___ года по «____» _____ 20___ года с указанием времени соединения, IP и MAC адресов.

_____	_____	_____
должность	подпись	расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 4
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА (ПОТЕРПЕВШЕГО) В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ О ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА ПО ФАКТУ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Начальнику ОВД по _____
наименование ОВД

от _____
должность, ФИО заявителя

проживающего: _____
адрес места жительства

паспорт: _____,
номер паспорта, дата выдачи, кем и когда выдан

место работы _____
наименование организации

контактный телефон: _____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

ЗАЯВЛЕНИЕ

Прошу провести проверку настоящего заявления по факту незаконного завладения принадлежащими _____»
наименование организации / ФИО потерпевшего

денежными средствами (кражи) с использованием системы дистанционного банковского обслуживания (далее – ДБО) «_____»
наименование банка

_____ 201__ г. неизвестными лицами по системе ДБО был осуществлен несанкционированный перевод денежных средств со следующими реквизитами:

Дата платежа: _____

Номер распоряжения: _____

Наименование банка плательщика: _____

Наименование плательщика: _____

ИНН плательщика: _____

Номер счета плательщика: _____

Наименование банка получателя: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____[8].

Оснований для данного денежного перевода нет: с получателем платежа отсутствуют договорные и иные деловые отношения, равно как и какие-либо обязательства перед ним; перевод расцениваю как хищение денежных средств.

Признаком хищения является то, что этот перевод не был осуществлен уполномоченными лицами.

Факт появления этого перевода был установлен «____» _____ 201__ г.

_____

ФИО лица, установившего факт несанкционированного перевода, должность, наименование организации

при _____.

обстоятельства обнаружения факта несанкционированного перевода

Электронное устройство, с которого осуществляется подключение к системе ДБО, располагается по адресу _____, доступ к электронному устройству ограничен, прямая кража реквизитов доступа (учетной записи, пароля и секретных ключей) маловероятна.

Вероятной причиной этого несанкционированного перевода считаю ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, поскольку данному событию сопутствовали следующие обстоятельства:

1. _____;
обстоятельства, снижающие вероятность прямого хищения реквизитов доступа в систему ДБО

2. _____.
наблюдавшиеся сбои, нехарактерное поведение системы ДБО и рабочего места системы ДБО

3. _____.
иное

На основании изложенного, прошу Вас провести необходимые оперативно-розыскные мероприятия для выявления виновных лиц и привлечь их к уголовной ответственности в соответствии с действующим законодательством.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__ г.

«___» _____ 20__г. _____ / /
подпись

[8] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

Приложение № 5
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА СПРАВКИ ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО

«___» _____ 20__ неустановленным лицом через систему ДБО была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[9]

Дополнительно сообщаю:

Количество ЭУ, настроенных для доступа в систему ДБО: _____.

Для доступа в системы ДБО хотя бы раз использовались

☐ корпоративные ЭУ
☐ личные ЭУ
☐ ЭУ, находящиеся в общественном пользовании

Периодичность смены пароля системы ДБО: _____

Применяемые элементы безопасности ЭУ включают:

☐ соблюден порядок подготовки ЭУ к установке системы ДБО
☐ используется только программное обеспечение для работы системы ДБО
☐ используется только лицензионное программное обеспечение
☐ операционная система и приложения обновляются в автоматическом режиме
☐ используется антивирусное программное обеспечение: _____
☐ антивирусное программное обеспечение обновляется ежедневно
☐ из числа съемных носителей информации на ЭУ используются только ключевые носители
☐ передача файлов и обмен сообщениями электронной почты на ЭУ ограничены
☐ целостность исполняемых файлов и файлов конфигураций контролируется с периодичностью _____

[9] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

☐ используются средства сетевой защиты: _____

☐ на ЭУ запрещены входящие соединения из сети Интернет

☐ с ЭУ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений программного обеспечения, число разрешенных сайтов составляет _____

☐ обеспечивается возможность доступа к ЭУ только уполномоченных лиц

☐ обеспечивается возможность доступа к ключевым носителям только уполномоченных лиц

Иная информация, имеющая отношение к инциденту: _____

_____

_____

_____ _____

подпись плательщика

☐ Я намерен обратиться в правоохранительные органы по факту хищения денежных средств.

Заявление в правоохранительные органы принято в ОВД _____

_____

район, округ, город, субъект федерации и иные идентифицирующие ОВД данные

и зарегистрировано за № _____ в КУСП

☐ Я не намерен обращаться в правоохранительные органы по факту хищения денежных средств.

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству, об ответственности за использование нелицензированного и контрафактного программного обеспечения в соответствии со статьей 146 УК Российской Федерации предупрежден.

Заявитель: _____/_____/

Дата: _____/**Телефон:** _____

Приложение № 6
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ДОКУМЕНТОВ, КОТОРЫЕ МОГУТ БЫТЬ ИСТРЕБОВАНЫ У ПЛАТЕЛЬЩИКА В СЛУЧАЕ ВЫЯВЛЕНИЯ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

1. Копия лицензии на операционную систему ПК.

2. Копия чека на приобретение операционной системы ПК

3. Описание используемого ПО (перечень использованного лицензионного ПО на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы)

4. Копия договора на оказание телематических услуг информационно–телекоммуникационной сети Интернет

5. Описание организации доступа в сеть Интернет на рабочем месте

6. Копия чека на оказание доступа в сеть Интернет на повременной основе

7. Копия заявления в правоохранительные органы

8. Копия лицензии на антивирусное ПО

9. Копия чека на антивирусное ПО

10. Описание по антивирусной защите рабочего места (наличие установленного на жестком диске автоматизированного рабочего места клиента антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на автоматизированном рабочем месте клиента вредоносных программ)

11. Описание системы защиты информации (наличие или отсутствие персонального межсетевого экрана у клиента, сведения об использовании рабочего места в иных целях, кроме осуществления платежно-расчетных операций, в частности – интернет-серфинга, сведения о порядке хранения и использования ключевых носителей).

Приложение № 7
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА СООБЩЕНИЯ В БАНК ПОЛУЧАТЕЛЯ ПО СИСТЕМЕ SWIFT О ПРИОСТАНОВЛЕНИИ ПЛАТЕЖА И ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ

(оформляется в виде сообщения свободного формата системы SWIFT (MT199) с соблюдением принятых в системе правил транслитерации.)

Поле «20» сообщения должно содержать подстроку «FRAUD»
Поле «79» сообщения должно содержать текст, аналогичный приведенному ниже:

UVAJAEMYE KOLLEGI, _____BANK PROSIT VAS OKAZATX SODEiSTVIE V BLOKIROVKE I VOZVRATE NESANKCIONIROVANNO SPISANNYH DENEJNYH SREDSTV NA OSNOVANII ZAYAVLENIa KLIENTA PO P/P __ OT _____ NA SUMMU _____ RUB. NAQ DEBET _____ PLATELXqIK _____ VAQ KREDIT _____ POLUcATELX _____. PROSIM VAS VERNUTX NESANKCIONIROVANNO SPISANNUu SUMMU PO SLEDUuqIM REKVIZITAM: _____ BANK BIK _____ K/ScET _____ R/ScET _____ POLUcATELX - _____ V SLUcAE NEVOZMOJNOSTI VOZVRATA INFORMIRUiTE NAS O PRIcINE OTKAZA S UKAZANIEM DANNYH POLUcATELa SWIFT SOOBqENIEM PISXMOM PO FAKSU _____ I PO BANKOVSKOi POcTE.
S UVAJENIEM, _____ TEL.(___) _____

Приложение № 8
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА ПИСЬМА БАНКА ПЛАТЕЛЬЩИКА В БАНК ПОЛУЧАТЕЛЯ ИЛИ К ОПЕРАТОРУ ПЛАТЕЖНОЙ СИСТЕМЫ ПО ФАКТУ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

_____
должность руководителя

_____
наименование организации

_____
Фамилия И.О.

Уважаемый (ая) _____!
имя, отчество руководителя

«____» _____ 20___ года с банковского счета нашего клиента, открытого в нашем банке, были переведены денежные средства на счет Вашего клиента со следующими реквизитами платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[10]

В связи с тем, что наш клиент заявил о хищении денежных средств, просим Вас приостановить прохождение платежа, блокировать систему ДБО и платежные карты Вашего клиента – получателя, применить к получателю платежа мер контроля в рамках системы ПОД/ФТ в связи с совершением операции, в отношении которой возникают подозрения в ее совершении в целях отмывания доходов, полученных преступным путем, или финансирования терроризма, зачислить указанную в сообщении сумму на счет 47416 «Суммы, поступившие на корреспондентские счета до выяснения» и осуществить мероприятия в порядке, предусмотренном пунктом 4.64 Положения от 26 марта 2007 г. № 302–П «О Правилах ведения бухгалтерского учета в кредитных организациях, расположенных на территории Российской Федерации».

Просим Вас также в соответствии с п.1.7 ст.6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» сообщить информацию о паспортных данных и

[10] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

месте нахождения получателя платежа, в целях исполнения статей 6 и 131 ГПК РФ, а также статьи 7 Федерального конституционного закона от 31.12.1996 №1-ФКЗ «О судебной системе Российской Федерации» и статьи 19 Конституции Российской Федерации, для предъявления ему судебного иска.

_____	_____	_____
должность	подпись	расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 9
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА ОБЪЯСНЕНИЯ БАНКА ПЛАТЕЛЬЩИКА ПО ФАКТУ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

ОБЪЯСНЕНИЕ

г. _____ «__» _____201__ г.
время ___ ч. ___ мин.

Оперуполномоченный _____
_____
получил объяснение от гр. _____
1. 1. Фамилия, имя, отчество _____
2. Год рождения _____
3. Место рождения _____
4. Образование _____
5. Национальность _____
6. Гражданство _____
7. Место работы, должность или род занятий _____
_____
8. Место жительства _____
9. Сведения о паспорте _____
_____

На русском языке разговариваю свободно. В услугах переводчика не нуждаюсь, ст. 51 Конституции РФ мне разъяснена и понятна. _____

По существу заданных мне вопросов могу показать следующее.

Я, _____ работаю в _____
ФИО наименование банка

(Банк) в должности _____.
должность

_____
наименование клиента

является Клиентом системы дистанционного банковского обслуживания (ДБО) нашего Банка. Реквизиты Клиента:

_____
ИНН; место нахождения/адрес регистрации и паспортные данные; почтовый адрес; контактные телефоны

_____

_____

_____

«___» _____ 20__ Клиент представил в Банк заявление, оспаривающее правомерность проведения Банком платежа со следующими реквизитами:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[11]

Указанный платеж проведен Банком на основании распоряжения, полученного Банком по системе ДБО. Клиент утверждает, что оснований для данного денежного перевода нет, поскольку с получателем платежа у него отсутствуют договорные и иные деловые отношения, равно как и какие-либо обязательства перед ним. Оспариваемый перевод Клиент расценивает как хищение принадлежащих ему денежных средств.

По факту оспоренного Клиентом перевода сообщаю следующее:

1. Оспоренное распоряжение получено по системе ДБО
2. Дата и время получения распоряжения: ___ч. ___ мин. «___» _____ 20__
3. Для получения доступа в систему ДБО использовались корректные реквизиты Клиента: _____
   перечислить: логин, пароль, одноразовый пароль с карты/СМС/брелока и т.п.
4. распоряжение содержит корректные электронные подписи (ЭП) Клиента в количестве _____ штук, определенном договором с Клиентом
5. ЭП Клиента являются действующими, оснований для отказа в исполнении ПП Банком не было
6. Используемый при совершении оспоренного платежа IP, MAC адреса _____
   IP и MAC адреса с указанием: использовались / не использовались Клиентом ранее
7. Аналогичные IP и MAC адреса при подключении других Клиентов _____
   зафиксированы / не зафиксированы
8. Использованные для подтверждения оспоренного Клиентом платежа пароли и криптографические ключи вырабатывались _____
   Клиентом / Банком
9. Сотрудники Банка доступ к электронным устройствам, к которых осуществлялась работа Клиента с системой ДБО _____
   имели / не имели

Иные существенные обстоятельства инцидента:

_____

_____

[11] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

На основании изложенного считаю, что создание оспоренного платежа сотрудниками Банка _____
возможно / маловероятно / невозможно

Объяснение получил: о\у _____

Приложение № 10
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА ЗАЯВЛЕНИЯ БАНКА ПЛАТЕЛЬЩИКА В МВД РОССИИ ОБ ОКАЗАНИИ СОДЕЙСТВИЯ В РАССЛЕДОВАНИИ ФАКТА ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Начальнику
Бюро специальных технических
мероприятий МВД России
генерал-майору полиции
А.Н. Мошкову

119049, Москва, ул. Житная, д. 16

О предоставлении информации

Уважаемый Алексей Николаевич!

«____» _____ 20___ года с банковского счета нашего клиента, открытого в нашем банке, были переведены денежные средства со следующими реквизитами платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[12]

Клиент обратился в Банк с заявлением о хищении денежных средств.

Инцидент произошел в результате получения доступа к счетам Клиента с использованием электронной системы дистанционного банковского обслуживания.

[12] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

Клиент обратился в ОВД _____
район, округ, город, субъект федерации и иные идентифицирующие ОВД данные

по месту регистрации. Заявление зарегистрировано за № _____ в КУСП.

Указанные противоправные действия совершены с использованием информационных технологий. Проблема хищения денежных средств со счетов клиентов банка посредством информационных технологий касается не только защиты законных интересов отдельных клиентов, но и затрагивает безопасность государства в кредитно-финансовой сфере, выявляет слабые звенья в противодействии посягательствам на общественные отношения, охраняемые законом, в частности, отношения в сфере компьютерной информации, что может привести к дестабилизации национальной платежной системы Российской Федерации.

Просим Вас оказать содействие в розыске и привлечении к ответственности лиц, совершивших незаконные действия в отношении Клиента нашего Банка.

Для сведения и оперативного взаимодействия Банк готов направить имеющиеся материалы по инциденту в соответствии с Вашим письмом от 17 января 2012 г. № 10/257.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 11

к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ПЕРЕЧЕНЬ ДОКУМЕНТОВ В ОТНОШЕНИИ ПОТЕРПЕВШЕГО ЮРИДИЧЕСКОГО ЛИЦА (ИНДИВИДУАЛЬНОГО ПРЕДПРИНИМАТЕЛЯ, ФИЗИЧЕСКОГО ЛИЦА, ЗАНИМАЮЩЕГОСЯ В УСТАНОВЛЕННОМ ЗАКОНОДАТЕЛЬСТВОМ ПОРЯДКЕ ЧАСТНОЙ ПРАКТИКОЙ) И (ИЛИ) ЮРИДИЧЕСКОГО ЛИЦА (ИНДИВИДУАЛЬНОГО ПРЕДПРИНИМАТЕЛЯ, ФИЗИЧЕСКОГО ЛИЦА, ЗАНИМАЮЩЕГОСЯ В УСТАНОВЛЕННОМ ЗАКОНОДАТЕЛЬСТВОМ ПОРЯДКЕ ЧАСТНОЙ ПРАКТИКОЙ), НА СЧЕТ КОТОРОГО НЕПРАВОМЕРНО ЗАЧИСЛЕНЫ ДЕНЕЖНЫЕ СРЕДСТВА

1. Договоры на открытие и обслуживание банковских счетов, договоры о предоставлении услуг ДБО.

2. Сведения о точном месте открытия и месте нахождения счета юридического лица, индивидуального предпринимателя, физического лица, занимающегося в установленном законодательством порядке частной практикой.

3. Заверенную копию банковской карточки с образцами подписей и оттиска печати.

4. Расширенную выписку по банковским счетам с отражением сведений о движении денежных средств в период осуществления несанкционированного перевода.

5. Заверенные копии платежных документов, на основании которых были несанкционированно переведены денежные средства.

6. Технический носитель информации, содержащий записи видеокамер, имеющие отношение к хищению (до процессуального изъятия оригинала технического носителя информации следует обеспечить сохранность записей).

7. Документы, отражающие статистику соединений с системой ДБО Банка, с указанием учетных записей, внешних IP-адресов клиента и точного времени соединений в период осуществления несанкционированного перевода.

8. Сведения о лицах, имеющих право первой и второй подписи, в том числе электронной подписи либо иного аналога собственноручной подписи.

9. Сведения о подключенных уведомительных услугах банка (СМС-уведомление, голосовая авторизация, уведомление на электронную почту, привязка к выделенному IP-адресу и другие имеющиеся услуги) с приложением копий документов, акцептованных банком при предоставлении указанных услуг.

10. Материалы, подготовленные службой безопасности банка по итогам проведения внутренних проверок.

Приложение № 12
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ПЕРЕЧЕНЬ ДОКУМЕНТОВ В ОТНОШЕНИИ ПОТЕРПЕВШЕГО ФИЗИЧЕСКОГО ЛИЦА И (ИЛИ) ФИЗИЧЕСКОГО ЛИЦА, НА СЧЕТ КОТОРОГО НЕПРАВОМЕРНО ЗАЧИСЛЕНЫ ДЕНЕЖНЫЕ СРЕДСТВА

1. Договоры на открытие и обслуживание банковских счетов, договоры о предоставлении услуг ДБО.

2. Сведения о точном месте открытия и месте нахождения счета физического лица.

3. Сведения о паспортных данных физического лица (в том числе копия паспорта и иного удостоверения личности – при наличии).

4. Технический носитель информации, содержащий записи видеокамер, имеющие отношение к хищению (до процессуального изъятия оригинала технического носителя информации следует обеспечить сохранность записей).

5. Документы, отражающие статистику соединений с системой электронных расчетов банка посредством ДБО «клиент-банк», с указанием учетных записей, внешних IP-адресов клиента и точного времени соединений в период осуществления несанкционированного перевода.

6. Журналы авторизации по электронным средствам платежа в банкоматах, данные о телефонах и адресах электронной почты, на которые было настроено оповещение об инцидентах, номера телефонов и адреса электронной почты, с которых поступали сообщения мошенников (при наличии), данные, указанные на подложных сайтах (при наличии).

7. Сведения о подключенных уведомительных услугах банка (СМС-уведомление, голосовая авторизация, уведомление на электронную почту, привязка к выделенному IP-адресу и других имеющихся услугах) с приложением копий документов, акцептованных банком при предоставлении указанных услуг.

8. Материалы, подготовленные службой безопасности банка по итогам проведения внутренних проверок.

Приложение № 13
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ОБРАЗЕЦ ИНФОРМАЦИОННОГО ПИСЬМА БАНКА ПЛАТЕЛЬЩИКА В ФСБ РОССИИ О ФАКТЕ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Директору Федеральной службы
безопасности России,
Генералу армии
А.В. Бортникову

107031, ул.Большая Лубянка, дом 1/3

О факте хищения денежных средств

Уважаемый Алексей Васильевич!

«_____» (*наименование банка*) настоящим письмом информирует о противоправных действиях по отношению к Клиенту нашего Банка с использованием компьютерных технологий, в результате которых произошло хищение денежных средств.

«____» _____ 20___ года с банковского счета нашего Клиента, открытого в нашем Банке, были переведены денежные средства со следующими реквизитами платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[13]

[13] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

Согласно имеющейся информации, на счету клиента находились/могли находиться бюджетные средства.

Клиент обратился в ОВД _____
район, округ, город, субъект федерации и иные идентифицирующие ОВД данные

по месту регистрации. Заявление зарегистрировано за № ___ в КУСП).

Хищение денежных средств со счета клиента банка посредством компьютерных технологий касается не только защиты законных интересов отдельного клиента, но и затрагивает безопасность государства в кредитно-финансовой и бюджетной сфере, выявляет слабые звенья в противодействии посягательствам на совершение преступления в сфере охраняемой законом компьютерной информации, что может привести к дестабилизации как бюджетной, так и национальной платежной системы Российской Федерации.

Для сведения и оперативного взаимодействия Банк готов направить имеющиеся материалы по инциденту.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 14
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ФОРМА ПИСЬМА О СОЗДАНИИ ЭКСПЕРТНОЙ КОМИССИИ ПО ПРОВЕРКЕ ПОДЛИННОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ

_____
должность руководителя

_____
наименование организации

_____
Фамилия И.О.

Уважаемый (ая) _____
имя, отчество руководителя

В связи с оспариванием Вами перевода денежных средств, совершенного Банком на основании электронного документа, полученного по системе ДБО, имеющего следующие реквизиты:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

согласно заключенному с Банком договором с целью установления подлинности электронной подписи в электронном документе, на основании которого Банком произведена оспариваемая Вами операция, Банк уполномочивает для участия в работе экспертной комиссии своего представителя: _____
должность представителя

_____
ФИО, контактные данные представителя

Экспертная комиссия будет созвана по Вашему письменному запросу. Работа экспертной комиссии по установлению подлинности электронной подписи согласно договору будет осуществляться по адресу: _____.
адрес места работы экспертной комиссии

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 15
к Методическим рекомендациям
о порядке действий в случае выявления хищения
денежных средств в системах дистанционного банковского
обслуживания, использующих электронные устройства клиента

ПЕРЕЧЕНЬ ИНФОРМАЦИИ О ДЕЙСТВИЯХ КЛИЕНТА В СИСТЕМАХ ДБО, ПОДЛЕЖАЩЕЙ РЕГИСТРАЦИИ И ХРАНЕНИЮ

Обязательные пункты, согласно 382-П:

1. Дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента;

2. идентификатор (идентификаторы) клиента;

3. идентификатор (код) осуществляемого действия клиента;

4. идентификатор устройства клиента, с использованием которого клиент осуществляет доступ к программному обеспечению и автоматизированным системам с целью осуществления переводов денежных средств и которым при наличии технической возможности могут являться IP-адрес, MAC-адрес, номер sim-карты, номер телефона и (или) иные идентификаторы.

Необязательные пункты:

1. Используемый клиентом браузер

2. Используемая клиентом операционная система

3. Запрашиваемый URL

4. Адрес страницы, с которой зашёл клиент

5. Географическое положение клиента

6. Технический заголовок HTTP

Оператор по переводу денежных средств обеспечивает регистрацию и хранение в течение трех лет следующих сведений о действиях клиентов, выполняемых с использованием программного обеспечения и автоматизированных систем