МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

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

1. Банку плательщика необходимо:

1.1. При получении телефонного обращения плательщика о приостановке исполнения платежа немедленно подтвердить обращение плательщика обратным звонком по номеру, указанному в предоставленных плательщиком документах на бумажном носителе. При наличии возможности использовать дополнительные каналы для подтверждения обращения (SMS-уведомление, сообщение по электронной почте).

1.2. При подтверждении обращения незамедлительно принять меры к приостановке дальнейшей обработки платежа.

1.3. 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 и возврате средств, используя данные, указанные в закрытом разделе сайта Национального платежного совета (www.platsovetrf.ru).

1.4. 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 № 1 к настоящим Рекомендациям).

1.5. 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.

1.6. Оперативно направить письмо в банк получателя или к оператору платежной системы по факту хищения денежных средств (Приложение № 2 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 № 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,

а также 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.

1.7. Подготовить документы, указанные в приложениях № 5 (в отношении юридического лица) и/или № 6 (в отношении физического лица) к настоящим Рекомендациям.

1.8. 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:

1.8.1. 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.

1.8.2. 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.

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

поступивших на счет физического или юридического лица, **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, 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, 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).

1.8.4. 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.

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

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

1.9.1. Найти оспоренный Клиентом платежный документ в базе данных системы ДБО банка и в базе данных АБС банка.

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

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

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

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

1.9.2.4. 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.

1.9.2.5. Получить записи систем видео-наблюдения, управления доступом в помещения и т.д.

1.9.2.6. Оценить возможность продолжения эксплуатации системы ДБО Банка.

1.9.3. Если платежный документ найден в базе данных ДБО банка, проверить подлинность оспариваемого платежного документа.[2]

1.9.3.1. Если подлинность платежного документа не установлена:

[2] **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.

1.9.3.1.1. 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).

1.9.3.1.2. 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.

1.9.3.2. Если подлинность электронного документа установлена:

1.9.3.2.1. Реализовать неотложные действия при компрометации закрытого ключа плательщика в соответствии с внутренним порядком банка.

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

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

1.9.3.2.4. Провести мероприятия, направленные на обеспечение целостности носителя.

1.9.4. 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.

1.10. Получить от плательщика Справку по факту инцидента информационной безопасности в системе ДБО (Приложение № 9 к настоящим Рекомендациям).

1.11. На основании собранной информации оформить и передать в правоохранительный орган, осуществляющий расследование по факту хищения денежных средств, объяснение по факту хищения денежных средств (Приложение № 3 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 № 3 к настоящим Рекомендациям.

1.12. 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 № 4 к настоящим Рекомендациям) и по запросу БСТМ МВД России направить документы, указанные в приложениях № 5 (в отношении юридического лица) и/или № 6 (в отношении физического лица) к настоящим Рекомендациям.

1.13. 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 № 7 к настоящим Рекомендациям) и по запросу ФСБ России направить документы, указанные в Приложении № 3 (в отношении юридического лица) и/или Приложении № 4 (в отношении физического лица) к настоящим Рекомендациям.

1.14. Направить в банк получателя полученную от плательщика копию заявления в правоохранительный орган по факту хищения денежных средств и номер КУСП.

1.15. 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 № 8 к настоящим Рекомендациям).

2. Банку получателя необходимо:

2.1. 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.

2.2. 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».

2.3. Получив информацию о поступлении несанкционированного платежа произвести сбор (обновление) информации о своем клиенте – получателе денежных средств (предполагаемом дроппере[3]).

2.4. Связаться с получателем по телефону и назначить ему встречу в офисе банка. Если связаться с получателем по указанным им реквизитам невозможно, осуществляется поиск получателя (выезд по его месту жительства и/или месту работы). При встрече с получателем у него необходимо выяснить, открывал ли он счет, должны ли ему поступить денежные средства.

2.5. Если получатель утверждает, что он не ожидает поступления денежных средств от плательщика, оспаривающего платеж, следует предложить ему осуществить возврат денег плательщику и при необходимости закрыть счет.

Если получатель утверждает, что он потерял, передал или продал электронное средство платежа, следует предложить получателю проехать в банк, осуществить возврат денег плательщику и закрыть счет.

Если получатель утверждает, что поступившие денежные средства предназначены ему, что у него есть договорные отношения с плательщиком, то следует получить от получателя подтверждение наличия таких отношений (договор и иные доказательства). Такие подтверждения должны быть проверены на подлинность (в том числе соответствие подписей с карточкой образцов плательщика, для чего необходимо запросить ее у банка плательщика).

Всю полученную информацию и копии документов необходимо передать в правоохранительный орган по месту регистрации банка плательщика с указанием данных о принятии заявления о возбуждении уголовного дела.

2.6. Если получатель настаивает на получении наличных денежных средств, необходимо предложить ему прийти в конкретный офис банка в установленное время, предварительно уведомив об этом местное отделение полиции, в присутствии сотрудников полиции проверить подлинность предъявленного получателем документа,

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

удостоверяющего личность, и получить объяснения по факту хищения денежных средств.

2.7. 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).

2.8. 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 № 5 (в отношении юридического лица) и/или в Приложении № 6 (в отношении физического лица) к настоящим Рекомендациям.

2.9. 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.

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

2.10.1. 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.

2.10.2. 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.

Приложение № 1
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 № 2
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 расчетного счета нашего клиента, открытого в нашем банке, были переведены денежные средства на счет Вашего клиента со следующими реквизитами платежа:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[4]

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

[4] 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 № 3
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 платежного поручения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[5]

Указанный платеж проведен Банком на основании платежного поручения, 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 платежное поручение (ПП) получено по системе ДБО
2. Дата и время получения ПП: ___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. ПП 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:

_____

_____

[5] 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 № 4
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 расчетного счета нашего клиента, открытого в нашем банке, были переведены денежные средства со следующими реквизитами платежа:

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

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.

[6] 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 банковской 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 № 5

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 И (ИЛИ) ЮРИДИЧЕСКОГО 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 юридического лица.

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 № 6
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 № 7
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 расчетного счета нашего Клиента, открытого в нашем Банке, были переведены денежные средства со следующими реквизитами платежа:

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

[7] 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 банковской 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 № 8
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 платежного поручения: _____
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__

Приложение № 9
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 платежного поручения: _____
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]

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 _____

[8] 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: _____

_____

_____

Подтверждаю отсутствие у меня претензий к _____
наименование банка плательщика

_____ _____
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:** _____