МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

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

1. **Клиенту (пострадавшему) – юридическому лицу 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 аккумуляторную батарею из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi и др.) или перевести в режим гибернации.

1.2. При наличии технической возможности отозвать перевод с использованием иного ЭУ, после чего заблокировать систему ДБО.

1.3. 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.

1.4. Произвести фотосъёмку 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 опечатать горловину. При необходимости ведения хозяйственной деятельности – задействовать другое ЭУ.

1.5. 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. В течение одного дня 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 видео-наблюдения, 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, серверов баз данных и иных компонент клиентского приложения системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), ЭУ, используемых для управления денежными средствами через систему ДБО банка, устройств, которые могут использоваться для удалённого управления указанными ЭУ.

1.10. В течение одного дня 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.

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 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.

1.14. В течение одного дня обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (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 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)[1].

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 аккумуляторную батарею 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.

2.2. При наличии технической возможности отозвать перевод с использованием иного ЭУ, после чего заблокировать систему ДБО.

2.3. 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.

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

2.4. 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.

2.5. 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.

2.6. 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.

2.7. В течение одного дня 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.

2.8. 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.

2.9. 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.

2.10. В течение одного дня обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (Приложение № 4 к настоящим Рекомендациям).

2.11. 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.

2.12. 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).

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 расчетного 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 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: _____[2]

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. _____

[2] 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 расчетного счета были похищены денежные средства, которые, по информации, полученной из банка, были переведены со следующим реквизитам 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: _____[3]

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

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

[3] 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 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].

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

[4] 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 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: _____[5]

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 _____

[5] 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:** _____

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).