Приложение № 4
к Регламенту работы с обращениями
клиентов банка по фактам нарушения
обеспечения защиты информации при
осуществлении переводов денежных
средств в системах ДБО

Рекомендации клиенту (пострадавшему) в случае выявления хищения денежных средств в системе ДБО Банка

1. Клиенту (пострадавшему) - юридическому лицу, индивидуальному предпринимателю или физическому лицу, необходимо:

1.1. В случае выявления хищения денежных средств в системе ДБО, зафиксировать данные расчетных документов, по которым совершено хищение, немедленно прекратить любые действия с электронными устройствами: персональными компьютерами, ноутбуками, планшетными компьютерами и т.п., используемыми в качестве удаленного рабочего места для целей дистанционного управления денежными средствами клиента (далее – ЭУ), подключенным к системе дистанционного банковского обслуживания (далее – 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).

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

1.3. При наличии технической возможности отозвать перевод с использованием иного ЭУ (отправить сообщение свободного формата по системе «Интернет-банк», «Частный – клиент» с указанием номера, даты, суммы расчетного документа), после чего принять меры к блокировке системы ДБО.

1.4. При отсутствии технической возможности отозвать перевод по системе ДБО, немедленно обратиться в Банк по телефону подразделения, обслуживающего счет клиента или по телефону операционного управления Банка (812)-329-55-46 с заявлением о блокировке системы ДБО, приостановке исполнения платежа и возврате денежных средств.

1.5. Оперативно обратиться в Банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе ДБО (форма заявления на стр.3 настоящих Рекомендаций), а также о компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в Банк незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в Банк как можно оперативнее.

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. Произвести фотосъемку ЭУ (с подключенными кабелями и иными переферийными 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.д.) 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.

1.8. 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 средств.

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

1.10. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его локальной вычислительной сети как минимум за три месяца, предшествовавшие факту хищения денежных средств (Рекомендуемая форма заявления на стр. 6 настоящих Рекомендаций).

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, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

1.13. Все действия, указанные в п. 1.1., 1.7., 1.8., 1.9., 1.12. настоящего раздела, производить коллегиально, прокотолировать и документировать, в т ч с использованием фотосъемки. При невозможности осуществления коллегиальных действий (для индивидуальных предпринимателей или физических лиц, занимающихся частной практикой) отдельно зафиксировать данный факт.

1.14. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении дела по факту хищения денежных средств (глава 21 УК РФ) (форма заявления на стр.7-8 настоящих Рекомендаций).

1.15. В случае невозможности отзыва расчетного документа из банка плательщика по причине его исполнения, 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 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 направить в банк плательщика с приложением Справки по факту инцидента информационной безопасности в системе ДБО, а также подтверждающих документов. (форма справки на стр.4-5 настоящих Рекомендаций).

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

Председателю Правления
Банка «Таврический» (ОАО)

"__" _____ 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: _____

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. _____

СПРАВКА
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: _____

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 _____

☐ 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 N _____ 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: _____

ПИСЬМО
ИНТЕРНЕТ ПРОВАЙДЕРУ О ПРЕДОСТАВЛЕНИИ ЖУРНАЛОВ СОЕДИНЕНИЙ (ЛОГОВ)

_____
должность руководителя

_____
наименование организации

_____
Ф.И.О.

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 N _____ 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. _____

ЗАЯВЛЕНИЕ
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: _____

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.