Приложение № 18
к Регламенту работы в системе ДБО «ИНТЕРНЕТ-БАНК»
в ООО «Банк РСИ»

Порядок действий

пострадавшего Клиента - юридического лица, индивидуального предпринимателю или физического лица, занимающегося в установленном законодательством порядке частной практикой

1. В случае выявления Клиентом хищения денежных средств в *системе ДБО «ИНТЕРНЕТ-БАНК»*

Клиент обязан:

1.1. немедленно прекратить любые действия с электронным устройством (далее – **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 по телефону (495) 951-72-32, в Операционный отдел/Отдел по работе с физическими лицами или Отдел Автоматизации с заявлением о блокировке системы ДБО и 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 с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе ДБО (*Приложение № 18а) к* Регламенту работы в системе ДБО «ИНТЕРНЕТ-БАНК» в ООО «Банк РСИ», 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 не позднее дня, следующего за днем телефонного обращения.

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.

При наличии необходимой информации обратиться в банк получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении платежа и возврате денежных средств (Приложении № 18б)

1.7. 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.

1.8. 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.

1.9. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи *(Приложение № 18в)* Регламента «Форма письма интернет провайдеру о предоставлении журналов соединений (логов)») 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.

1.10. 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.

1.11. 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.

1.12. 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.

1.13. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ) (*Приложение № 18г Регламента*).

1.14. 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.

1.15. Копии вышеуказанных документов по перечню, установленному банком плательщика, направить в Банк с приложением Справки по факту инцидента информационной безопасности в системе ДБО (*Приложение № 18д* Регламента), а также подтверждающих документов (*Приложение № 18е Регламента*)