Небанковская кредитная организация
«Платежи и Расчеты» (акционерное общество)

Требования по обеспечению мер безопасности при использовании клиентского рабочего места Системы ДБО iBank

2018

1. Область применения

1.1. Рекомендации, настоящего документа распространяются на клиентов Небанковской кредитной организации «Платежи и Расчеты (акционерное общество) (далее – НКО), использующих систему дистанционного банковского обслуживания (далее - Систему ДБО).

1.2. Настоящий документ описывает риски, возникающие на стороне клиента при использовании Системы ДБО, и определяет перечень мер по снижению этих рисков.

2. Описание рисков

2.1. Основным риском при использовании Системы ДБО является риск получения злоумышленником несанкционированного доступа к управлению счетом клиента и к документам клиента, передаваемым в НКО через Систему ДБО.

2.2. Последствиями несанкционированного доступа могут быть списание денежных средств со счета клиента или утечка конфиденциальной информации о совершаемых клиентом операциях.

3. Способы несанкционированного доступа к Системе ДБО

3.1. Основными способами получения несанкционированного доступа к Системе ДБО являются:

- перехват злоумышленником управления компьютером клиента;
- кража логина и пароля клиента для входа в Систему ДБО, а также закрытой части ключа ЭП клиента;
- перехват данных, передаваемых клиентом в НКО и получаемых клиентом из НКО.

3.2. Получение несанкционированного доступа может быть осуществлено:

- штатными сотрудниками организации клиента;
- нештатными сотрудниками, приходящими по вызову для обслуживания компьютеров организации клиента;
- злоумышленниками, получившими доступ к компьютерам организации клиента через сеть Интернет или иные каналы связи.

4. Признаки несанкционированного использования клиентского рабочего места Системы ДБО

- наличие в системе нелегитимного платёжного поручения (платёжное поручение сформировано злоумышленником);
- наличие в системе не заказанных выписок, или иных документов (документы заказаны злоумышленником);
- «самостоятельная» (независимая от действий пользователя) работа компьютера: перемещение курсора, открытие и закрытие окон программ, заполнение форм и документов и пр. (управление компьютером захвачено злоумышленником);
- отсутствие доступа к Системе ДБО по причине неверного пароля (пароль изменен злоумышленником);
- нестабильная работа компьютера или полная его неработоспособность (последствия деятельности злоумышленника по уничтожению следов вторжения);
- не работает ключевой носитель – повреждены, отсутствуют файлы с криптографическими ключами (последствия деятельности злоумышленника).

Данный перечень признаков несанкционированного использования Системы ДБО не является исчерпывающим. В зависимости от новых видов атак список может дополняться и

корректироваться. Извещения о новых признаках публикуются на сайте www.1erc.ru и/или рассылаются клиентам НКО через Систему ДБО.

5. Компрометация закрытой части ключа ЭП (ключевого носителя)

К событиям, на основании которых принимается решение о компрометации, относятся, включая, но, не ограничиваясь, следующие события:

- потеря ключевых носителей (даже с их последующим обнаружением);
- увольнение сотрудников, имевших доступ к ключевым носителям;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

6. Меры по предотвращению несанкционированного использования клиентского рабочего места Системы ДБО

Клиенту, в целях снижения возможного риска несанкционированного использования рабочего места Системы ДБО и списания третьими лицами денежных средств со счета клиента, необходимо:

6.1. Соблюдать правила пользования Системы ДБО.

6.2. Выполнять следующие организационные и технические меры:

- минимизировать количество пользователей, которые имеют право доступа к компьютеру с установленным рабочим местом Системы ДБО, ограничив его кругом лиц, непосредственно использующих Систему ДБО;
- осуществлять оценку деловой репутации пользователей, имеющих доступ к Системе ДБО;
- использовать на компьютерах только лицензионное программное обеспечение;
- регулярно обновлять операционную систему и используемое для работы с ДБО программное обеспечение. Установку обновлений необходимо производить только с официальных сайтов разработчиков соответствующего программного обеспечения;
- установить на компьютерах систему антивирусной защиты. Обновление баз данных антивирусного ПО должно осуществляться ежедневно, либо по мере выхода новых официальных версий баз данных;
- при работе с электронной почтой не открывать письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам. Наилучшей практикой является отказ от использования электронной почты на компьютерах с установленными рабочими местами Системы ДБО;
- использовать для размещения закрытых ключей ЭП только внешние извлекаемые носители информации. Рекомендуется использовать специальные флэш-носители типа eToken. Использование в качестве места хранения ключевой информации реестра или жесткого диска компьютера увеличивает риск хищения закрой части ключей ЭП;
- извлекать ключевой носитель сразу после окончания сеанса работы с Системой ДБО;
- хранить ключевой носитель в недоступном для посторонних месте, например в сейфе;
- не использовать ключевой носитель для иных, кроме работы с Системой ДБО, целей, например, для хранения файлов, электронных документов и т.п.

- не передавать ключи ЭП и не сообщать логин и пароль доступа к Системе ДБО кому-либо, сотрудники НКО никогда не запрашивают пароли своих клиенов;
- всегда проверять, правильный ли адрес отображается в строке браузера, организационно или технически ограничить доступ в Интернет с компьютеров, на которых установлены рабочие места Системы ДБО, разрешив доступ только к доверенным ресурсам сети Интернет. К доверенным сайтам следует отнести сайты:
  а) *.1erc.ru;
  б) сайты и адреса, необходимые для функционирования Системы ДБО «iBank»;
  в) официальные сайты разработчиков используемого на рабочем месте программного обеспечения (в т.ч. операционной системы, системы антивирусной защиты, сетевого экрана);
- не использовать компьютер, на котором установлено рабочее место Системы ДБО, не по назначению, например, для игр, просмотра фильмов и т.п. и не использовать для работы с Системой ДБО недоверенные, чужие компьютеры (интернет-кафе, интернет-киски и т.п.);
- если компьютер установлен внутри локальной сети организации, провести мероприятия по защите локальной сети от зловредных воздействий со стороны сети Интернет.

6.3. В случае подозрения на несанкционированный доступ к компьютеру с установленным рабочим местом Системы ДБО или установлении фактов компрометации закрытой части ключа ЭП:

- срочно связаться с НКО и проинформировать об имеющихся подозрениях или фактах;
- проверить легитимность всех выполненных за последнее время платежей;
- направить в НКО заявление о блокировке операций в Системе ДБО;
- произвести смену ключей ЭП.