Правила

по обеспечению мер информационной безопасности при работе с системой дистанционного банковского обслуживания «Клиент-Банк»

1.1. Область применения

1.1.1. Рекомендации настоящих Правил распространяются на клиентов - юридических лиц, индивидуальных предпринимателей или лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой (далее – Клиенты), использующих систему дистанционного банковского обслуживания (далее – ДБО) АКБ «СОЮЗ» (ОАО) (далее – Банк).

1.1.2. Настоящие Правила описывают риски, возникающие на стороне Клиента при работе в ДБО, и устанавливает перечень мер по снижению таких рисков.

1.1.3. Настоящие Правила или выдержки из них размещаются на официальном сайте Банка. При изменении настоящих Правил Банк размещает на своем официальном сайте их новую редакцию, о чем может информировать Клиента с использованием ДБО или путем сообщения на своем официальном сайте. Клиенту необходимо регулярно знакомиться с изменениями в Правила и принимать, в соответствии с ними, необходимые меры информационной безопасности при работе в ДБО.

1.2. Описание рисков

1.2.1. Основным риском при использовании ДБО является риск получения злоумышленником несанкционированного доступа к управлению счетом Клиента и к документам Клиента, передаваемым в Банк через ДБО.

1.2.2. Последствиями несанкционированного доступа могут быть списание денежных средств со счета Клиента или утечка конфиденциальной информации о совершаемых Клиентом операциях.

1.3. Способы несанкционированного доступа к ДБО

1.3.1. Основными способами получения несанкционированного доступа к ДБО являются:

- перехват злоумышленником управления компьютером Клиента;

- кража логина и пароля Клиента для входа в ДБО, а также закрытой части ключа электронной подписи (далее – ЭП) Клиента;

- перехват данных, передаваемых клиентом в Банк и получаемых Клиентом из Банка.

1.3.2. Получение несанкционированного доступа может быть осуществлено:

- штатными сотрудниками Клиента;

- нештатными сотрудниками, приходящими по вызову для обслуживания компьютеров Клиента;

- злоумышленниками, получившими доступ к компьютерам Клиента через сеть Интернет или иные каналы связи.

1.4. Признаки несанкционированного использования клиентского рабочего места ДБО

- наличие в ДБО нелегитимного платежного документа (документ, сформированный злоумышленником);

- наличие в ДБО не заказанных выписок или иных документов (документ, заказанный 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 ДБО по причине неверного пароля (пароль изменен злоумышленником);

- нестабильная работа компьютера или его неработоспособность (последствия действия злоумышленника по уничтожению следов вторжения);

- не работает ключевой носитель – повреждены/отсутствуют файлы с криптографическими ключами (последствия действия злоумышленника).

Данный перечень признаков несанкционированного использования ДБО не является исчерпывающим. В зависимости от новых видов атак список может дополняться и корректироваться. Извещения о новых признаках будут публиковаться на сайте Банка и/или рассылаться Клиентам Банка через ДБО.

1.5. 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, имеющих доступ к ключевым носителям;

- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (например, при выходе из строя ключевого носителя нет достоверной возможности установить причину, т.к. к этому могли привести действия злоумышленника)

1.6. Меры по предотвращению несанкционированного использования клиентского рабочего места ДБО

Клиенту, для снижения возможного риска несанкционированного использования рабочего места ДБО и списания третьими лицами денежных средств со счета Клиента, необходимо:

1.6.1. Соблюдать правила пользования ДБО, в т.ч. знакомиться с информацией и материалами, касающимися работы ДБО на сайте Банка.

1.6.2. Использовать услугу в виде возможности подключения к ДБО только с определенных IP-адресов компьютеров Клиента и/или информирование о входе в ДБО, посредством технологии сотовой связи – службы коротких сообщений (СМС).

1.6.3. Выполнять следующие организационные и технические меры:

- минимизировать количество пользователей, которые имеют право доступа к компьютеру с установленным рабочим местом ДБО, ограничив его кругом лиц, непосредственно использующим ДБО;

- осуществлять оценку деловой репутации пользователей, имеющих доступ к ДБО;

- использовать на компьютерах только лицензионное программное обеспечение;

- регулярно обновлять операционную систему и используемое для работы с ДБО программное обеспечение. Установку обновлений необходимо проводить только с официальных сайтов разработчиков соответствующего программного обеспечения;

- установить на компьютерах систему антивирусной защиты. Обновление баз данных антивирусных программ должно осуществляться ежедневно, либо по мере выхода новых официальных версий баз данных;

- использовать сетевые экраны при выходе в сеть Интернет, разрешив доступ только к доверенным ресурсам сети Интернет. Запретить в межсетевом экране соединение с сетью Интернет по протоколам ftp, smtp. Разрешить соединения по протоколу smtp только с конкретными почтовыми серверами, на которых зарегистрированы почтовые ящики Клиента;

- 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 ДБО;

- не использовать права администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора;

- включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал регистрации и реагировать на ошибки;

- использовать для размещения закрытых ключей ЭП только внешние извлекаемые носители информации. Использование в качестве места хранения ключевой информации реестра или жесткого диска компьютера увеличивает риск хищения закрытой части ключа ЭП;

- извлекать ключевой носитель сразу после окончания сеанса работы с ДБО;

- хранить ключевой носитель в недоступном для посторонних месте, например, в сейфе;

- не использовать ключевой носитель для иных, кроме работы с ДБО, целей, например, для хранения файлов, электронных документов и т.п.;

- не передавать ключи ЭП и не сообщать логин и пароль доступа к ДБО третьим лицам;

- не использовать компьютер, на котором установлено рабочее место ДБО, не по назначению, например, для игр, просмотра фильмов и т.п.;

- в случае если компьютер установлен внутри локальной сети организации, провести мероприятия по защите локальной сети от несанкционированных воздействий со стороны сети Интернет;

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

- срочно связаться с Банком и проинформировать об имеющихся подозрениях или фактах;

- проверить легитимность всех выполненных за последнее время платежей;

- направить в Банк заявление о блокировке операций по ДБО;

- произвести смену ключей ЭП.