Приложение № 1

к Правилам электронного документооборота для корпоративных клиентов Акционерного общества Банк конверсии «Снежинский»

Требования информационной безопасности при работе в СЭД

1. Клиент подтверждает, что до заключения Договора присоединения проинформирован Банком об условиях использования СЭД, в т.ч. об ограничениях способов и мест использования, случаях повышенного риска использования СЭД.
2. С целью исключения возможности хищения персональной и/или ключевой информации третьими лицами, а также несанкционированного доступа третьих лиц к счету (счетам) и хищения денежных средств Клиент обязан:
   - обеспечить работу с ключами ЭП только тем сотрудникам, которые имеют навык работы на персональном компьютере и которые ознакомлены с настоящими требованиями информационной безопасности;
   - установить СЭД на рабочее место, оборудованное лицензионным, регулярно обновляемым программным обеспечением (включая операционную систему, средства защиты);
   - установить на рабочее место актуальное антивирусное программное обеспечение и регулярно обновлять вирусные базы данных;
   - производить установку и обновление программного обеспечения только с доверенных источников (рекомендуемых производителем или поставщиком программного обеспечения);
   - установить на компьютер межсетевой экран (брандмауэр, файервол) с «Белым списком», в котором будут указаны только необходимые адреса (сервер СЭД Банка, сервера обновлений операционной системы, средств защиты, интернет-браузера и других необходимых приложений);
   - исключить возможность разглашения персональной ключевой информации, путем строгого ограничения доступа к ней (хранение электронных носителей ключевой информации в сейфах, организации использования и системы контроля доступа к компьютеру, к электронным носителям и т.д.)
3. В целях обеспечения исполнения обязанностей соблюдения требований информационной безопасности Клиенту необходимо:
   - работу на компьютере производить под ограниченными в правах учетными записями (без прав администратора);
   - отключить функцию «Автоматическое выполнение» для подсоединяемых к компьютеру внешних носителей (копакт-дисков, флэш-карт и т.д.);
   - с рабочего места, на котором установлена СЭД, организационно и технически запретить посещение сотрудниками Клиента ресурсов сети Интернет, получение сообщений по электронной почте, а также запретить установку и/или использование программного обеспечения, не участвующего напрямую в работе СЭД или в подготовке платежных документов;
   - для хранения ключей ЭП использовать только внешние носители (дискеты, флеш-накопители и т.п.). Ни в коем случае не сохранять ключи ЭП на жёстких/сетевых дисках компьютера, в реестре операционной системы. Для хранения внешних носителей с ключами ЭП используйте сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
   - каждый раз, сразу после окончания работы в СЭД и на время перерыва в работе извлекать внешний носитель с ключами ЭП из компьютера;
   - хранить резервную копию ключей ЭП только на внешнем носителе, помещенном в недоступное для посторонних лиц место (сейф).
4. В том случае, если представители Клиента, на которых оформлены ключи ЭП, доверяют кому-либо использовать свои ключи ЭП, то Клиент (руководитель Клиента) несет полную ответственность за соблюдение условий Правил электронного документооборота для корпоративных клиентов Акционерного общества Банк конверсии «Снежинский», как со своей стороны, так и со стороны лиц, пользующихся ключами ЭП.
5. Осуществляйте информационное взаимодействие с Банком только с использованием средств связи и реквизитов, указанных в документах, получаемых непосредственно в Банке.
6. При эксплуатации СКЗИ недопустимо:
   - подключать к компьютеру с СЭД дополнительные устройства и соединители без соответствующего предписания на возможность их совместного использования;
   - оставлять без контроля рабочее место с СЭД. При кратковременном перерыве в работе необходимо производить блокирование компьютера, разблокирование производить с использованием регулярно обновляемого пароля доступа;
   - вносить какие-либо изменения в программное обеспечение СКЗИ.

7. При утрате или компрометации ключей ЭП и/или при обнаружении несанкционированного списания денежных средств со счета Клиента, необходимо незамедлительно уведомить о данном факте Банк способом, указанным в Договоре присоединения.
8. **При увольнении сотрудника, на которого были оформлены ключи ЭП, увольнении сотрудника, имевшего технический доступ к ключам ЭП, незамедлительно заблокировать старые ключи ЭП и предоставить информацию в Банк**.

Помните, что Клиент (представитель Клиента) берет на себя полную ответственность и обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение ключей ЭП.

При возникновении сомнений в авторстве почтовых сообщений, полученных от лиц технической поддержки или иных подразделений Банка, технической поддержки иных организаций, сообщений государственных органов, незнакомых контрагентов, **ни в коем случае не открывать вложенные в письме материалы и не переходить по ссылкам, указанным в письме**.

В случае невыполнения Клиентом и/или сотрудниками Клиента Требований информационной безопасности при работе в СЭД Банк не несет ответственности за несанкционированное списание денежных средств со счета Клиента (принятия поручения от неуполномоченного лица, в результате которого у Клиента возникли убытки).

Ознакомлен: _____/_____/ «__»_____20__

МП подпись и ФИО руководителя Клиента