ПОРЯДОК
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ ИНТЕРНЕТ-БАНКИНГА

1. Общие положения

1.1. Организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи электронных документов в СИБ с использованием средств криптографической защиты информации (средств ЭП) Клиент проводит в соответствии с приказом ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» и эксплуатационной и технической документацией на СИБ и средства защиты информации.

1.2. Клиент назначает ответственных за эксплуатацию СИБ (пользователей СКЗИ) и администратора безопасности.

2. Размещение рабочего места

2.1. Размещение, специальное оборудование, охрана и организация режима помещений, в которых расположены рабочее место и хранятся носители с ключами ЭП, должны исключать возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

2.2. Помещения, предназначенные для размещения рабочего места и хранения носителей с ключами ЭП, должны быть оборудованы прочными дверьми, замками повышенной секретности и сигнализацией. Окна помещений, расположенных на первых или последних этажах зданий, а также находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, должны быть оборудованы решетками и/или сигнализацией.

3. Защита от несанкционированного доступа на рабочем месте

3.1. Клиентом должны быть разработаны нормативные документы, регламентирующие правила хранения, доступа и использования ключей ЭП от несанкционированного доступа, и строго им соблюдаться.

3.2. Клиент должен принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства, используемые для работы в СИБ, изменение их состава, появление компьютерных вирусов, а также программ, направленных на разрушение или модификацию программного обеспечения СИБ, ЭД, либо на перехват паролей, ключей ЭП и другой информации.

3.3. На рабочем месте должен быть реализован комплекс мер и средств защиты от угроз публичной сети Интернет, обеспечивающий защиту данных от несанкционированного доступа по сети. Клиент должен постоянно использовать антивирусное программное обеспечение и своевременно осуществлять его обновление, а также обновления компонентов СИБ, операционной системы, прикладного программного обеспечения.

3.4. Запрещается передавать третьим лицам пароли (PIN коды) для доступа в СИБ и к носителю с ключами ЭП, включая сотрудников Банка и сотрудников Клиента или родственников уполномоченных лиц.

3.5. Запрещается установка программных средств на рабочем месте, не предназначенных для выполнения служебных обязанностей уполномоченных лиц, допущенных к работе с СИБ в том числе программных средств для удаленного управления рабочим местом Клиента.

3.6. Ключи ЭП должны размещаться только на съемном носителе (USB Flash, USB-токен и др.) Подключение носителей с ключами ЭП к компьютеру, на котором осуществляется работа в СИБ, допускается только непосредственно на время работы с СИБ; после окончания сеанса работы носитель с ключами ЭП должен быть извлечен.

3.7. Носители ключевой информации с ключами ЭП и СКЗИ должны браться на поэкземплярный учет в специально выделенных для этих целей журналах.

3.8. Порядок хранения и использования носителей ключевой информации должен исключать возможность несанкционированного доступа к ним.

3.9. При выявлении признаков нарушения информационной безопасности рабочего места, при наличии подозрений на несанкционированный доступ к счетам через СИБ, получения посредством SMS или E-mail информации о действиях, которые Клиент не совершал, Клиенту необходимо временно приостановить эксплуатацию (отключить технические средства) рабочего места и незамедлительно проинформировать об этом Банк.

4. Правила хранения и уничтожения носителей с ключами ЭП и СКЗИ

4.1. Для хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к СКЗИ, носителей с ключами ЭП необходимо использовать надежные металлические шкафы или сейфы (хранилище), оборудованные внутренними замками.

4.2. Хранение носителей с ключами ЭП допускается в хранилище, используемом совместно с другими сотрудниками, но при этом в отдельной упаковке (контейнере), опечатанной личной печатью владельца ключа ЭП и исключающей возможность несанкционированного доступа к ним посторонних лиц.

4.3. Запрещается передавать носители с ключами ЭП другим лицам, выводить ключи ЭП на дисплей или принтер, оставлять носители с ключами ЭП без присмотра, а также записывать на носитель ключевой информации постороннюю информацию.

4.4. Уничтожение ключей ЭП может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (форматирования) ключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Уничтожение СКЗИ проводится в соответствии с эксплуатационной документацией на эти средства.

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

Факт уничтожения ключей ЭП, СКЗИ и эксплуатационной и технической документации должен фиксироваться в клиентских журналах учета.

5. Требования к лицам, ответственным за работу с СИБ

5.1. Сотрудники, допущенные к работе с СИБ, назначаются приказом и должны иметь утвержденные должностные инструкции.

5.2. Непосредственная работа сотрудников с СИБ возможна только после прохождения ими обучения и проверки знания ими правил эксплуатации.

5.3. Каждый сотрудник, имеющий доступ к носителям с ключами ЭП, паролям и другим конфиденциальным сведениям в соответствии с Договором и Правилами, должен быть проинформирован об ответственности за разглашение таких сведений и подписать соответствующие обязательства.