ТРЕБОВАНИЯ
по обеспечению безопасности в процессе эксплуатации средства криптографической защиты информации (СКЗИ)

В целях обеспечения информационной безопасности при использовании Системы «Интернет-Банк» Банк рекомендует:

1. Соблюдать меры безопасности по режиму:

- размещать Систему «Интернет-Банк» на специально выделенном для этого компьютере;
- исключить доступ к компьютерам, использующимся в Системе «Интернет-Банк», персонала, не имеющего отношения к работе в Системе «Интернет-Банк»;
- обеспечить контроль за действиями IT-специалистов при обслуживании компьютеров, подключенных к Системе «Интернет-Банк»;
- размещение и установка СКЗИ должны удовлетворять требованиям документации на СКЗИ.

2. Обеспечить безопасность закрытых ключей ЭЦП:

- хранить закрытые ключи ЭЦП только на eToken;
- использовать eTokenPass для генерации одноразовых паролей на вход;
- не использовать съемные носители информации, предназначенные для хранения закрытых ключей ЭЦП, для каких-либо иных целей;
- категорически запрещается хранить закрытые ключи ЭЦП на жестком диске компьютера;
- работу с ключами поручать только специально выделенным работникам, которые должны нести персональную ответственность за сохранность ключей;
- незамедлительно сообщать Банку о фактах компрометации или подозрения в компрометации ключей, в том числе, - о переводе на другую работу или увольнении работников, имевших доступ к ключевой информации (использование скомпрометированного ключа должно быть немедленно прекращено);
- предусмотреть хранение носителей с ключами ЭЦП в надежном хранилище (сейф, металлический шкаф), допуская их извлечение только на период непосредственной работы с ключами;
- обеспечить контроль носителей с ключами при их нахождении вне хранилища (в случае даже кратковременного отсутствия на рабочем месте работника, ответственного за ключи, носители ключей должны быть убраны в хранилище);
- при использовании Системы «Интернет-Банк» устанавливать в компьютер носители с ключами только для авторизации клиента и подписания электронного документа ЭЦП (после выполнения отмеченных операций носители с ключами должны быть извлечены из компьютера);
- не передавать ключи ЭЦП, а также логин и пароль доступа к Системе «Интернет-Банк» кому-либо, в том числе IT-специалистам при проверке работоспособности Системы «Интернет-Банк», установке параметров и настройке аппаратуры;
- находясь в общественном месте (выставка, библиотека, магазин, интернет-кафе и др.) по возможности исключить какие-либо действия с ключами ЭЦП, логином и паролем доступа к Системе «Интернет-Банк», а также использование публичных компьютеров, находящихся в общественном месте, для обмена сообщениями с Банком.

3. Применять необходимые меры антивирусной защиты:

- применять на рабочем месте лицензионные средства антивирусной защиты; обеспечить регулярное обновление антивирусных баз и их поддержание в актуальном состоянии; еженедельно проводить полную антивирусную проверку;
- обеспечить своевременное (не реже одного раза в неделю) обновление системного программного обеспечения ;
- исключить посещение любых интернет-сайтов с компьютеров, подключенных к

Системе «Интернет-Банк»;

- при работе с электронной почтой не открывать письма и вложения к ним, поступившие от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам (не активизировать ссылки);

- не отвечать на письма, якобы от имени Банка, с предложениями (просьбами, требованиями) зайти на сайт, не принадлежащий домену http://assotsiatsiyabank.ru/;

- использовать только программное обеспечение Системы «Интернет-Банк», предоставленное Банком;

- если компьютер, предназначенный для работы в Системе «Интернет-Банк», неожиданно перестал запускаться или выдает непонятные сообщения, или происходит нештатный выход из программы необходимо незамедлительно проинформировать об этом сотрудников технической поддержки Банка и исключить использование действующих рабочих ключей ЭЦП (извлечь носитель с ключами в случае его нахождения в компьютере);

- при увольнении штатных IT-специалистов, осуществлявших обслуживание компьютеров, используемых для работы в Системе «Интернет-Банк», а также после любых действий внештатных IT-специалистов или других работников, выполнявших какие-либо операции с компьютерами, предназначенными для работы в Системе «Интернет-Банк», провести проверку компьютеров на отсутствие вредоносных программ и произвести смену пароля;

- при возникновении подозрений о наличие в компьютере вредоносных программ незамедлительно исключить использование действующих рабочих ключей ЭЦП (извлечь носитель с ключами в случае его нахождения в компьютере) и сообщить об инциденте в Банк (возобновление работы с ключами допустимо только после проверки компьютера и устранения зараженности).

4. Формировать пароль доступа к Системе «Интернет-Банк» с учетом следующих требований:

- пароль должен содержать не менее 10 символов, при создании пароля могут быть использованы 4 группы символов (заглавные буквы, строчные буквы, цифры и специальные символы), в пароле должны присутствовать символы не менее чем из 3-х групп;

- последовательность символов не должна содержать очевидных закономерностей;

- пароль не должен содержать:

  комбинации символов, несущих смысловую нагрузку (имена, фамилии, названия)

  последовательность символов, состоящих только из цифр (в том числе, - номера телефонов, памятные даты, реквизиты клиента и т.п.) или букв;

  последовательности повторяющихся букв и цифр;

  подряд идущие в алфавите или раскладке клавиатуры символы;

- регулярно проводить смену пароля (не реже 1 раза в месяц).

Использовать дополнительное средство аутентификации — одноразовые пароли.

5. Помнить, что Банк никогда не запрашивает у клиентов информацию (в том числе, путем рассылки электронных писем) об их персональных данных, ключах ЭЦП, логине и пароле доступа к Системе «Интернет-Банк». При поступлении таких запросов, не отвечая на них, следует незамедлительно поставить в известность Банк.

6. Строго соблюдать положения документов Банка, регламентирующих условия доступа клиента к Системе «Интернет-Банк», требования по использованию, хранению, уничтожению криптографических ключей ЭЦП, СКЗИ, логинов, паролей, а также выполнять все рекомендации Банка по эксплуатации технических средств.

7. Обращаться по всем вопросам организации электронного документооборота по телефонам, переданным клиенту при открытии банковского счета или указанным в договоре банковского обслуживания с использованием Системы «Интернет-Банк».