Приложение № 6
к договору о предоставлении услуг с использованием
системы дистанционного банковского обслуживания

Рекомендации
по обеспечению безопасности использования средств криптографической защиты информации и электронной подписи (снижению рисков осуществления перевода денежных средств со счета без согласия Клиента) и меры по их реализации

1. Требования к организации режима обеспечения безопасности помещения, в котором эксплуатируется средства криптографической защиты (далее – СКЗИ) и применяется ЭП.

1.1. Клиентом должны быть приняты меры по исключению несанкционированного доступа посторонних лиц (включая и собственных сотрудников, не имеющих допуск к Системе) в помещение, в котором осуществляется хранение ключей ЭП и размещены СКЗИ.

1.2. В случае необходимости присутствия посторонних лиц в указанном помещении должен быть обеспечен контроль их действий во избежание негативных воздействий с их стороны на ключи ЭП, СКЗИ и передаваемую информацию.

1.3. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключи ЭП.

2. Требования по защите информации от несанкционированного доступа к СКЗИ, общесистемному и специальному программному обеспечению АРМ.

2.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в операционную систему, BIOS и т.д.). Периодичность смены пароля не должна превышать 90 календарных дней.

2.2. При использовании ключей ЭП АРМ должен быть сконфигурирован с учетом следующих требований:
- не использовать нестандартные, измененные или отладочные версии операционных систем;
- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;
- на АРМ должна быть установлена только одна операционная система;
- на АРМ должно устанавливаться только лицензионное ПО;
- все неиспользуемые сетевые компоненты системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;
- необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части): системному реестру, файлам и каталогам, временным файлам, журналам системы, кэшируемой информации (пароли и т.п.), отладочной информации.

2.3. АРМ необходимо использовать в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.

2.4. Администрирование АРМ должно осуществляться доверенными лицами.

2.5. Программное обеспечение, используемое на АРМ, не должно содержать возможностей, позволяющих:
- модифицировать: настройки операционной системы, содержимое произвольных областей памяти, собственный код и код других подпрограмм, а также память, выделенную для других подпрограмм;
- передавать управление в области собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- использовать недокументированные фирмой-разработчиком функции операционной системы.

2.6. На АРМ необходимо исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий, регулярно устанавливать пакеты обновлений безопасности операционной системы, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

2.7. При подключениях АРМ к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных с ресурсов или с использованием общедоступных сетей передачи данных (в т.ч. Интернет), без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам АРМ, в окружении которых функционируют СКЗИ, со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

2.8. Необходимо организовать и использовать систему аудита, организовать регулярный анализ результатов аудита, а также комплекс мероприятий по антивирусной защите, включающий установку антивирусного программного обеспечения с постоянно включенной защитой.

3. Требования к паролям для Клиентов Банка.

3.1. Логины и пароли для работы в Системе – это Ваша персональная конфиденциальная информация. Ни при каких обстоятельствах не сообщайте свой логин и пароль никому, включая сотрудников Банка. Если к Вам обращаются от имени Банка (по телефону, электронной почте, через SMS) с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова, и т.д.), ни при каких обстоятельствах не сообщайте эту информацию.

3.2. Не храните логин и пароль в текстовых файлах на компьютере или на других электронных носителях, чтобы его не украли и не скомпрометировали.

3.3. Общие требования к защите пароля:
- логин и пароль к персональной учетной записи должны знать только Вы;
- запрещается хранение паролей в доступном для чтения виде;
- запрещается использовать функции автосохранения паролей в браузерах;
- запрещается передавать пароли по каналам связи (например, по электронной почте) в открытом виде;
- при вводе пароля исключите возможность его подсматривания посторонними лицами и фиксирования фото/видеокамерами.

3.4. Требования к формированию пароля:
- длина пароля должна быть не менее чем 8 символов;
- среди символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные

символы (@, #, $, &, *, % и т.п.);
- пароль не должен содержать легко вычисляемые сочетания символов, например: имена, фамилии, даты, имя учетной записи; распространенные последовательности символов («QAZwsx123», «Qwe123!» и т.п.); общепринятые сокращения;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

4. Требования по обеспечению информационной безопасности при обращении с ключевыми носителями.

4.1. Меры защиты ключей ЭП:
- ключи ЭП при их создании должны записываться только на ключевые носители, полученные в Банке, которые поддерживаются используемыми СКЗИ согласно технической и эксплуатационной документации к ним;
- для контроля доступа к ключевому носителю установите на него пароль. Не сообщайте никому пароль для доступа к ключевому носителю (включая сотрудников Банка и сотрудников Вашей организации или Ваших родственников);
- ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на Владельца ключа ЭП.

4.2. Обращение с ключевой информацией и ключевыми носителями:
- Клиент может иметь необходимое ему количество ключевых носителей;
- ключевые носители должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, закрывающийся металлический ящик и т.д.);
- ключевой носитель должен подключаться в считывающее устройство только на время работы с Системой. Запрещается оставлять ключевой носитель подключенным в USB-порт при отсутствии лица, уполномоченного на работу в Системе. После окончания сеанса работы в Системе извлеките ключевой носитель из компьютера;
- на ключевом носителе недопустимо хранить иную информацию (в том числе рабочие или личные файлы);
- если Вы используете несколько ключей ЭП, не переносите эти ключи на один носитель, а также не подключайте к компьютеру одновременно разные ключевые носители;
- в случае прекращения действия Договора о предоставлении услуг с использованием системы дистанционного банковского обслуживания (далее - Договор) Клиент обязан в течение 10 (десяти) дней уничтожить по акту (по форме устанавливаемой Клиентом) ключевой носитель.

5. Срок действия ключей ЭП, порядок смены ключей ЭП.

5.1. Срок действия ключа ЭП в Системе составляет один календарный год с момента генерации Сертификата ключа ЭП, но не может превышать срока действия полномочий Владельца ключа ЭП, наделенного правом подписи, указанной в карточке с образцами подписей и оттиска печати Клиента.

5.2. Срок действия ключа Клиента может быть изменен администратором Системы в следующих случаях:
- выявление угрозы безопасности дальнейшего использования данного ключа ЭП Клиентом, о чем Банк уведомляет Клиента по Системе;
- изменение срока действия полномочий уполномоченных лиц, указанных в карточке с образцами подписей Клиента, являющихся Владельцем ключа ЭП.

5.3. Система автоматически уведомляет Клиента при каждом сеансе связи об истечении срока действия ключа ЭП, начиная с 30 суток до момента полной блокировки ключа ЭП, исключая случаи, описанные в п. 4.2.

5.4. Генерация нового ключа ЭП осуществляйте лично с записью на ключевой носитель в порядке, предусмотренном Договором, при этом приобретать новый ключевой носитель не обязательно, генерацию можно произвести на ранее используемый Клиентом ключевой носитель. Не допускайте копирования сгенерированных ключей ЭП.

5.5. Перевыпускайте ключи ЭП до истечения срока их действия. По окончании срока действия ключи ЭП подлежат обязательной перегенерации Клиентом, при этом прежние ключи ЭП Клиента, по которым истек срок действия, считаются недействительными.

5.6. Перевыпускайте ключи ЭП в случаях:
- увольнения или смены лиц, имеющих доступ к Системе;
- смены руководителей с правом подписи доверенностей на получение ключей ЭП;
- подозрения на их компрометацию.

6. Действия при Компрометации.

6.1. Клиент (Владелец Сертификата) должен самостоятельно определять факт Компрометации и оценивать значение этого события.

6.2. Мероприятия по розыску и локализации последствий Компрометации организует и осуществляет сам Клиент.

6.3. В случае Компрометации или подозрении на Компрометацию, в том числе утраты ключевого носителя и (или) о его использовании без согласия Клиента, а также при внезапном выходе из строя АРМ Клиента, возникновении любых подозрений на Компрометацию (наличие в компьютере вредоносных программ, нестандартная работа системного программного обеспечения и т.д.), Клиент обязан:
- прекратить использование ключа ЭП и соответствующего Сертификата;
- незамедлительно сообщить в Банк любым из следующих способов и заблокировать ключи ЭП:
  - путем передачи в Банк письменного заявления в произвольной форме на бумажном носителе за подписью руководителя Клиента, заверенной печатью (при наличии);
  - путем направления Банку уведомления в Системе;
  - по телефону 8 495 276-06-16 с обязательным подтверждением сообщения Кодовым словом.

6.4. Получив сообщение о Компрометации, Банк незамедлительно приостанавливает операции по Счету (Счетам) Клиента с использованием Системы.

7. Порядок смены Кодового слова.

7.1. В случае компрометации Кодового слова (разглашение или подозрение на разглашение Кодового слова, увольнения или прекращения по другим причинам полномочий сотрудников, допущенных к работе с Кодовым словом) - Кодовое слово подлежит обязательной незамедлительной смене.

7.2. Для смены Кодового слова, Клиент предоставляет в Банк заявление об изменении кодового слова по форме Приложения № 1 к Соглашению об использовании кодового слова (далее – Заявление).

7.3. Производить смену Кодового слова может только Руководитель Клиента, чьи данные внесены в карточку образцов подписей и печатей и обладающий соответствующими полномочиями.

7.4. Заявление предоставляется только на бумажном носителе, при личном визите в Банк. Направление заполненного Заявления иными каналами связи (факс, почта, электронный документооборот) не допускается.

7.5. Кодовое слово считается обновленным по истечению не более 24 часов, после предоставления Банку заполненного Заявления.

8. Общие правила эксплуатации и хранения ключевого носителя.

- необходимо оберегать ключевой носитель от воздействия влаги и агрессивных сред сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т. п.), воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного ключевого носителя с мороза в теплое помещение) не рекомендуется использовать ключевой носитель в течение 3 часов во избежание повреждения ключевого носителя из-за сконденсированной на его электронной схеме влаги. Необходимо оберегать ключевой носитель от попадания на него прямых солнечных лучей;
- недопустимо воздействие на ключевой носитель сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества;
- при подключении ключевого носителя к компьютеру недопустимо прилагать излишние усилия;
- ключевой носитель в нерабочее время необходимо всегда держать закрытым во избежание попадания на его разъем пыли, грязи, влаги и т. п. При засорении разъема USB-токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо. Не следует разбирать ключевой носитель, это ведет к потере гарантии. В случае неисправности или неправильного функционирования ключевого носителя необходимо обратиться в Банк.

9. Правила безопасности при работе в Системе с целью снижению рисков осуществления перевода денежных средств со счета без согласия Клиента.

- ежедневно осуществляйте в Системе контроль за состоянием Счета (путем просмотра статуса ЭД и выписки по Счету) и при обнаружении подозрительных или несанкционированных операций незамедлительно обращайтесь в Банк. **НЕЗАМЕДЛИТЕЛЬНОЕ обращение в Банк с предоставлением полной информации о несанкционированном списании денежных средств со Счета может позволить оперативно приостановить транзакцию и предотвратить финансовые потери**;
- обращайте внимание на дату и время последнего входа в Систему (данные фиксируются на главной странице Системы, а также в специальном разделе «Безопасность – Журнал сеансов работы»);
- регулярно, не реже одного раза в 45 дней, производите смену ПИН-кода для защиты ключей ЭП на ключевом носителе;
- своевременно устанавливайте все официальные обновления к Системе;
- подключайте услугу e-mail или SMS-сообщений об отправке, исполнении платежных документов по Счету, а также обо всех входах в Систему;
- если Вы потеряли ключевой носитель или подозреваете, что доступ к Системе получили посторонние лица, немедленно обратитесь в Банк, чтобы заблокировать ключ ЭП и сообщить о Компрометации;
- после окончания работы в Системе обязательно корректно завершите работу (выйдите из Системы с использованием кнопки «Выход») или закройте браузер;
- если при работе в Системе или сразу после завершения сеанса возникли следующие проблемы:
  - при подключении к системе появилось предупреждение браузера о перенаправлении Вас на другой сайт;
  - вышел из строя жесткий диск;
  - возникли проблемы с загрузкой операционной системы;
  - внезапно прервался сеанс работы с Системой;
  - обнаружено заражение компьютера вредоносными программами;
  - возникли сомнения в правильности функционирования Системы;
  - появились платежные документы, которые Вы не формировали.

  НЕМЕДЛЕННО извлеките ключи ЭП и выключите компьютер, п также обратитесь в Банк и убедитесь, что от Вашего имени не производились несанкционированные операции.