РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ ЭП

Уважаемый Клиент!

Ключ электронной подписи (ЭП) и Ключ проверки ЭП, владельцем которых Вы теперь стали, являются элементами средств криптографической защиты информации (СКЗИ) обрабатываемой в электронном виде.

Ключ ЭП (секретный ключ) предназначен для создания ЭП при подписании ею документов и сообщений. Ваш Ключ ЭП, в том числе, может быть записан на специальный ключевой носитель (USB-ключ), который обеспечивает парольную защиту ключа ЭП. Ключ проверки ЭП (открытый ключ) включен в состав Сертификата, сформированного на Ваше имя. Сертификат записан на Ваш ключевой носитель, а также размещен в открытом доступе и может быть получен по открытым каналам связи. Кроме того, Сертификат необходимо установить на Ваш АРМ. Сертификат предназначен для обеспечения возможности расшифровки, определения подлинности и достоверности документов и сообщений, подписанных Вашей ЭП, а также доступа к различным системам Банка.

Основными Вашими обязанностями как Владельца СКП ЭП являются:

а) обеспечивать конфиденциальность Ключа ЭП, в частности не допускать использование принадлежащего Вам Ключа ЭП без Вашего согласия;

б) не использовать Ключ ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

в) уведомить Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности Ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

Рекомендации по работе с Ключом ЭП

а) применять для формирования ЭП только действующий Ключ ЭП;

б) применять Ключ ЭП с учетом ограничений, содержащихся в Сертификате, если такие ограничения были установлены;

в) не использовать Ключ ЭП, связанный с Сертификатом, заявление на прекращение или приостановление действия которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи соответствующего заявления в УЦ до момента времени официального уведомления о прекращении или приостановлении действия Сертификата, либо об отказе в прекращении его действия;

г) не использовать Ключ ЭП, связанный с Сертификатом, который аннулирован, действие которого прекращено или приостановлено;

д) после получения Ключа ЭП в УЦ на ключевом носителе в однодневный срок смените пароль доступа к Ключу ЭП (персональный ПИН-код) ЭП. Плановая смена пароля должна проводиться не реже, чем раз в квартал. Внеплановая смена пароля производится в случае компрометации пароля, при смене Ключа ЭП или при увольнении сотрудника, знавшего пароль доступа;

е) Владелец СКП ЭП должен осуществлять доступ для работы с СКЗИ только с помощью своего Ключа ЭП. В случае размещения Ключа ЭП на ключевом носителе во время работы носитель с Ключом ЭП подключается к компьютеру, а после работы необходимо закрыть программу, отключить носитель, убрать его в недоступное для посторонних место (например, в сейф или запираемый шкаф);

ж) запрещается оставлять ключевые носители подключенными к компьютеру или лежащими на рабочем месте во время Вашего отсутствия;

з) при длительном плановом перерыве в использовании Ключа ЭП (например, отпуск) желательно приостанавливать действие Ключа ЭП, направив соответствующее заявление в УЦ.

Владельцу СКП ЭП категорически не рекомендуется:

- оставлять носитель Ключа ЭП без присмотра, покидая рабочее место;
- несанкционированно сообщать кому-либо (разглашать) пароль доступа к Ключу ЭП;
- оставлять пароль (персональный ПИН-код) и памятку на бумажном носителе в любом месте, доступном посторонним лицам;
- распечатывать пароль (персональный ПИН-код) на общем принтере, оставлять выведенным на дисплей компьютера;
- копировать Ключ ЭП с ключевого носителя на жесткий диск компьютера или на обычный USB-накопитель;
- использовать программную опцию сохранения пароля (персонального ПИН-кода) в памяти системы.

Рекомендации по обеспечению доверенной среды Вашего компьютера

а) на компьютере, который предназначен для работы с использованием Ключа ЭП, должно быть установлено только лицензионное программное обеспечение (далее – ПО). Установленное ПО должно регулярно обновляться. Если Сертификат выпускался на Вас, как на работника организации, то состав ПО и порядок его обновления должен быть согласован со службой обеспечения безопасности информации вашей организации;

б) на Вашем компьютере должно быть установлено и регулярно обновляться средство антивирусной защиты. Все внешние электронные носители информации, а также загружаемые из сетей файлы и программы должны проверяться на наличие программных вирусов;

в) доступ для работы на компьютере должен быть ограничен за счет парольного доступа либо иными средствами защиты информации. Должна быть активирована функция автоматической блокировки компьютера при перерыве в работе;

г) запрещается использовать функцию «автоматического выполнения» для съемных носителей и компакт-дисков;

д) по возможности необходимо использовать на компьютере или в локальной сети, к которой она подключена, программные средства фильтрации трафика, ограничения IP-диапазона, блокировки сетевых атак;

е) использовать для создания и проверки ЭП, создания Ключей ЭП и Ключей проверки ЭП только сертифицированные Средства ЭП.

В случае наличии оснований полагать, что конфиденциальность Вашего ключа ЭП нарушена, пропажи (даже временной) ключевого носителя необходимо:

а) незамедлительно сообщить об этом в УЦ:

- по телефону: 8-800 333-25-50
- на адрес электронной почты: psbca@psbank.ru

б) направить в УЦ заявление на аннулирование действия Сертификата ключа проверки электронной подписи. Оператор УЦ сделает ответный звонок, чтобы убедиться, что это именно Вы звонили (отправили письмо).

Форму заявления можно получить по электронной почте или скачать с сайта Удостоверяющего центра.