

Руководство по обеспечению безопасности использования ключей электронной подписи и средств электронной подписи

1. Общие положения

Настоящее Руководство подготовлено в соответствии с частью 2 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и предназначено для официального информирования владельцев сертификатов ключей проверки электронной подписи, выдаваемых Удостоверяющим центром АО «Россельхозбанк», подчиненным подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (далее – ПУЦ), о рисках, условиях и правилах применения электронной подписи (далее – ЭП) и средств ЭП, а также о мерах, необходимых для обеспечения безопасности использования ЭП и средств ЭП.

При использовании в правоотношениях ЭП, использовании и эксплуатации средств ЭП владельцы СКП ЭП и средств ЭП должны соблюдать требования:

- Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- 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, утвержденной приказом ФАПСИ от 13.06.2001 № 152;
- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66;
- эксплуатационной документации на средства ЭП;
- Регламента Удостоверяющего центра АО «Россельхозбанк», подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (далее – Регламент ПУЦ);
- настоящего Руководства.

2. Риски, связанные с использованием ЭП

К основным рискам, связанным с использованием ЭП, относятся:

2.1. Несанкционированное подписание электронного документа ЭП, которое может быть произведено в результате:

- компрометации ключа ЭП;
- подмены подписываемого электронного документа в результате работы на компьютере или мобильном устройстве вредоносного программного обеспечения.

2.2. Негативные последствия, вызванные невозможностью подписания электронного документа ЭП, обусловленной следующими событиями:

- уничтожение (удаление с ключевого носителя) ключа ЭП и (или) СКП ЭП;
- неисправность ключевого носителя, на котором хранятся ключ ЭП и (или) СКП ЭП;
- блокировка доступа к ключу ЭП, вызванная неоднократным вводом некорректного кода доступа (пароля или PIN-кода);
- физическая утрата ключевого носителя.

3. Основные меры безопасности для владельцев СКП ЭП, направленных на избежание указанных рисков

3.1. Порядок получения сертифицированных средств ЭП

3.1.1. Путем скачивания дистрибутива средства ЭП из точки распространения на

Интернет-ресурсе производителя или магазинов приложений RuStore, GooglePlay, AppStore, Huawei App Gallery. Такой способ получения средства электронной подписи является легальным только в отношении тех средств ЭП, распространение которых через сеть Интернет согласовано с ФСБ России.

3.1.2. На устанавливающих средствах ЭП носителях информации. Распространение устанавливающих средств ЭП носителей осуществляется лицами, имеющими лицензию ФСБ России на выполнение соответствующих видов работ и оказание услуг в отношении шифровальных (криптографических) средств.

3.2. Требования по размещению средств вычислительной техники с установленными средствами ЭП

3.2.1. При размещении стационарных средств вычислительной техники (далее – СВТ) с установленными на них средствами ЭП должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых размещены данные СВТ.

3.2.2. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны выполняться, исходя из необходимости создания условий для обеспечения сохранения конфиденциальности используемых ключей ЭП и иной конфиденциальной информации.

3.3. Требования к общесистемному и специальному программному обеспечению

3.3.1. На СВТ, предназначенных для работы со средствами ЭП, необходимо использовать только лицензионное программное обеспечение (далее – ПО).

3.3.2. На СВТ с установленными средствами ЭП не должны использоваться средства разработки ПО и отладчики.

3.3.3. Не допускается установка операционных систем (далее – ОС), не предусмотренных документацией на средства ЭП либо измененных или отладочных версий ОС, указанных в документации;

- не допускается установка программных средств, реализующих функции удаленного управления, администрирование, модификацию ОС и ее настроек, а также среды разработки;

- не допускается установка нескольких ОС;

- неиспользуемые ресурсы СВТ должны быть отключены (протоколы, сервисы и т.п.);

- реализованные на СВТ режимы безопасности должны быть настроены на максимальный уровень;

- зарегистрированным пользователям СВТ назначаются минимально возможные для нормальной работы права;

- предоставление минимальных прав доступа к ресурсам СВТ, включая доступ к системному реестру, файлам и каталогам, временным файлам, файлам подкачки и т.п.

3.3.4. Программное обеспечение, устанавливаемое на СВТ с установленным средством ЭП, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;

- модифицировать собственный код и код других программ;

- модифицировать память, выделенную для других программ;

- передавать управление в область собственных данных и данных других программ;

- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;

- модифицировать настройки ОС;

- использовать недокументированные функции ОС.

3.4. Требования по защите от несанкционированного доступа при эксплуатации средств ЭП

При организации работ по защите ключевой информации от несанкционированного доступа (далее – НСД) необходимо руководствоваться требованиями эксплуатационной документации на соответствующее средство ЭП, а также учитывать следующие общие требования:

3.4.1. Правом доступа к СВТ с установленными средствами ЭП должны обладать только владельцы ключей ЭП, установленных на данных СВТ. Каждый СИО должен быть ознакомлен с настоящим Руководством и документацией на средства ЭП.

3.4.2. На СВТ с установленными средствами ЭП необходимо использовать средства антивирусной защиты.

3.4.3. При использовании средств ЭП необходимо использовать пароли, сформированные в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, а также цифры;
- использование в составе символов пароля специальных символов (@, #, \$, &, *, % и т.п.) позволяет при необходимости значительно увеличить стойкость используемого пароля;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- периодичность смены пароля определяется политикой безопасности, но не должна превышать 1 (одного) календарного года.

3.4.4. Запрещается:

- оставлять без контроля СВТ, на котором установлены средства ЭП, после ввода ключевой информации либо иной конфиденциальной информации;
- использовать несертифицированные средства ЭП;
- вносить какие-либо изменения в ПО средств ЭП;
- осуществлять несанкционированное копирование ключевой информации;
- разглашать содержимое ключевой информации или передавать ключевые носители посторонним лицам, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, в отношении которого в ПУЦ зарегистрировано заявление об аннулировании.

3.4.5. Необходимо своевременно устанавливать обновления ОС и антивирусного ПО, в том числе и обновления баз данных антивирусного ПО.

3.4.6. При подключении СВТ с установленными средствами ЭП к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

3.4.7. При использовании средств ЭП на СВТ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых ОС, к ПО, в окружении которого функционируют средства ЭП, и к компонентам средств ЭП со стороны указанных сетей, рекомендуется использовать дополнительные методы и средства защиты (например, установка межсетевых экранов и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

3.4.8. Перед началом работы со средствами ЭП необходимо изучить настоящее Руководство и эксплуатационную документацию на средства ЭП.

3.4.9. Ответственность за обеспечение конфиденциальности PIN-кода и ключа ЭП возлагается на владельца ключа ЭП.

3.5. Требования по защите от несанкционированного доступа к ключевой информации при использовании ключевых носителей

3.5.1. Создаваемые ключи ЭП должны записываться на ключевые носители, имеющее подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности. Не допускается

хранение на носителе ключевой информации любой иной информации (в том числе рабочих или личных файлов). Типы ключевых носителей, которые поддерживаются применяемым средством ЭП, устанавливаются согласно технической и эксплуатационной документации на средство ЭП.

3.5.2. После получения ключевого носителя (типа eToken, JaCarta, Рутокен и т.п.) пользователь должен произвести смену предустановленных на нем PIN-кодов пользователя и администратора, используемых для аутентификации. Значения предустановленных PIN-кодов указаны в эксплуатационной документации на соответствующий ключевой носитель.

3.5.3. PIN-коды должны состоять не менее чем из 8 символов. Символы могут включать в себя как буквы и цифры, так и знаки препинания и т.п.

3.5.4. В ходе эксплуатации ключевого носителя рекомендуется производить смену действующих PIN-кодов с периодичностью, не превышающей 6 календарных месяцев.

3.5.5. Ключевые носители должны использоваться только владельцем ключа ЭП, размещенного на ключевом носителе, и храниться в нерабочие периоды времени в месте, исключающем возможность его бесконтрольного использования. В частности, одним из способов контроля сохранности ключей ЭП, содержащегося на ключевом носителе, является его хранение в сейфе (металлическом шкафу, колбе), опечатываемом личной печатью владельца ключа ЭП (владельца ключевого носителя).

3.5.6. Ответственность за обеспечение конфиденциальности PIN-кода и ключа ЭП возлагается на владельца ключа ЭП.

4. Действия при компрометации ключей ЭП

4.1. СИО самостоятельно должен определить факт компрометации ключа ЭП, оценить значение такого события и выполнить мероприятия по локализации последствий компрометации ключа ЭП.

4.2. При компрометации ключа ЭП СИО должен немедленно инициировать мероприятия по аннулированию СКП ЭП в соответствии с требованиями Регламента ПУЦ.