

Правила по обеспечению безопасности TLS-ключей

1. Общие положения

Правила по обеспечению безопасности TLS-ключей (далее – Правила) предназначены для информирования владельцев TLS-сертификатов, выдаваемых Удостоверяющим центром АО «Россельхозбанк», о рисках, условиях и правилах применения TLS-ключей и СКЗИ, а также о мерах, необходимых для обеспечения безопасности TLS-ключей и СКЗИ.

При использовании в правоотношениях TLS-ключей, эксплуатации СКЗИ СИО 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 СКЗИ;
- Регламента Удостоверяющего центра АО «Россельхозбанк»;
- настоящих Правил.

2. Риски, связанные с использованием TLS-ключей

К основным рискам, связанным с использованием TLS-ключей, относятся:

2.1. Несанкционированный доступ (далее – НСД) к проведению операций с ЦР, который может быть осуществлен в результате компрометации TLS-ключа;

2.2. Негативные последствия, вызванные невозможностью доступа к операциям с ЦР, обусловленной следующими событиями:

- уничтожение (удаление с ключевого носителя) TLS-ключа и (или) TLS-сертификата;
- неисправность ключевого носителя, на котором хранятся TLS-ключ и (или) TLS-сертификат;
- блокировка доступа к TLS-ключу, вызванная неоднократным вводом некорректного пароля к хранилищу криптографических ключей в Программном модуле Банка России (далее – хранилище криптографических ключей), кода доступа к ключевому носителю;
- физическая утрата ключевого носителя.

3. Основные меры безопасности для владельцев TLS-сертификатов, направленных на избежание указанных рисков

3.1. Требования к общесистемному и специальному программному обеспечению.

3.1.1. На ключевых носителях необходимо использовать только лицензионное программное обеспечение (далее – ПО).

3.1.2. На ключевых носителях не должны использоваться средства разработки ПО и отладчики.

3.1.3. Не допускается установка операционных систем (далее – ОС), не предусмотренных эксплуатационной документацией на СКЗИ, либо измененных или отладочных версий ОС;

- не допускается установка программных средств, реализующих функции удаленного управления, администрирования, модификации ОС и ее настроек, а также среды разработки;
- не допускается установка нескольких ОС;
- неиспользуемые ресурсы ключевых носителей должны быть отключены (протоколы, сервисы и т.п.);
- реализованные на ключевых носителях режимы безопасности должны быть настроены на максимальный уровень;
- пользователям ключевых носителей назначаются минимально возможные для нормальной работы права.

3.1.4. Программное обеспечение, устанавливаемое на ключевые носители, 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.

3.2. Требования по защите от несанкционированного доступа при эксплуатации СКЗИ.

При организации работ по защите ключевой информации от НСД необходимо руководствоваться требованиями эксплуатационной документации на СКЗИ, а также учитывать следующие общие требования:

3.2.1. Правом доступа к ключевым носителям должны обладать только владельцы TLS-сертификатов. Каждый СИО должен быть ознакомлен с настоящими Правилами и эксплуатационной документацией на СКЗИ.

3.2.2. На ключевых носителях необходимо использовать средства антивирусной защиты.

3.2.3. Операции с хранилищем криптографических ключей, требующие обращения к TLS-ключам СИО, должны быть защищены паролем. Пароль к хранилищу криптографических ключей должен задаваться СИО при первом обращении к программному модулю Банка России. Длина пароля должна быть не менее 8 и не более 32 символов, и может содержать латинские буквы в верхнем и нижнем регистре, цифры и спецсимволы: | \ / . , < > ; " ' { } [] _ - = + () * & ? ^ % \$ # @ ! ` ~. Срок действия пароля — 6 календарных месяцев.

3.2.4. Запрещается:

- оставлять без контроля ключевые носители после ввода пароля от хранилища криптографических ключей либо иной конфиденциальной информации;
- использовать несертифицированные СКЗИ;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять копирование ключевой информации, содержащейся на ключевом носителе;
- разглашать содержимое ключевой информации, пароли к хранилищу криптографических ключей, коды доступа к ключевому носителю или передавать ключевые носители посторонним лицам, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать TLS-ключ, связанный с TLS-сертификатом, в отношении которого в УЦ РСХБ зарегистрировано заявление об аннулировании.

3.2.5. Необходимо своевременно устанавливать обновления ОС и антивирусного ПО,

в том числе и обновления баз данных антивирусного ПО.

3.2.6. При подключении ключевых носителей 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.

3.2.7. При использовании ключевых носителей, подключенных к общедоступным сетям связи, с целью исключения возможности НСД к системным ресурсам используемых ОС, к ПО, в окружении которого функционируют ключевые носители, и к компонентам ключевых носителей со стороны указанных сетей, рекомендуется использовать дополнительные методы и средства защиты.

3.2.8. Перед началом работы со СКЗИ необходимо изучить настоящие Правила и эксплуатационную документацию на СКЗИ.

3.2.9. Ответственность за обеспечение конфиденциальности ключевой информации, паролей к хранилищу криптографических ключей и кодов доступа к ключевому носителю возлагается на владельца TLS-сертификата.