



**Руководство по обеспечению безопасности использования
усиленной квалифицированной электронной подписи и
средств электронной подписи**

Версия 1

Москва 2024

ИСТОРИЯ ВЕРСИЙ	
Версия №	Дата и № Приказа\Распоряжения
№ 1	04.12.2024 № 4715

Оглавление

1. Общие положения	4
2. Требования по обеспечению безопасности использования квалифицированной ЭП и средств ЭП	4

1. Общие положения

Настоящее руководство (далее - Руководство) подготовлено в соответствии с частью 4 статьи 18 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон) и предназначено для официального информирования владельцев квалифицированных сертификатов ключей проверки электронной подписи (далее – квалифицированный сертификат), выдаваемых аккредитованным удостоверяющим центром Акционерного общества «АЛЬФА-БАНК» (далее - АУЦ), о рисках, условиях и правилах применения усиленной квалифицированной электронной подписи (далее – квалифицированная ЭП) и средств электронной подписи (далее – средства ЭП), а также о мерах, необходимых для обеспечения безопасности использования квалифицированной ЭП и средств ЭП.

Определения понятий «электронная подпись», «средство электронной подписи» содержатся в статье 2 Федерального закона. Признаки квалифицированной ЭП содержатся в ч.3 и 4 ст.5 Федерального закона.

При использовании в правоотношениях квалифицированной ЭП, использовании и эксплуатации средств ЭП владельцы квалифицированных сертификатов и средств квалифицированной 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;
- правил пользования средствами ЭП;
- настоящего Руководства.

2. Требования по обеспечению безопасности использования квалифицированной ЭП и средств ЭП

2.1. Требования к средствам ЭП.

Для создания и проверки квалифицированной ЭП необходимо использовать только средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируются средства ЭП;
- вносить любые изменения в программное обеспечение средств ЭП;
- обрабатывать на вычислительных средствах, оснащённых средствами ЭП, информацию, содержащую государственную тайну.

2.2. Меры защиты ключей ЭП.

Создаваемые ключи квалифицированной ЭП должны записываться на ключевые носители (далее – КН). Типы КН устанавливаются согласно правилам пользования средствами ЭП.

Ключи квалифицированной ЭП, содержащиеся на КН, рекомендуется защищать паролем (ПИН-кодом).

Ответственность за обеспечение конфиденциальности пароля (ПИН-кода) и ключа квалифицированной ЭП возлагается на владельца ключа квалифицированной ЭП.

2.3. Обращение с ключами ЭП и ключевыми носителями.

Размещение ключей ЭП на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами ЭП, не является безопасным, в связи с тем, что это создает предпосылки для совершения несанкционированных или преступных действий неуполномоченными лицами.

КН должны использоваться только владельцем ключа ЭП, размещенного на КН, и храниться в нерабочие периоды времени в месте, исключающем возможность его бесконтрольного использования. В частности, одним из способов контроля сохранности ключей ЭП, содержащегося на КН является хранение КН в сейфе (металлическом шкафу, колбе).

В целях минимизации случаев компрометации ключа ЭП, содержащегося на КН, рекомендуется вставлять носитель в считывающее устройство только в необходимых случаях, а именно на период выполнения операций формирования и проверки квалифицированной ЭП. В прочее время КН рекомендуется изымать из считывателя в целях исключения риска несанкционированного доступа к КН и его содержимому третьими лицами.

Запрещается:

- передавать КН с записанными на него ключами ЭП третьим лицам;
- сообщать ПИН - код к КН третьим лицам;
- записывать ПИН - код к КН на корпусе КН или запоминать его в программах;
- хранить ПИН – код к КН в одном месте с КН;
- записывать на КН постороннюю информацию;
- осуществлять несанкционированное копирование ключей ЭП;
- оставлять КН без присмотра или хранить его в месте, доступном для третьих лиц.

2.4. Владелец квалифицированного сертификата ключа проверки электронной подписи обязан:

- обеспечить конфиденциальность ключа ЭП;
- перед началом работы с КН, проверить штатное функционирование антивирусного программного обеспечения, убедиться в наличии и при необходимости обеспечить своевременную установку обновлений операционной системы и прикладных программ;
- принять меры по исключению несанкционированного доступа в помещения посторонних лиц, в которых размещены вычислительные средства с установленным средством ЭП;
- применять для формирования квалифицированной ЭП только действующий ключ ЭП;
- не использовать ключ ЭП и немедленно обратиться в АУЦ для прекращения действия квалифицированного сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- не использовать ключ ЭП, связанный с квалифицированным сертификатом, заявление, на прекращение действия которого подано в Удостоверяющий центр;

- осуществлять контроль сроков действия квалифицированного сертификата. При необходимости получения нового квалифицированного сертификата Владелец сертификата имеет право обратиться в любой аккредитованный удостоверяющий центр в порядке, установленном соответствующим аккредитованным удостоверяющим центром.

2.5. Компрометация ключа ЭП.

Под компрометацией ключа ЭП понимается утрата доверия к тому, что используемые ключи ЭП обеспечивают безопасность информации. Компрометация ключей ЭП происходит, как правило, вследствие событий:

- потеря КН либо потеря КН с их последующим обнаружением;
- получение доступа к ключам ЭП неуполномоченных лиц;
- нарушение правил уничтожения ключей ЭП;
- подозрения на утечку информации или её искажение в системе конфиденциальной связи;
- нарушение работоспособности КН при допущении условия возможных несанкционированных воздействий на носитель.

В первых четырех случаях компрометация ключа ЭП носит явный характер и реагирование в этих случаях должно заключаться в немедленном обращении владельца ключа ЭП в АУЦ для прекращения действия квалифицированного сертификата. Контакты АУЦ: телефон - +7 (495) 620-91-91; e-mail - samail@alfabank.ru.

Прочие случаи должны рассматриваться и анализироваться в индивидуальном порядке. Использование ключа ЭП может быть продолжено только в случаях обоснованной уверенности в сохранении свойств безопасности ключа ЭП.

Процедура смены ключей ЭП и получения новых квалифицированных сертификатов осуществляется в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и Порядком реализации функции АУЦ и исполнении его обязанностей.