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

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи

1.1. Обеспечить конфиденциальность ключей электронных подписей.

1.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

1.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

1.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

1.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.

1.8. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

2. Порядок применения средств квалифицированной электронной подписи

2.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.

3. Не допускается:

3.1. Разглашать содержимое носителей ключевой информации, выводить ключевую информацию на дисплей и принтер.

3.2. Передавать пароли и сами носители ключевой информации лицам, к ним не допущенным.

3.3. Записывать на ключевой носитель постороннюю информацию.

3.4. Использовать ключевые носители, не предусмотренные эксплуатационной документацией на средства электронной подписи.

3.5. Вносить какие-либо изменения в программное обеспечение средств электронной подписи.

4. **Настоятельно рекомендуется:**

4.1. Для хранения носителей ключевой информации в помещениях использовать надежные хранилища (например, сейфы), оборудованные надежными запирающими устройствами. Режим хранения должен исключать возможность несанкционированного доступа к ним.

4.2. Для исключения утраты ключевой информации вследствие дефектов носителя рекомендуется использовать дополнительный носитель для создания резервной копии ключевой информации.