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

Настоящее руководство предназначено для обязательного ознакомления Пользователей Удостоверяющего центра Ханты-Мансийского автономного округа – Югры, использующих средства квалифицированной электронной подписи.

1. Термины и определения

Квалифицированный сертификат ключа проверки электронной подписи - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном порядке выдан сертификат ключа проверки электронной подписи;

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

2. Обязанности владельца ключа квалифицированной электронной подписи:

2.1. Обеспечить конфиденциальность ключа квалифицированной электронной подписи.

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

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

2.4. Применять ключ квалифицированной электронной подписи с учетом ограничений, содержащихся в квалифицированном сертификате, если такие ограничения были установлены.

2.5. Немедленно обратиться в удостоверяющий центр с заявлением на прекращение действия квалифицированного сертификата в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

2.7. Не использовать ключ квалифицированной электронной подписи, заявление на прекращение действия (отзыв) которого подано в удостоверяющий центр.

2.8. Не использовать ключ квалифицированной электронной подписи, связанный с квалифицированным сертификатом, который аннулирован или действие которого прекращено.

2.9. Не передавать ключевые носители, содержащие ключи проверки электронной подписи, лицам, к ним не допущенным, не выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации.

2.10. Не вносить какие – либо изменения в программное обеспечение и средства усиленной квалифицированной электронной подписи.
2.11. Не оставлять без контроля ключевые носители, содержащие ключи проверки электронной подписи.
2.12. Не оставлять без контроля вычислительные средства, на которых эксплуатируется средства усиленной квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации.
2.15. Не осуществлять несанкционированное администратором безопасности копирование ключевых носителей.
2.16. Не записывать на ключевые носители постороннюю информацию.
2.17. Сдать средства квалифицированной электронной подписи и ключи электронной подписи, эксплуатационную и техническую документацию к ним в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи;

3. Порядок применения средств квалифицированной электронной подписи.
3.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.
3.2. Для предотвращения заражения компьютера с установленными средствами усиленной квалифицированной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.
3.3. Помещения, в которых установлены средства квалифицированной электронной подписи или хранятся носители ключей электронной подписи должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.
3.4. Используемые или хранимые средства квалифицированной электронной подписи, эксплуатационная и техническая документация к ним, носители ключей проверки электронной подписи подлежат учету в соответствии с требованиями Приказа ФАПСИ от 13 июня 2001 г. № 152.