РУКОВОДСТВО
по обеспечению безопасности использования усиленной квалифицированной электронной подписи и средств усиленной квалифицированной электронной подписи

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи (далее – квалифицированный сертификат).

1.1. Обеспечить конфиденциальность ключей электронных подписей.

1.2. Применять для формирования усиленной квалифицированной 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 квалифицированном сертификате (в расширениях Extended Key Usage, Application Policy квалифицированного сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

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

1.6. Не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, заявление на прекращение действия которого подано в удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия квалифицированного сертификата в удостоверяющий центр по момент времени официального уведомления о прекращении действия квалифицированного сертификата.

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

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

2. Порядок применения средств усиленной квалифицированной электронной подписи.

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

2.2. 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.

2.3. В организации должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств усиленной квалифицированной электронной подписи, назначены владельцы средств усиленной квалифицированной электронной подписи и должностные лица, ответственные за обеспечение безопасности информации и эксплуатации этих средств.

2.4. Помещения, в которых установлены средства усиленной квалифицированной электронной подписи или хранятся носители ключей электронной подписи должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

2.5. В помещениях пользователей средств усиленной квалифицированной электронной подписи для хранения выданных им носителей ключей электронной подписи, эксплуатационной и технической документации, инсталлирующих средства усиленной квалифицированной электронной подписи носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей средств усиленной квалифицированной электронной подписи.

2.6. Используемые или хранимые средства усиленной квалифицированной электронной подписи, эксплуатационная и техническая документация к ним, носители ключей электронной подписи подлежат поэкземплярному учету в соответствии с требованиями Приказа ФАПСИ от 13 июня 2001 г. № 152 "Об утверждении 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".