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

1. Риски, возникающие при использовании электронной подписи.

Владелец сертификата ключа проверки электронной подписи (далее СКПЭП) может подвергнуться следующим рискам при использовании электронной подписи:

1.1. Несанкционированное подписание документа электронной подписью (события: компрометация ключа электронной подписи, подмена документа при подписании);
1.2. Невозможность подписания документа электронной подписью (события: физическая неисправность/утрата ключевого носителя, блокировка доступа к ключевому носителю или уничтожение с него ключа электронной подписи);
1.3. Отказ владельца СКПЭП от своей электронной подписи или информации, подписанной этой электронной подписью (события: использование несертифицированных средств электронной подписи или установка сертифицированных средств электронной подписи из недоверенных источников).

2. Меры по обеспечению безопасности использования электронной подписи и средств электронной подписи.

Для предотвращения событий, которые могут повлечь вышеуказанные риски, необходимо выполнение владельцем СКПЭП следующих организационно-технических мер:

2.1. Использовать для штатной работы с квалифицированной электронной подписью только сертифицированные средства электронной подписи, полученные на инсталлирующих носителях в организациях-лицензиатах ФСБ или загруженные с интернет-ресурса с обязательной проверкой контроля целостности дистрибутива.
2.2. Размещать технические средства с установленными средствами электронной подписи в помещениях (местах), исключающих несанкционированный доступ в эти помещения посторонних лиц.
2.3. Использовать на технических средствах, предназначенных для работы со средствами электронной подписи, только лицензионное программное обеспечение фирм-изготовителей.
2.4. Использовать на технических средствах, предназначенных для работы со средствами электронной подписи, средства антивирусной защиты с актуальными базами вирусов и средства сетевой безопасности.
2.5. Обеспечить контроль целостности аппаратной части технических средств с установленными средствами электронной подписи (например, путем опечатывания).
2.6. Определить лиц, обладающих правом доступа к техническим средствам с установленными средствами электронной подписи. Организовать ознакомление этих лиц с эксплуатационной документацией на средства электронной подписи и с настоящим руководством.
2.7. Применять политику назначения и смены сложных паролей (длина не менее 8 символов, спецсимволы и цифры в различных регистрах, периодичность смены и т.п.) для входа в операционную систему и базовую систему ввода/вывода (BIOS).
2.8. Исключить использование PIN-кодов «по умолчанию» к носителям, содержащим ключ электронной подписи.
2.9. Исключить использование ключа электронной подписи без письменного согласия (делегирования полномочий) владельца СКПЭП.
2.10. Исключить несанкционированное копирование ключа электронной подписи, в том числе создание неучтенных копий.
2.11. Сохранять в тайне сведения, предоставленные удостоверяющим центром для удаленной идентификации владельца СКЭП в случае компрометации ключа электронной подписи.
2.12. Незамедлительно сообщать в удостоверяющий центр о фактах компрометации ключа электронной подписи в соответствии с порядком, предусмотренном в Регламенте удостоверяющего центра.

Безопасность использования электронной подписи и средств электронной подписи должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.