Использование усиленной электронной подписи предусматривает работу с криптографическими средствами и ключами для них. Безопасность использования криптографических методов в значительной мере основывается на конфиденциальности носителей, содержащих криптографические ключи, и обеспечении доверенной компьютерной среды, в которой функционирует криптографическое средство.

В соответствии с Федеральным законом Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи» владелец квалифицированного сертификата ключа проверки электронной подписи (далее — квалифицированный сертификат), изготовленного аккредитованным Удостоверяющим центром InfoTrust ООО НПП «Ижинформпроект», обязан соблюдать следующие требования по обеспечению безопасности использования электронной подписи и средств электронной подписи.

1 Для обеспечения безопасности использования квалифицированной электронной подписи нужно следующее.

1.1 Обеспечить конфиденциальность ключей электронной подписи.

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 квалифицированном сертификате ключа проверки электронной подписи (расширения Extended Key Usage, Application Policy, Certificate Policies сертификата), если такие ограничения были установлены.

1.5 Немедленно обратиться в Удостоверяющий центр InfoTrust с заявлением об аннулировании (прекращении действия/отзыве) сертификата в случае нарушения (или подозрения в нарушении) конфиденциальности ключа электронной подписи (компрометация ключа).

1.6 Не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, заявление об аннулировании которого подано в Удостоверяющий центр InfoTrust, в течение времени, исчисляемого с момента времени подачи заявления в Удостоверяющий центр InfoTrust по момент времени официального уведомления об аннулировании сертификата, либо об отказе в аннулировании.

1.7 Не использовать ключ электронной подписи, связанный с сертификатом, который аннулирован.

1.8 Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в установленном в Российской Федерации порядке средства электронной подписи.

1.9 Соблюдать требования Регламента удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект», в том числе обеспечить защиту от несанкционированного доступа своего мобильного абонентского устройства и/или идентификационного модуля при использовании персонального абонентского номера подвижной (мобильной) связи для удаленной идентификации и получения одноразовых паролей, отправляемых в коротких текстовых сообщениях.

2 Для обеспечения безопасности использования средств электронной подписи необходимо следующее.

2.1 Сертифицированные средства электронной подписи должны применяться владельцем квалифицированного сертификата в соответствии с требованиями технической и эксплуатационной документации на применяемые средства электронной подписи. В том числе, должны соблюдаться следующие требования:

— обеспечение защиты компьютера от несанкционированного доступа путем настройки политики безопасности, установки дополнительных сертифицированных средств защиты от несанкционированного доступа, установки лицензионного программного обеспечения, полученного из надежных источников и не содержащего средств разработки и отладки программ, своевременной установки обновлений безопасности для него, удаление/отключение средств удаленного доступа и администрирования;

— соблюдение правил безопасной работы в сети Интернет и обеспечение непрерывной комплексной защиты компьютера от вирусов, атак, спама, шпионского программного обеспечения и других вредоносных программ при подключении к сетям передачи данных путем установки антивирусных программ, средства обнаружения вторжений и персонального межсетевого экрана с периодическим обновлением их баз данных решающих правил;

— установка надежных (не менее 6 символов, использование букв, цифр и спецсимволов) паролей к ключевым носителям, системе конфигурирования компьютера (BIOS/UEFI), учетной записи и экранной заставке операционной системы, обеспечение их регулярной смены.

2.2 Должны соблюдаться требования нормативных актов регуляторов, в том числе приказа ФАПСИ от 13.06.2001 № 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»:

— поэкземплярный учет средств электронной подписи, эксплуатационной и технической документации к ним, носителей ключей электронной подписи;

— безопасный порядок изготовления, санкционированного копирования, выбор отчуждаемых защищенных носителей ключей электронной подписи и защищенных мест их хранения;

— обеспечение контроля вскрытия компьютеров с установленными средствами электронной подписи;

— безопасное размещение, специальное оборудование, охрана и организация режима в помещениях с установленными средствами электронной подписи и мест хранения носителей ключей электронной подписи.

Подробная информация содержится в документах аккредитованного Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект»:
— Положение о порядке использования средств криптографической защиты информации и ключевой информации к ним;
— Требования по обеспечению безопасности автоматизированного рабочего места;
— Памятка пользователю средств криптографической защиты информации;
— Памятка пользователю Удостоверяющего центра InfoTrust.