Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Условия и порядок использования электронной подписи и средств электронной подписи

Организация электронного взаимодействия с использованием ЭП (далее – ЭП) осуществляется с учетом требований: ФЗ №63 «Об ЭП», ФЗ №149 «Об информации, информационных технологиях и о защите информации», Инструкции ФАПСИ № 152, руководящих документов ФСТЭК России и ФСБ России, эксплуатационной и технической документации на используемые средства электронной подписи (далее – средства ЭП), средства криптографической защиты информации (далее также – СКЗИ).

2. Риски, связанные с использованием ЭП и средств ЭП:

– риски, связанные с аутентификацией (подтверждением подлинности) пользователя.

– риски, связанные с отрекаемостью (отказом от содержимого документа).

– риски, связанные с юридической значимостью ЭП.

– риски, связанные с несоответствием условий использования ЭПустановленному порядку.

– риски, связанные с нарушением конфиденциальности ключей ЭП (использование ключей ЭП без согласия владельца).

– риски, связанные с несовместимостью средств ЭП, используемых сторонами для организации электронного взаимодействия.

– риски, связанные с определением полномочий лица, подписавшего электронной подписью документ.

– риски, связанные с использованием сертификатов ключей проверки ЭП и ключей ЭП, прекративших своё действие.

3. Меры, необходимые для обеспечения безопасности при использовании ЭП.

3.1 Должны быть предусмотрены организационные и организационно-технические мероприятия, направленные на обеспечение информационной безопасности прииспользовании средств ЭП и определяющие требования к ответственным лицам, автоматизированным рабочим местам пользователей СКЗИ (далее также - АРМ), системному и прикладному программному обеспечению, условиямхранения и использования средств ЭП, ключей ЭПи ключевых носителей.

3.2 Должны быть определены лица, ответственные за осуществление электронного взаимодействии с использованием ЭП и имеющие доступ к ключевым носителям, а также лица, ответственные за организацию работ по защите информации и соблюдению условий хранения и использования ключей ЭП и средств ЭП.

3. 3 В помещения, в которых расположены АРМ, предназначенные для работы со средствами ЭП (далее – спецпомещения), должн быть исключен бесконтрольный допуск лиц, не допущенных к работе в указанных спецпомещениях.

3.4 Не допускается оставлять без контроля АРМ при включенном питании и подключенными ключевыми носителями. Перед уходом пользователь СЗКИ должен выключить АРМ либо заблокировать рабочую станцию.

3.5 На технических средствах АРМ с установленными средствами ЭП необходимо использовать только лицензионное ПО,полученное из доверенных источников. Не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

3.6 Рекомендуется ограничить права пользователя АРМ по самостоятельной установке программного обеспечения и настроить возможность выполнения пользователем АРМ только тех приложений, которые разрешены администратором информационной безопасности.

3.7 Необходимо регулярно отслеживать и устанавливать обновления безопасности для операционной системы, программного обеспечения АРМ, регулярно осуществлять обновление антивирусных баз.

3.8 Рекомендуется разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, доступа к ключам ЭП).

3.9 Установка и настройка средств ЭП (СКЗИ) должна выполняться администратором информационной безопасности либо лицом,ответственным за работоспособность.

3.10 Использование средств ЭП должно осуществляться в соответствии с эксплуатационной документацией и инструкциями на средства ЭП.

3.11 Подключение к Интернет рекомендуется производить с использованием сертифицированного межсетевого экрана, настроенного в соответствии с требованиямиэксплуатационной документации на средства межсетевого экранирования.

3.12 При использовании и хранении ключей ЭП должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации (ключевых носителей), содержащих ключи ЭП, которыйдолжен исключать возможность несанкционированного доступа к ним.

3.13 Хранить ключевые носители рекомендуется в сейфах.

3.14 В качестве ключевых носителей рекомендуется использовать сертифицированные ключевые носители USB-ключи и смарт- карты.

3.15 При хранении и использовании ключей ЭП пользователю СКЗИ запрещается:

– выполнять копирование ключа ЭП на иные ключевые носителибез разрешения администратора информационной безопасности;

– знакомить с содержанием ключевых носителей или передавать ключевые носители иным лицам;

– устанавливать ключевой носитель в другие АРМ, не предназначенные для работыс ключевой информацией;

– записывать на ключевой носитель постороннюю информацию;

– использовать ранее использовавшиеся ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации с использованием сертифицированных средств ЭП либо средств, гарантирующих практическую невозможность восстановления информации с ключевыхносителей.

3.16 Владелец ключа ЭП (владелец сертификата) обязан:

– хранить в тайне ключ ЭП;

– немедленно обратиться в удостоверяющий центр для приостановления действия сертификата ключа проверки ЭП или его отзыва в случае компрометации ключа ЭП или при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

– не использовать ключ проверки ЭП, связанный с сертификатомключа проверки ЭП, который отозван или действие которого приостановлено.

3.17 Действия, связанные с хранением и эксплуатацией средств ЭПи ключей ЭП, должны фиксироваться в журналах поэкземплярного учета, ведение которого осуществляется в соответствии с Инструкцией ФАПСИ № 152.