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

1. Организационное обеспечение безопасности использования квалифицированной электронной подписи (далее – КЭП) и средств КЭП

1.1. Участники электронного взаимодействия назначают (определяют) перечень должностных лиц, ответственных за обеспечение безопасности использования КЭП и средств КЭП, разрабатывают и утверждают организационно-распорядительные документы, регламентирующие вопросы безопасности использования КЭП и средств КЭП.

1.2. Участники электронного взаимодействия допускают к использованию КЭП и средств КЭП лиц, имеющих навыки работы на персональном компьютере, прошедших обучение и (или) ознакомленных с правилами использования КЭП и средств КЭП.

1.3. Соответствующими приказами по организации должны быть утверждены нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств КЭП, назначены владельцы ключей КЭП и соответствующих им квалифицированных сертификатов (далее – владельцы КЭП), а также должностные лица, ответственные за обеспечение безопасности информации и эксплуатацию указанных средств.

1.4. Требования к хранению и учету средств КЭП и ключевых носителей КЭП определены в разделе III «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации», утвержденной Приказом ФАПСИ при Президенте РФ от 13.06.2001 г. № 152 (далее – «Инструкция-152»).

1.5. Требования к качеству криптографической защиты информации конфиденциального характера определены пунктами 11, 12 «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденном Приказом ФСБ России от 09.02.2005 г. № 66.

2. Обеспечение безопасности помещений, в которых хранятся ключевые носители и эксплуатируются средства КЭП

Требования к помещениям, в которых хранятся ключевые носители и эксплуатируются средства КЭП, определены в разделе IV «Инструкции-152».

3. Обеспечение безопасности ключевой информации

3.1. Владелец КЭП обязан обеспечить конфиденциальность ключей КЭП, в том числе:

– после получения ключевого носителя из удостоверяющего центра (далее – УЦ) изменить назначенный по умолчанию PIN-код, который должен содержать не менее 8-и символов случайной цифровой последовательности;

– хранить персональный ключевой носитель в запираемом и опечатываемом хранилище (сейф, ящик, шкаф и т.п.);

– применять для формирования КЭП только действующий ключ КЭП. При подписании электронного документа КЭП, срок действия которой истек, данный документ может быть признан недействительным;

– в течение не более чем одного рабочего дня обратиться в УЦ с заявлением на прекращение действия квалифицированного сертификата в случае компрометации ключа КЭП. Под компрометацией ключей КЭП понимается

хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых указанные ключи могут стать доступными несанкционированным лицам и (или) процессам;

– применять ключ КЭП с учетом ограничений, содержащихся в соответствующем квалифицированном сертификате, если таковые ограничения были установлены;

– выполнить условия, обеспечивающие при эксплуатации и транспортировке ключевых носителей защиту от компрометации, физических повреждений и внешнего воздействия на записанную ключевую информацию;

– уничтожение выведенных из действия ключей КЭП осуществлять в порядке, определенном пунктом 42 «Инструкции-152».

3.2. Владельцу КЭП запрещается:

– передавать персональный ключевой носитель и сообщать PIN-код доступа к нему, а также оставлять персональный ключевой носитель и PIN-код доступа к нему без присмотра;

– осуществлять несанкционированное копирование ключей КЭП;

– использовать ключ КЭП, заявление на прекращение (приостановление) действия квалифицированного сертификата которого подано в УЦ, с момента времени подачи соответствующего заявления в УЦ;

– использовать ключ КЭП, действие которого прекращено или приостановлено;

– применять ключ КЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена (компрометации ключа КЭП);

– пересылать ключевую информацию по электронной почте (запросы на получение сертификатов и сертификаты пересылать допустимо);

– копировать ключевую информацию на локальный диск компьютера, а также в реестр операционной системы;

– вносить какие-либо изменения в средства КЭП и использовать их в режимах, не предусмотренных эксплуатационной документацией.

4. Обеспечение безопасного использования средств КЭП

Владельцу ключа КЭП необходимо:

– использовать в соответствии с эксплуатационной документацией сертифицированные по требованиям обеспечения безопасности информации средства КЭП, средства защиты информации (в том числе средства антивирусной защиты) и лицензионно чистое ПО, полученные из доверенных источников;

– работать под учетной записью пользователя (не администратора) с минимально необходимыми для нормальной работы правами. Защищать вход в учетную запись надежным паролем и хранить его в тайне;

– исключить установку на компьютер ПО удаленного управления (администрирования) компьютером, средств разработки и отладки ПО;

– обеспечить регистрацию событий информационной безопасности и автоматическую блокировку учетной записи при оставлении пользователем персонального компьютера, с установленными средствами КЭП, по истечении временного интервала не превышающего 10 минут.