РУКОВОДСТВО
по обеспечению безопасности использования электронной подписи и средств электронной подписи

Общие положения

Настоящее Руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированным сертификатом ключа проверки электронной подписи (далее – сертификат), об условиях, рисках и порядке использования усиленной квалифицированной электронной подписи (далее – квалифицированная ЭП) и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной ЭП.

При применении квалифицированной ЭП в информационных системах владельцу сертификата необходимо выполнять требования:

- 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, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152, в части обращения со средствами криптографической защиты информации;
- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66, в части эксплуатации средств криптографической защиты информации;
- эксплуатационной документации к средствам электронной подписи;
- приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

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

Риски использования электронной подписи

При использовании электронной подписи существуют определенные риски, основными из которых являются следующие:

- Риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает подпись под документом, может заявить о том, что подпись сфальсифицирована и не принадлежит данному лицу.
- Риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом.
- Риски, связанные с юридической значимостью электронной подписи. В случае судебного разбирательства одна из сторон может заявить о том, что документ с электронной подписью не может порождать юридически значимых последствий или считаться достаточным доказательством в суде.
- Риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.

- Риски, связанные с несанкционированным доступом (использованием электронной подписи без ведома владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

Для снижения данных рисков или их избежания помимо определения порядка использования электронной подписи при электронном взаимодействии предусмотрен комплекс правовых и организационно-технических мер обеспечения информационной безопасности.

Работа со средствами электронной подписи (ЭП)

Пользователи Удостоверяющего центра, осуществляющие работу со средствами электронной подписи, получившие и использующие ключи электронной подписи, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы со средствами ЭП;
- сохранение в тайне содержания средств ЭП;
- сохранность носителей ключевой информации и других документов, выдаваемых с ключевыми носителями;
- сохранение в тайне пин – кодов для доступа к электронным ключам и средствам ЭП;
- самостоятельное удаление информации с электронного ключа;
- самостоятельное проведение инициализации электронного ключа, повлекшее удаление информации с электронного ключа;
- своевременную подачу заявления о прекращении действия сертификата ключа проверки электронной подписи при наличии оснований полагать, что тайна ключа электронной подписи нарушена

Пользователями УЦ должны быть обеспечены соответствующие условия хранения электронных ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования средств ЭП.

Пользователь УЦ так же несет ответственность за то, чтобы на компьютере, на котором установлены средства ЭП, не были установлены и не эксплуатировались программы (в том числе, - вирусы), которые могут нарушить функционирование программных средств и средств ЭП.

При работе с ЭП запрещается:

- осуществлять несанкционированное копирование ключевых контейнеров/носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- вносить какие-либо изменения в программное обеспечение средств квалифицированной ЭП;
- записывать на ключевые носители постороннюю информацию;
- оставлять средства вычислительной техники с установленными средствами квалифицированной ЭП без контроля после ввода ключевой информации;
- использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена (необходимо немедленно обратиться в удостоверяющий центр с заявлением на прекращение действия сертификата в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи);

- использовать ключ электронной подписи и соответствующий сертификат, заявление на прекращение действия которого подано в удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в удостоверяющий центр по момент времени прекращения действия сертификата;
- использовать ключ электронной подписи, связанный с сертификатом, который аннулирован или действие которого прекращено;
- использовать для создания и проверки квалифицированных ЭП, создания ключей электронной подписи и ключей проверки электронной подписи несертифицированные в соответствии законодательством Российской Федерации средства электронной подписи;

Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной ЭП

Ключи квалифицированной ЭП на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной ЭП.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца сертификата.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме ключей проверки ЭП).

Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной ЭП, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной ЭП операций формирования и проверки квалифицированной ЭП, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

С целью контроля исходящего и входящего подозрительного трафика технические средства с установленными средствами квалифицированной ЭП должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования.

На технических средствах, используемых для работы в информационных системах:

- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
- должны быть отключены все неиспользуемые службы и процессы операционной системы (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);
- должны регулярно устанавливаться обновления операционной системы;
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной ЭП и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;

- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной ЭП, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред владельцу сертификата, в том числе средства квалифицированной ЭП, журналы работы систем обмена электронными документами и т.д..