Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

Термины и определения

Владелец сертификата ключа проверки электронной подписи (владелец сертификата) - лицо, которому в установленном Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.
Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи**.**
Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка ЭП).
Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.
Компрометация ключа электронной подписи - утрата доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам или подозрение, что ключи электронной подписи были временно доступны неуполномоченным лицам. К событиям, связанным с компрометацией ключа электронной подписи, относятся (включая, но не ограничиваясь):

- физическая утрата ключевого носителя;
- потеря ключевого носителя с его последующим обнаружением;
- передача ключа электронной подписи по открытым каналам связи;
- перехват ключа электронной подписи вредоносным программным обеспечением;
- несанкционированный доступ постороннего лица к устройству хранения ключа электронной подписи;
- случаи, когда невозможно достоверно установить, что произошло с ключевым носителем (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- сознательная передача ключа электронной подписи постороннему лицу;
- увольнение сотрудников, имевших доступ к ключу электронной подписи;
- нарушение правил хранения ключевой информации.

Конфиденциальная информация - сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их владельца, а также информация, доступ к которой ограничен в соответствии с действующим законодательством РФ.
Несанкционированный доступ к информации - доступ к информации в нарушение должностных полномочий сотрудника или доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.
Плановая смена ключей электронной подписи - смена ключей электронной подписи, производимая в период действия ключей электронной подписи в соответствии с установленной в Удостоверяющем центре периодичностью, не вызванная компрометацией ключей электронной подписи.
Пользователь Удостоверяющего центра (пользователь) – лицо, пользующееся услугами Удостоверяющего центра.
Сертификат ключа проверки электронной подписи (сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи**.**
Список аннулированных (отозванных) сертификатов - списков уникальных номеров сертификатов ключей проверки ЭП, действие которых на определенный момент было прекращено Удостоверяющим центром до истечения их действия.
Средства криптографической защиты информации – аппаратные, программные и аппаратно-программные средства, системы и комплексы, осуществляющие криптографические преобразования информации для обеспечения ее защиты от несанкционированного доступа, от навязывания ложной информации и/или обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи, создание ключей электронной подписи и ключей проверки электронной подписи
Средства электронной подписи (далее - средства ЭП) - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.
Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».
Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.
Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию**.**

1. Риски, связанные с использованием электронной подписи.

К основным рискам, связанным с использованием электронной подписи, относятся:

1.1. Несанкционированное подписание электронного документа электронной подписью, которое может быть произведено в результате:

- компрометации ключа электронной подписи;
- подмены подписываемого документа в результате работы на компьютере вредоносного программного обеспечения.

1.2. Негативные последствия, вызванные невозможностью подписания электронного документа электронной подписью, обусловленной следующими событиями:

- уничтожение (удаление с ключевого носителя) ключа и/или сертификата ключа проверки электронной подписи;
- неисправность ключевого носителя, на котором хранятся ключ и/или сертификата ключа проверки электронной подписи;
- блокировка ключевого носителя, вызванная неоднократным вводом некорректного кода доступа (пароля или ПИН-кода);
- физическая утрата ключевого носителя.

1.3. Риск фальсификации электронной подписи.
Данный риск является скорее гипотетическим, но при использовании несертифицированного средства ЭП или использовании средства ЭП, полученного нелегально, в том числе и не определенным для данного средства способом, может породить следующие реальные риски:

- Риски отказа автора от своей электронной подписи под электронным документом или признания электронной подписи под электронным документом недействительной, которые могут быть аргументированы возможностью подделки электронной подписи при использовании несертифицированных или полученных нелегальным путем средств ЭП (т.е. не обладающих гарантированной криптографической стойкостью).
- Риск отказа автора от содержания подписанного электронной подписью электронного документа, которое может быть аргументировано возможностью модификации подписываемого документа при использовании несертифицированных или полученных нелегальным путем средств ЭП (т.е. обладающего недекларированными возможностями).

В целях снижения рисков, связанных с использованием электронной подписи, необходимо выполнение комплекс организационно-технических и административных мер по обеспечению безопасности использования электронной подписи и средств электронной подписи.

2. Порядок получения сертифицированных средств ЭП.
Возможны два легальных способа получения средств ЭП:
2.1. Путем загрузки дистрибутива средства ЭП из точки распространения на Интернет-ресурсе производителя. Такой способ получения средства электронной подписи является легитимным только в отношении тех средств ЭП, распространение которых через сеть Интернет согласовано с Федеральной службой безопасности РФ. В настоящее время легитимно распространяемым через сеть Интернет средством ЭП является ViPNet CSP.
2.2. На инсталлирующих средства ЭП носителях информации. Распространение инсталлирующих средств ЭП носителей осуществляется организациями, имеющими лицензию Федеральной службы безопасности РФ на выполнение соответствующего вида работ и оказания услуг в отношении шифровальных (криптографических) средств.

3. Организация работ по обеспечению безопасности использования электронной подписи и средств электронной подписи.
3.1. Безопасность использования электронной подписи и средств ЭП должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
3.2. Правом доступа к рабочим местам с установленными средствами ЭП должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Каждый пользователь, применяющий средства ЭП, должен быть ознакомлен с настоящим Руководством и документацией на средства ЭП.

4. Требования по размещению технических средств с установленными средствами ЭП.

При размещении технических средств с установленными на них средствами ЭП:

4.1. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средствами ЭП, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.
4.2. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключи электронной подписи.

5. Требования по установке средств ЭП, а также общесистемного и специального программного обеспечения.

5.1. Установку общесистемного и специального программного обеспечения (далее – ПО), а также средств ЭП, должны осуществлять лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и средство ЭП.
5.2. При установке средств ЭП следует:

- На технических средствах, предназначенных для работы со средствами ЭП, использовать только лицензионное программное обеспечение фирм - изготовителей.
- На компьютере не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода средств ЭП и приложений, использующих средства ЭП, а также для просмотра кода и областей памяти, используемой средствами ЭП, в процессе обработки средствами ЭП информации и/или при загруженной ключевой информации.
- Предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлены средства ЭП (например, путем опечатывания системного блока и разъемов компьютера).
- Программное обеспечение, устанавливаемое на компьютер с установленным средством ЭП, не должно содержать возможностей, позволяющих:
  - модифицировать содержимое произвольных областей памяти;
  - модифицировать собственный код и код других программ;
  - модифицировать память, выделенную для других программ;
  - передавать управление в область собственных данных и данных других программ;
  - несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
  - модифицировать настройки операционной системы (далее – ОС);
  - использовать недокументированные фирмой-разработчиком функции ОС.

6. Требования по защите от несанкционированного доступа при эксплуатации средств ЭП.

При организации работ по защите информации от несанкционированного доступа (далее – НСД) необходимо учитывать следующие требования:

6.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS (basic input/output system) и т.д.), использовать пароли, сформированные в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 года.

6.2. Запрещается:

- оставлять без контроля компьютер, на котором эксплуатируются средства ЭП, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение средств ЭП;
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств ЭП;
- записывать на ключевые носители постороннюю информацию.

6.3. Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.
6.4. Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.
6.5. При подключении компьютера с установленными средствами ЭП к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.
6.6. При использовании средств ЭП на компьютерах, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют средства ЭП, и к компонентам средств ЭП со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.
6.7. Необходимо организовать и использовать комплекс мероприятий антивирусной защиты.
6.8. Необходимо исключить одновременную работу средств ЭП различных производителей.
6.9. К работе со средствами допускаются лица, изучившие настоящее Руководство и пользовательскую документацию на средства ЭП.

7. Действия при компрометации ключей электронной подписи.

7.1. Пользователь самостоятельно должен определить факт компрометации ключа электронной подписи, оценить значение этого события и выполнить мероприятия по розыску и локализации последствий компрометации ключа электронной подписи.

7.2. При компрометации ключа электронной подписи пользователь должен немедленно сообщить в Удостоверяющий центр о факте компрометации. Информация о компрометации должна передаваться в Удостоверяющий центр способом, определенным Регламентом Удостоверяющего центра. По получении информации о компрометации ключа электронной подписи Удостоверяющий центр осуществляет аннулирование сертификата ключа проверки электронной подписи, в результате чего создание действительной электронной подписи с использованием скомпрометированного ключа электронной подписи становится невозможным.