Утверждено
приказом Акционерного общества
«ИнфоТеКС Интернет Траст»
от 14.09.2021 № 40-09/21

Руководство
по порядку использования и обеспечению безопасности использования электронных подписей 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 № 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 ключа электронной подписи (жесткий диск компьютера, смарт-карта, USB-токен, устройство памяти в составе мобильного устройства и т.п.).

Компрометация ключа электронной подписи - нарушение конфиденциальности ключа электронной подписи, связанное с утратой доверия к тому, что используемый ключ электронной подписи недоступен посторонним лицам или подозрением, что ключ электронной подписи был временно доступен посторонним 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 ключевому носителю;
- случаи, когда невозможно достоверно установить, что произошло с ключевым носителем, в том числе случаи выхода ключевого носителя из строя;
- передача ключа электронной подписи постороннему лицу;
- увольнение работников юридического лица, имевших доступ к ключу электронной подписи юридического лица;
- 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 законодательством Российской Федерации.

Сертификат ключа проверки электронной подписи (сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи**.**

Средства вычислительной техники (далее - СВТ) – совокупность программных и технических элементов средств и систем обработки информации, к которым относятся, в частности, стационарные персональные компьютеры, ноутбуки, планшетные компьютеры, смартфоны.

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, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по

созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Усиленная электронная подпись (далее – электронная подпись) - информация в электронной форме, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи, 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**.**

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием СВТ, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

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 электронного документа в результате работы на компьютере или мобильном устройстве вредоносного программного обеспечения.

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

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

1.3. Риск подделки электронной подписи.

Данный риск является скорее гипотетическим, поскольку подбор ключа электронной подписи в целях подделки электронной подписи является задачей практически невыполнимой в связи со сложностью используемых при создании электронной подписи криптографических алгоритмов.

2. Порядок получения сертифицированных средств ЭП.

Возможны два легальных способа получения средств ЭП:

2.1. Путем скачивания дистрибутива средства ЭП из точки распространения на Интернет-ресурсе производителя или магазинов приложений GooglePlay, AppStore, Huawei App Gallery. Такой способ получения средства электронной подписи является легальным только в отношении тех средств ЭП, распространение которых через сеть Интернет согласовано с Федеральной службой безопасности Российской Федерации.

2.2. На инсталлирующих средства ЭП носителях информации. Распространение инсталлирующих средств ЭП носителей осуществляется лицами, имеющими лицензию ФСБ России на выполнение соответствующих видов работ и оказание услуг в отношении шифровальных (криптографических) средств.

3. Требования по размещению СВТ с установленными средствами ЭП.

3.1. При размещении стационарных СВТ с установленными на них средствами ЭП должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых размещены эти СВТ.

3.2. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны выполняться, исходя из необходимости создания условий для обеспечения сохранения конфиденциальности используемых ключей электронной подписи и иной конфиденциальной информации.

4. Требования к общесистемному и специальному программному обеспечению.

4.1. На СВТ, предназначенных для работы со средствами ЭП, необходимо использовать только лицензионное программное обеспечение (далее – ПО).

4.2. На СВТ с установленными средствами ЭП не должны использоваться средства разработки ПО и отладчики.

4.3. Программное обеспечение, устанавливаемое на СВТ 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 функции ОС.

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

При организации работ по защите ключевой информации от несанкционированного доступа (далее – НСД) необходимо руководствоваться требованиями эксплуатационной документации на соответствующее средство ЭП, а также учитывать следующие общие требования:

5.1. Правом доступа к СВТ с установленными средствами ЭП должны обладать только владельцы ключей электронных подписей, установленных на этих СВТ. Каждый пользователь, применяющий средства ЭП (далее – Пользователь), должен быть ознакомлен с настоящим Руководством и документацией на средства ЭП.

5.2. На СВТ с установленными средствами ЭП необходимо использовать средства антивирусной защиты.

5.3. При использовании средств ЭП необходимо использовать пароли, сформированные в соответствии со следующими правилами:
- длина пароля должна быть не менее 8 символов;
- в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, а также цифры;
- использование в составе символов пароля специальных символы (@, #, $, &, *, % и т.п.) позволяет при необходимости значительно увеличить стойкость используемого пароля;
- 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;
- периодичность смены пароля определяется политикой безопасности Пользователя, но не должна превышать 1 года.

5.4. Запрещается:
- оставлять без контроля СВТ, на котором установлены средства ЭП, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение средств ЭП;
- осуществлять несанкционированное копирование ключевой информации;
- разглашать содержимое ключевой информации или передавать ключевые носители посторонним лицам, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации.

5.5. Необходимо своевременно устанавливать обновления ОС и антивирусного ПО, в том числе и обновления баз данных антивирусного ПО.

5.6. При подключении СВТ с установленными средствами ЭП к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

5.7. При использовании средств ЭП на СВТ, 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, рекомендуется использовать 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.

5.8. Перед началом работы со средствами ЭП необходимо изучить настоящее Руководство и пользовательскую документацию на средства ЭП.

6. Требования по защите от несанкционированного доступа к ключевой информации при использовании специализированных ключевых носителей (аппаратных токенов).

6.1. После получения аппаратного токена (типа eToken, JaCarta, Рутокен и пр.) Пользователь должен произвести смену предустановленных на нем PIN-кодов пользователя и администратора, используемых для аутентификации. Значения предустановленных PIN-кодов указаны в эксплуатационной документации на соответствующий аппаратный токен.

6.2. PIN-коды должны состоять не менее чем из 6 символов. Символы могут включать в себя как буквы и цифры, так и знаки препинания и т.п., то есть. любые символы, которые можно ввести со стандартной клавиатуры.

6.3. При эксплуатации аппаратного токена необходимо учитывать, что после введения неправильного PIN-кода пользователя несколько раз подряд токен блокируется. Разблокировать токен можно при помощи PIN-кода администратора или PUK-кода, в случае использования JaCarta-2 SE. В случае введения несколько раз подряд неправильного PIN или PUK-кода администратора разблокировка токена становится невозможной.

6.4. В ходе эксплуатации аппаратного токена рекомендуется производить смену действующих PIN-кодов с периодичностью, не превышающей 6 месяцев.

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 локализации последствий компрометации ключа электронной подписи.

7.2. При компрометации ключа электронной подписи Пользователь должен немедленно сообщить в удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, о факте компрометации. Информация о компрометации должна передаваться в удостоверяющий центр способом, определенным порядком реализации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей, установленным удостоверяющим центром, выдавшим сертификат ключа проверки электронной подписи[*] . По получении информации о компрометации ключа электронной подписи Удостоверяющий центр прекращает действие сертификата соответствующего ключа проверки электронной подписи, в результате чего создание действительной электронной подписи с использованием скомпрометированного ключа электронной подписи становится невозможным.

8. Использование средств ЭП за пределами территории Российской Федерации

8.1. Правомерность использования средств ЭП на территории Российской Федерации определяется нормами законодательства Российской Федерации.

8.2. При нахождении Пользователя за пределами Российской Федерации, правомерность использования средств электронной подписи определяется законодательством государства, на территории которого находится Пользователь.

8.3. Правообладатель средств ЭП не несет ответственности в случае если наличие средств ЭП на СВТ Пользователя, находящегося за пределами Российской Федерации, и (или) использование Пользователем средств ЭП за пределами Российской Федерации повлечет нарушение Пользователем законодательства государства, на территории которого находится Пользователь.

---

[*] Порядок реализации функций Удостоверяющего центра Акционерного общества «ИнфоТеКС Интернет Траст» установлен соответствующими регламентами оказания Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию сертификатов ключей проверки электронных подписей, опубликованными на сайте Удостоверяющего центра.