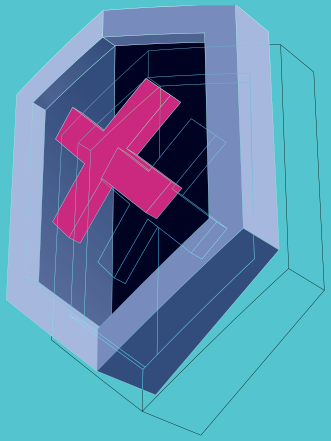
ЭЛЕКТРОННАЯ ПОДПИСЬ

ПРОСТО О СЛОЖНОМ



ВВЕДЕНИЕ

Неотъемлемой частью юридически значимого электронного документооборота является электронная подпись[1]. Безопасность электронной подписи зависит от:

- свойств закрытого ключа[2];
- функциональных возможностей ключевого носителя[3];
- ответственного хранения.

Рекомендуется использовать защищенные носители ключевой информации (далее — ключевые носители), которые, в свою очередь, делятся на пассивные (с защитой данных только по PIN-коду) и активные (со встроенными на аппаратном уровне функциями средства криптографической защиты информации, далее — СКЗИ[4]).

Соблюдение настоящих методологических рекомендаций по использованию ключевых носителей поможет защитить участников электронного документооборота от рисков:

- получения несанкционированного доступа третьих лиц к закрытому ключу для создания его копии;
- подписания электронных документов третьими лицами от имени владельца электронной подписи;
- хищения ключевого носителя или его уничтожение.

---

1 Электронная подпись — это аналог собственноручной подписи для подписания электронных документов.

2 Закрытый (секретный) ключ электронной подписи — это уникальный набор символов (байт), сформированный средством электронной подписи. Используется для формирования самой электронной подписи на электронном документе и хранится в зашифрованном виде на ключевом носителе. Доступ к закрытому ключу защищен паролем (PIN-кодом) и его нужно хранить в секрете.

3 Ключевой носитель — это устройство для хранения закрытого ключа. Ключевой носитель внешне напоминает «флешку» для компьютера, но отличается по своим свойствам: память у него защищена паролем (PIN-кодом). Может иметь встроенное средство криптографической защиты информации. В этом случае он является программно-аппаратным ключевым носителем и позволяет максимально безопасно формировать электронную подпись на электронном документе.

4 Средство криптографической защиты информации (СКЗИ) — термин используется в соответствии с частью 2 раздела I Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ РФ от 09.02.2005 № 66 (Зарегистрировано в Минюсте России 03.03.2005 N 6382).

СВОЙСТВА ЗАКРЫТОГО КЛЮЧА

Экспортируемые и неэкспортируемые закрытые ключи

Свойство экспортируемости или неэкспортируемости закрытого ключа присваивается на этапе формирования закрытого ключа и записи его на ключевой носитель. Указанное свойство может быть реализовано в средствах электронной подписи и управляться его настройками, которые следует установить до формирования закрытого ключа.

Для экспортируемых закрытых ключей доступно их копирование, что несет риски нарушения конфиденциальности закрытого ключа.

Для копирования закрытого ключа нарушителю потребуется получить физический доступ к ключевому носителю и узнать пароль (PIN-код).

Возможность копирования закрытого ключа создаёт риск возникновения неучтенных копий, усложняет контроль за его хранением, использованием и уничтожением. Также указанное усложняет определение возможного нарушителя, особенно когда нарушитель начнет использовать копию не сразу.

Неэкспортируемые закрытые ключи обладают большей защищенностью, так как записанный на ключевой носитель закрытый ключ не подлежит копированию при помощи стандартных СКЗИ. Получение доступа к такому ключу требует применения специальных средств и техники.

Извлекаемые и неизвлекаемые закрытые ключи

Свойство неизвлекаемости закрытого ключа достигается способом его создания[5] и хранения[6], и напрямую зависит от вида ключевого носителя. Для обеспечения свойства неизвлекаемости закрытого ключа используются только активные ключевые носители, содержащие в себе аппаратно реализованные функции СКЗИ, при использовании которых создается и используется неизвлекаемый закрытый ключ.

---

5 Генерация закрытого ключа — создание закрытого ключа с использованием средства электронной подписи.

6 Хранение и использование закрытого ключа происходит только в специальной и защищенной микропроцессором области памяти ключевого носителя, доступ к которой осуществляется с помощью нередактируемого перечня команд микропроцессора, среди которых отсутствуют команды, позволяющие получить доступ к содержанию закрытого ключа

Для некоторых ключевых носителей существует возможность записи закрытого ключа на активные ключевые носители сторонними СКЗИ (установленными локально на компьютерное устройство[7] или непосредственно в информационной системе удостоверяющего центра) и, в таком случае, такой носитель применяется как пассивный ключевой носитель, который может обеспечить только свойство неэкспортируемости закрытого ключа.

К извлекаемым закрытым ключам относятся все виды закрытых ключей, за исключением неизвлекаемых, включая экспортируемые и неэкспортируемые.

ВИДЫ КЛЮЧЕВЫХ НОСИТЕЛЕЙ

Пассивный ключевой носитель

Виды реализации: носитель с USB интерфейсом, носитель с бесконтактным интерфейсом (NFC интерфейс), смарт-карта.

Для доступа к защищенному содержимому данного ключевого носителя необходимо ввести пароль (PIN-код). Закрытый ключ хранится в ключевом контейнере[8] на ключевом носителе. Пароль (PIN-код), которым защищён от доступа закрытый ключ на таком носителе, при получении следует изменить, обеспечить его надежное хранение и исключить доступ к паролю любых лиц.

При подписании электронного документа с использованием пассивного носителя и средства электронной подписи вычисляется уникальный набор символов — хэш документа[9], однозначно связанных с содержанием электронного документа. Далее закрытый ключ копируется в память компьютерного устройства, где с его помощью средство электронной подписи выполняет криптографические операции[10] форми-

7 Компьютерное устройство — мобильный телефон, смартфон, компьютер, планшет.

8 Ключевой контейнер — способ хранения закрытого ключа на ключевом носителе. Доступ к ключевому контейнеру защищается установкой пароля. Защита ключевого контейнера индивидуальна для каждого типа ключевого носителя.

9 Хэш документа (хэш значение документа) — уникальный набор символов, полученный в результате вычисления однонаправленной функции, который неразрывно связан с содержанием электронного документа: в случае изменения электронного документа, даже незначительного, например, добавления в текст пробела, хэш значение электронного документа изменится.

10 Криптографические операции формирования электронной подписи — преобразование ранее вычисленного хеш-значения электронного документа таким образом, что его обратное преобразование возможно только с помощью сертификата ключа проверки электронной подписи.

рования электронной подписи — подписание электронного документа. По завершении процедуры подписания закрытый ключ удаляется из памяти компьютерного устройства. Процедура подписания электронного документа происходит незаметно для пользователя в течение нескольких секунд.

На ключевом носителе установлено ограничение попыток неправильного ввода пароля (PIN-кода) и при превышении такого лимита ключевой носитель блокируется. Несмотря на это, пассивный ключевой носитель обладает средним уровнем защищенности от атак злоумышленников — в момент подписания документа образуется короткий промежуток времени, когда закрытый ключ находится в памяти компьютерного устройства, где существует возможность его перехвата злоумышленником с высоким уровнем технических знаний и/или с использованием специальных технических средств. Для исключения такого вида атак существует активный ключевой носитель.

Активный ключевой носитель (криптографический ключевой носитель)

Виды реализации: носитель с USB интерфейсом, носитель с бесконтактным интерфейсом (NFC интерфейс), смарт-карта.

Активный ключевой носитель содержит в себе функции СКЗИ. Закрытый ключ на таком ключевом носителе хранится в защищенном ключевом контейнере и в специальном внутреннем формате.

У такого носителя существует ряд технических преимуществ перед пассивным ключевым носителем:

- создание закрытого ключа происходит на самом носителе с использованием аппаратных криптографических функций ключевого носителя;
- при подписании электронного документа закрытый ключ не копируется в память или реестр компьютерного устройства — подписание электронного документа происходит на самом ключевом носителе;
- закрытый ключ ни в какой момент времени не покидает ключевой носитель.

Вычисление значения хэш документа может происходить на компьютерном устройстве, а итоговое формирование электронной подписи только на самом активном клю-

чевом носителе.

Компрометация закрытого ключа на таком носителе возможна только в случае его хищения вместе с паролем (PIN-кодом).

Активный ключевой носитель (криптографический ключевой носитель) обладает высоким уровнем защищенности от атак злоумышленников. Риск атаки «подмена хэша»[11] злоумышленником присутствует, но такие случаи крайне редки.

МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ РАБОТЕ С КЛЮЧЕВЫМИ НОСИТЕЛЯМИ

Технические меры предосторожности

При выборе вида ключевого носителя для хранения закрытого ключа электронной подписи следует учитывать, что электронная подпись считается равнозначной собственноручной подписи в случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Рекомендуется использовать ключевые носители с наивысшей степенью защиты закрытого ключа.

Рекомендуется сменить пароль доступа к ключевому носителю (PIN-код), установленный его изготовителем, на уникальный — известный только владельцу электронной подписи. Рекомендуемая длина пароля — не менее 6 символов с использованием специальных символов, прописных и строчных латинских букв. Рекомендуется периодическая смена пароля.

Не рекомендуется при выборе пароля основываться на типовых шаблонах и идущих подряд на клавиатуре или алфавите символах (qwerty, abcde, 12345 и другие), на каком-либо идентификаторе, паспортных данных, кличах питомцев и подобных ассоциацях.

Не рекомендуется активировать функцию «запомнить пароль» в средствах электронной подписи и настройках программного обеспечения, которое необходимо для использования ключевого носителя.

---

11 Атака «подмена хэша» — тип атаки злоумышленником, когда последний вычисляет хэш-значение поддельного документа и перехватив в памяти компьютера хэш-значение подписываемого документа, заменяет его своим .

ОРГАНИЗАЦИОННЫЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ

Не рекомендуется в рамках организации процедур безопасной работы с ключевым носителем:

- передавать ключевой носитель третьим лицам;
- записывать пароль доступа к ключевому носителю (PIN-код) на бумаге или непосредственно на ключевом носителе, запоминать пароли в реестровой памяти систем электронных устройств и хранить парольную информацию в общедоступных местах;
- оставлять ключевой носитель без присмотра в доступных или общественных местах;
- оставлять без присмотра ключевой носитель в компьютерном устройстве, на котором осуществляется подписание электронных документов (usb-порты в системном блоке компьютера, ноутбука, планшета или других электронных устройствах).

Рекомендуется в рамках организации процедур безопасной работы с ключевым носителем:

- при необходимости, обеспечивать сотрудников организации, не имеющих права действовать без доверенности, их персональными закрытыми ключами и сертификатами электронной подписи, с наделением их правом подписи распорядительными документами организации путем оформления доверенности;
- хранить ключевой носитель в недоступном для третьих лиц месте;
- при потере или краже ключевого носителя незамедлительно обратиться в удостоверяющий центр, выпустивший сертификат электронной подписи, прекратить действие такого сертификата электронной подписи, и, не дожидаясь завершения процедуры аннулирования, уведомить контрагентов о том, что утраченный сертификат с соответствующим серийным номером считается уже недействительным.

ЭЛЕКТРОННАЯ ПОДПИСЬ

ПРОСТО О СЛОЖНОМ

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА