Методологические рекомендации по использованию носителей ключевой информации (защищенных ключевых носителей)

1. Введение

Неотъемлемой частью юридически значимого электронного документооборота является электронная подпись[1]. Безопасность закрытого ключа[2] электронной подписи зависит от свойств экспортируемости и извлекаемости, а также функциональных возможностей носителя ключевой информации[3], на котором он хранится и ответственного его хранения владельцем.

В качестве носителей закрытых ключей электронной подписи 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[4]).

Соблюдение настоящих методологических рекомендаций по использованию носителей ключевой информации поможет защитить участников юридически значимого электронного документооборота от рисков:

- получение несанкционированного доступа третьих лиц к закрытому ключу для создания его копии или подписания электронных документов такими лицами от имени владельца электронной подписи или уничтожения закрытого ключа;
- хищение ключевого носителя или его уничтожение.

2. Разновидности (свойства) закрытого ключа

2.1. Экспортируемые и неэкспортируемые закрытые ключи

Свойство экспортируемости или неэкспортируемости закрытого ключа (ключевого контейнера) 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.

---

[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 электронной подписи. В этом случае он является программно-аппаратным ключевым носителем и позволяет безопасно формировать электронную подпись на электронном документе. Хранить закрытый ключ также можно на компьютере пользователя.

[4] Средство криптографической защиты информации – 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).

Для экспортируемых закрытых ключей доступно их санкционированное копирование или несанкционированное копирование (что несет риски нарушения конфиденциальности закрытого ключа) и/или перенос на другие ключевые носители, например, на жесткий диск компьютера при помощи штатных возможностей конкретных средств электронной подписи. Для несанкционированного копирования нарушителю потребуется получить физический доступ к ключевому носителю и узнать PIN-код (пароль). Возможность копирования создаёт риск возникновения неучтенных копий закрытого ключа и усложняет контроль за его хранением, использованием и уничтожением, риск отложенного несанкционированного использования закрытого ключа, что усложняет определение возможного нарушителя.

Неэкспортируемые закрытые ключи обладают большей защищенностью, т.к. однажды записанный на ключевой носитель закрытый ключ не подлежит копированию при помощи штатных возможностей средства криптографической защиты информации. Неэкспортируемые закрытые ключи являются более надежным вариантом использования, поскольку получение доступа к такому закрытому ключу требует применения специальных средств и техники.

2.2. Извлекаемые и неизвлекаемые закрытые ключи

Свойство неизвлекаемости закрытого ключа достигается определенным способом[5] его генерации[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 средства криптографической защиты информации, при использовании которых генерируется и используется неизвлекаемый закрытый ключ.

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

К извлекаемым закрытым ключам относятся все закрытые ключи, за исключением неизвлекаемых, включая экспортируемые и неэкспортируемые.

3. Взаимосвязь разновидностей (свойств) закрытого ключа и типа ключевого носителя

[5] 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.

[6] Генерация закрытого ключа – создание закрытого ключа с использованием средства электронной подписи.

[7] Компьютерное устройство – мобильный телефон, смартфон, компьютер, планшет.

3.1. 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.

При обращении к ключевому контейнеру на ключевом носителе запрашивается пароль (PIN-код), и, после принятия верного пароля, закрытый ключ из защищённой памяти ключевого носителя считывается в оперативную память компьютерного устройства для подписания электронного документа. Закрытый ключ на таком носителе защищён от доступа: для доступа к нему необходимо ввести пароль доступа к устройству (PIN-код), при условии, что владельцем ключевого носителя стандартный пароль доступа к ключевому носителю был сменен на персонализированный.

При подписании электронного документа с использованием такого 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] формирования 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.

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.

На ключевом носителе установлено ограничение попыток неправильного ввода пароля (PIN-кода) и при превышении такого лимита ключевой носитель блокируется.

---

[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.

Пассивный ключевой носитель обладает средним уровнем защищенности от атак злоумышленников.

3.2. 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 аппаратно реализованные функции СКЗИ[11]. Закрытый ключ на активном (криптографическом) ключевом носителе хранится в его памяти, в защищенном ключевом контейнере и в специальном внутреннем формате. Помимо невозможности экспорта закрытого ключа, в таком ключевом носителе отсутствует возможность импорта закрытых ключей, что обеспечивает отсутствие возможности существования копии (путем клонирования) закрытого ключа пользователя вне конкретного аппаратного модуля (свойство неизвлекаемости). В связи с указанными техническими характеристиками, у такого носителя появляется ряд индивидуальных технических преимуществ перед пассивным ключевым носителем:

1) генерация закрытого ключа происходит на самом носителе с использованием аппаратных криптографических функций ключевого носителя;

2) при подписании электронного документа закрытый ключ не копируется в память или реестр компьютерного устройства – подписание электронного документа происходит на самом ключевом носителе. Вычисление значения хэш документа может происходить на компьютерном устройстве (присутствует риск атаки «подмена хэша»[12] злоумышленником), а итоговое формирование электронной подписи на основе закрытого ключа и хэш документа – на самом криптографическом ключевом носителе. Закрытый ключ ни в какой момент времени не покидает такой ключевой носитель, в связи с чем, его компрометация возможна только в случае хищения ключевого носителя вместе с паролем (PIN-кодом), что и является следствием его неизвлекаемости.

Активный ключевой носитель (криптографический ключевой носитель) обладает высоким уровнем защищенности от атак злоумышленников.

4. Меры предосторожности при работе с ключевыми носителями

4.1. Технические меры предосторожности

При выборе вида ключевого носителя для хранения закрытого ключа электронной подписи следует учитывать, что электронная подпись считается

---

[11] СКЗИ – средство криптографической защиты информации.

[12] 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 .

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 символов (qwerty, abcde, 12345 и другие часто используемые последовательности) на каком-либо слове, идентификаторе, паспортных данных, кличек питомцев и подобных ассоциаций. Не рекомендуется активировать в настройках программного обеспечения, которое необходимо для использования ключевого носителя, и средств электронной подписи, свойство «запомнить пароль».

4.2. 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 сопряженным с компьютерным устройством, на котором осуществляется подписание электронных документов (usb-порты в системном блоке компьютера, ноутбука, смартфона, планшета или других электронных устройствах).

Рекомендуется в рамках организации процедур безопасной работы с ключевым носителем:

- при необходимости участия в электронном документообороте сотрудников хозяйствующего субъекта, помимо руководящего состава, рекомендуется обеспечивать таких сотрудников персональными закрытыми ключами и сертификатами электронной подписи, выданными на их имя, и наделять их правом подписи распорядительными документами хозяйствующего субъекта, путем оформления доверенности;
- хранить ключевой носитель в недоступном для третьих лиц месте;

- при потере или краже ключевого носителя незамедлительно приостановить бизнес-процессы хозяйствующего субъекта, связанные с электронным документооборотом и обратиться в удостоверяющий центр, выпустивший сертификат электронной подписи, и прекратить действие соответствующего сертификата электронной подписи, в соответствии с положением/регламентом выполнения функций удостоверяющего центра;
- при потере или краже ключевого носителя незамедлительно, не дожидаясь завершения процедуры аннулирования, уведомить ключевых контрагентов о том, что сертификат с серийным номером, соответствующим утраченному носителю, будет аннулирован и поэтому считается уже недействительным.