

ИНФОРМАЦИОННЫЙ ЛИСТ

Носители для личного ключа ЭЦП



Носители для личного ключа ЭЦП

При генерации ключей Электронной цифровой подписи (ЭЦП), в Центре сертификации ключей (ЦСК) «MASTERKEY» личный ключ ЭЦП клиента записывается на носитель ключевой информации.

В качестве носителя ключевой информации в ЦСК «MASTERKEY» могут использоваться следующие типы носителей:

- компакт-диск;
- портативный накопитель на флэш-памяти;
- защищенный портативный накопитель на флэш-памяти;
- смарт-карта.

Важными качествами каждого типа носителей являются:

- физическая надежность (количество циклов перезаписи и срок эксплуатации носителя);
- функция защиты информации.

В таблице 1 приведена сравнительная характеристика типов носителей ключевой информации с точки зрения физической надежности и наличия функции защиты информации.

Таблица 1. Сравнительная характеристика типов носителей ключевой информации¹

Тип носителя	Физическая надежность	Функция защиты информации
компакт-диск	средняя	отсутствует
портативный накопитель на флэш-памяти	высокая	отсутствует
защищенный портативный накопитель на флэш-памяти	высокая	присутствует
смарт-карта	высокая	присутствует

Высокая физическая надежность носителя ключевой информации гарантирует то, что личный ключ ЭЦП, записанный на такой носитель, не будет испорчен в процессе длительной эксплуатации, в то время как носитель с низкой или средней физической надежностью такой гарантии не имеет.

В случае если носитель ключевой информации вышел из строя, был поврежден или испорчен, и личный ключ ЭЦП не читается, клиенту необходимо повторно пройти процедуру генерации ключей.

Повторная процедура генерации ключей ЭЦП происходит в ЦСК аналогично процедуре первоначальной генерации ключей. Оплата этой услуги производится согласно тарифам ЦСК.

¹ Оценка проводилась специалистами ЦСК «MASTERKEY» на основании материалов прессы, профессиональных обзоров и технических характеристик. Данная оценка не претендует на 100% достоверность и отражает лишь мнение специалистов ЦСК по данному вопросу.

Что касается функции защиты информации, то при хранении личного ключа ЭЦП на носителе информации, в котором эта функция отсутствует, доступ к личному ключу может быть получен сразу же после ввода пароля к личному ключу (однофакторная аутентификация).

При хранении личного ключа ЭЦП на носителе в котором функция защиты информации присутствует, доступ к личному ключу может быть получен только после ввода пароля, защищающего носитель и пароля к самому личному ключу ЭЦП (двухфакторная аутентификация).

На носителе ключевой информации запрещается хранить какие-либо иные данные, кроме личного ключа ЭЦП.

Анализ типов предлагаемых носителей

Компакт-диск (CD) не подвержен воздействию магнитных полей, достаточно устойчив к механическим повреждениям, информация на нем может храниться очень долго.

Однако если часто использовать данный носитель личного ключа для подписания документов, то со временем поверхность диска может покрыться царапинами и он перестанет нормально функционировать.

Компакт-диск обладает средней физической надежностью, и не защищен от несанкционированного доступа.

Портативный накопитель на флэш-памяти достаточно надежный носитель с точки зрения физической надежности, но он тоже не обеспечивает защиту личного ключа ЭЦП от несанкционированного доступа.

Одним из недостатков накопителя на флэш-памяти является то, что личный ключ ЭЦП может быть стерт или перезаписан по неосторожности.

Защищенный портативный носитель и смарт-карта наиболее надежные с физической точки зрения и с точки зрения безопасности.

Их недостатками является высокая, по сравнению с другими типами носителей, стоимость и необходимость предварительной установки программного обеспечения, позволяющего с ними работать. То есть такими типами носителей нельзя воспользоваться на произвольном компьютере без осуществления процедуры предварительной установки драйверов устройства.

Решение о выборе типа носителя принимает пользователь, исходя из своих технических и финансовых возможностей.

С целью обеспечения требований безопасности ЦСК генерация личного ключа проводится только на носители ключевой информации, предоставляемые ЦСК «MASTERKEY». Стоимость носителя ключевой информации входит в стоимость услуги генерации ключей ЭЦП.