Электронная подпись: понятие, принцип функционирования, свойства, особенности использование. Инфраструктура открытых ключей.

Подготовил:
Студент 4-го курса
кафедры УПиНБ ЮФ НГУЭУ
Карнаух Д.В.

Проверил:
доцент кафедры ИТ ФГС НГУЭУ
Пургина М.В.

Технический прогресс не стоит на месте. С течением времени появляется множество технологических новинок, активно внедряемых в жизнь человека. В том числе и в IT-сфере.

С появлением компьютеров и доступа к информационно-телекоммуникационной сети Интернет широких масс значительно упростился процесс выполнения тех или иных работ.

Вместе с тем перед предприятиями и рядовыми пользователями возникла острая необходимость защиты своих данных, т.к. в любом обществе есть процент людей, желающих заполучить информацию незаконным путём, исходя из своих корыстных побуждений

Именно в целях защиты электронных данных была разработана электронная подпись.

Термин

Согласно п.1 ст.2 ФЗ от 06.04.2011 №63 «Об электронной подписи»:

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.

Принцип работы

Файл электронной подписи генерирует специальная программа — средство криптографической защиты информации.

Когда вы подпишете документ электронной подписью, эта программа просканирует документ. В итоге она создаст уникальное сочетание данных документа — хэш-сумму.

Она шифруется с помощью закрытого ключа — особой последовательности символов, которая формирует файл подписи. Ключ выдают владельцу подписи.

Сертификат закрытого ключа хранится у владельца на любом удобном носителе: будь то внешнее железо, внутреннее или даже облачное хранилище.

Свойства электронной подписи

- ЭП упрощает процесс обмена данными;

- сокращает расходы;

- экономит время на оформление;

- гарантирует целостность передаваемого документа

Особенности использования электронной подписи

1. порядок использования электронных цифровых подписей в информационной системе устанавливается решением владельца данной системы или соглашением участников этой системы

2. Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юр.силы в информационной системе регламентируются решением владельца системы или соглашением участников данной системы

Инфраструктура открытых ключей

состоит из программных и аппаратных элементов, которые доверенная третья сторона может использовать для установления целостности и принадлежности **открытого ключа**. Доверенная сторона, называемая центром сертификации (CA), обычно выполняет эту задачу, выдавая подписанные (зашифрованные) двоичные сертификаты, подтверждающие подлинность субъекта сертификата, и привязывает удостоверение к **открытому ключу**, содержащемуся в сертификате.

Вопросы

1. Что есть электронная подпись документа?

2. В каких сферах может быть применима электронная подпись?

3. Что влечёт за собой факт установления несоответствия между электронной подписью и документом, в отношении которого она была установлена в качестве защиты?

Презентация завершена