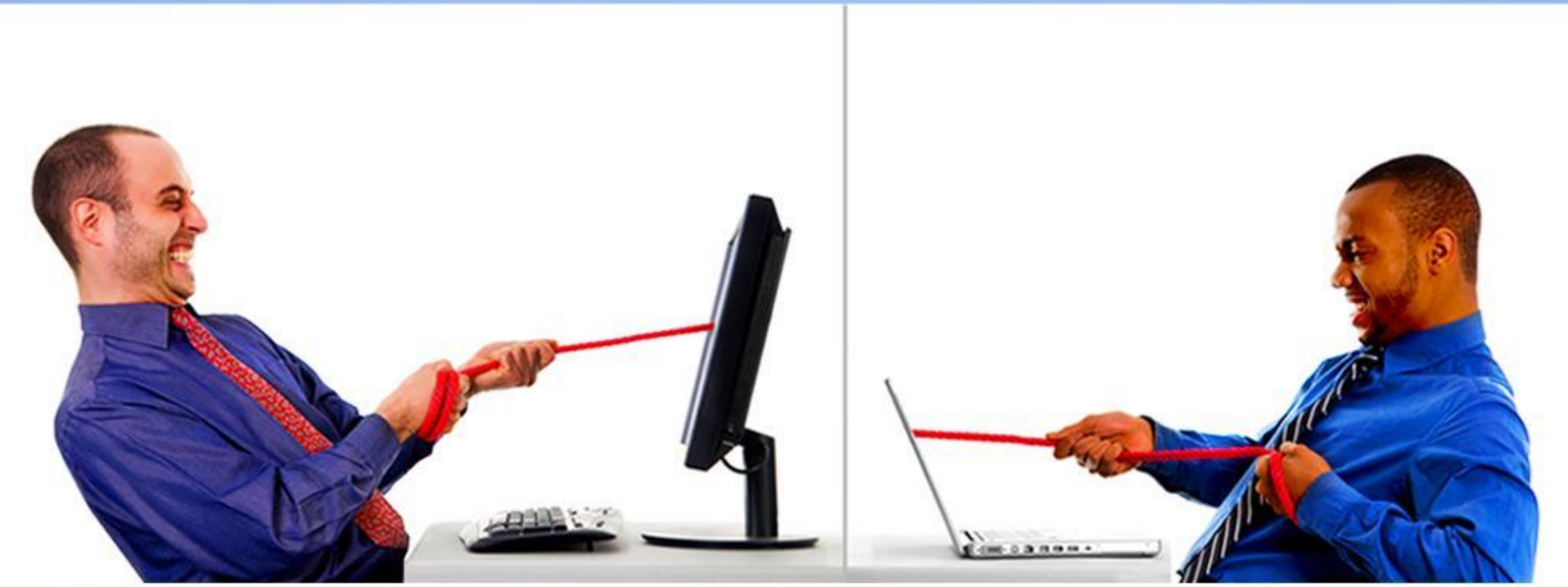
Электронная цифровая подпись



Подготовила студентка группы
2Л-1 Хакимова Ю.Ф.

Понятия электронной цифровой подписи (ЭЦП)

ЭЦП– это криптографическое средство, которое позволяет удостовериться в отсутствие искажений в тексте электронного документа, а в соответствующих случаях – распозновать лицо, создавшее такую подпись.

ЭЦП используется в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе.

Электронный документ - это любой документ, созданный и хранящийся на компьютере.

ЭЦП обеспечивает:

1) **Подлинность** - Цифровая подпись помогает гарантировать, что поставивший подпись — тот, кем он является в действительности.

2) **Целостность** - Цифровая подпись помогает гарантировать, что содержимое документа не менялось после ввода цифровой

3) **Неотрекаемость** - ЭЦП помогает доказать любой из сторон авторство подписанного

Категории шифрования

Большинство криптографических компьютерных систем принадлежат к одной из двух категорий:

1) Шифрование симметричным ключом;

2) Шифрование открытым ключом.

Шифрование симметричным ключом

Симметричный ключ –это секретный код, который должны знать оба компьютера, чтобы иметь возможность расшифровывать сообщения друг от друга.

В секретном коде содержится "ключ" для расшифровки сообщений.

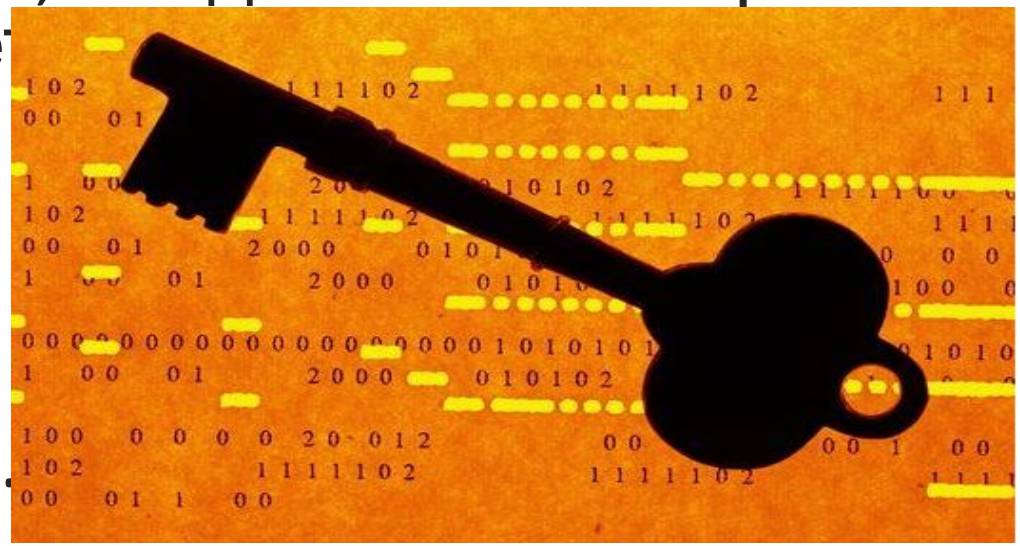
Шифрование открытым ключом

Шифрование открытым ключом использует комбинацию из секретного ключа и открытого ключа.

Секретный ключ известен только вашему компьютеру, в то время как открытый ключ свободно передается вашим компьютером любым другим, которые хотят вести с вами зашифрованное общение.

Сочетание открытых и симметричных ключей

При соединении двух компьютеров, одна машина создает симметричный ключ и отправляет его другой, используя при этом шифрование открытым ключом. После этого компьютеры будут общаться, используя шифрование симметричным ключом. После окончания соединения, каждый компьютер избавляется от симме



Каждое новое соединение требует создания нового симметричного ключа.

Идентификация

Идентификация (распознание) используется для проверки того, что информация или данные поступают к вам от доверенного источника и не были и

Способы идентификации на компьютер

1) **Пароль** - использование имени и пароля пользователя .

2) **Карты допуска** - эти карты могут быть разного типа, от простой карты с магнитной дорожкой до смарт карт.

3) **Цифровая подпись** - в основном способ убедиться в том, что электронн документ (например, e-mail) является . подлинным.

Условия исполнения Закона «Об электронной цифровой подписи»

10 января 2002 года был принят Федеральный Закон «Об электронной цифровой подписи», вступивший в силу

с 22 января текущего года.

Условия использования ЭЦП в электронных документах:

1) Средства создания подписи признаются надежными;

2) Сама ЭЦП признается достоверной, а ее подделка подписанных данных могут быть точно установлены;

3) Предоставляются юридические гарантии безопасности передачи информации;

4) Соблюдаются правовые нормы, содержащие требования к письменной форме документа;

5) Сохраняются все традиционные процессуальные функции подписи;

6) Обеспечивается охрана персональной информации

Обладатель ЭЦП

Владельцем сертификата ключа подписи (обладателем ЭЦП) является физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП подписывать электронные документы.

Владелец сертификата ключа подписи обязан:

1) Хранить в тайне закрытый ключ ЭЦП;

2) Не использовать для ЭЦП открытые и закрытые ключи ЭЦП, если ему известно, что эти ключи используются или использовались ранее;

3) Немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа ЭЦП нарушена.

Удостоверяющий центр обязан аннулировать сертификат ключа подписи:

Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его (статья 14 Федерального закона):

1) По истечении срока его действия;

2) При утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;

3) В случае если удостоверяющему центру стало известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;

4) По заявлению в письменной форме владельца сертификата ключа подписи;

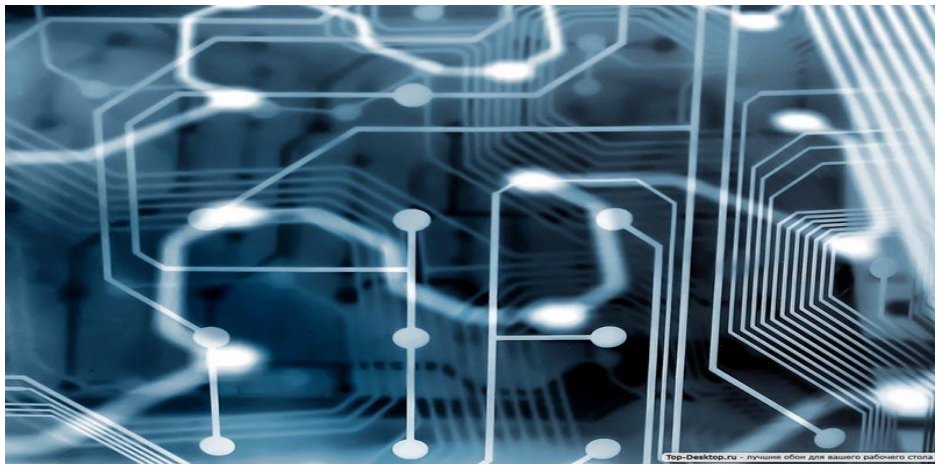
5) В иных установленных нормативными правовыми актами или соглашением сторон случаях.

ЭЦП это код, содержащий в зашифрованном виде:

1) Идентификацию секретного ключа владельца как лица, подписавшего документ;

2) Дату и время произведения подписи;

3) Весь исходный текст документа в том виде, в каком он существовал на момент произведения подписи.



Спасибо за внимание!!!☺️