

Криптографические средства защиты объектов информатизации

Криптографические стандарты

A decorative graphic consisting of several sets of concentric circles in a lighter blue shade, scattered across the bottom right portion of the slide.

Отечественные криптографические стандарты

- ГОСТ 28147-89 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”
- ГОСТ Р 34.11-94 “Информационная технология. Криптографическая защита информации. Функция хеширования”
- ГОСТ Р 34.10-94 “Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма”
- ГОСТ Р 34.10-2001 “Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи”

Правовое регулирование применения ЭЦП

- Федеральные законы:
 - Гражданский кодекс РФ
 - Об электронной цифровой подписи (№ 1-ФЗ от 10.01.2002)
 - Об информации, информационных технологиях и защите информации
 - Материалы Высшего Арбитражного суда
 - иные федеральные законы
- Иные нормативные правовые акты РФ:
 - Государственные криптографические стандарты РФ
- Соглашение сторон

Гражданский Кодекс РФ

- Часть 1, статья 160, п.2
 - Использование при совершении сделок ...электронно-цифровой подписи ...допускается в случаях и порядке, предусмотренных законом, иными правовыми актами или **соглашением сторон**
- Часть 1, статья 434, п.1
 - Если **стороны договорились** заключить договор в определенной форме, он **считается заключенным** после придания ему **условленной формы**, хотя бы законом для договоров данного вида такая форма не требовалась
- Часть 1, статья 434, п.2
 - **Договор** в письменной форме **может быть заключен** ...путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, **электронной** или иной связи, **позволяющей достоверно установить, что документ исходит от стороны по договору**

Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

□ Статья 11, п.3

- **Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.**

□ Статья 11, п.4

- **В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.**

Федеральный закон РФ от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи»

□ Статья 4 п.1

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- **сертификат ключа подписи, относящийся к электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания**
- **подтверждена подлинность электронной цифровой подписи в электронном документе**
- **электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи**

Федеральный закон РФ от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи»

□ Статья 5 п.2

- При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи.
- Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается.