

# ***ПРОГРАММНО-АППАРАТНАЯ РЕАЛИЗАЦИЯ СОВРЕМЕННЫХ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ И СИСТЕМ***

Борисов В.А.

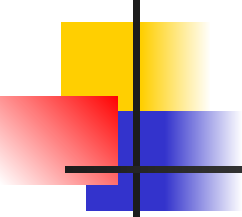
КАСК – филиал ФГБОУ ВПО РАНХ и ГС

Красноармейск 2011 г.



---

***Стандартизация программно-  
аппаратных  
криптографических систем и  
средств***

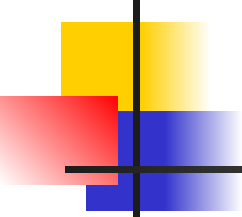
- 
- 
- Программно-аппаратная реализация криптографических систем и средств в мировой практике основывается на криптографических стандартах DES и ГОСТ 28147 — 89.

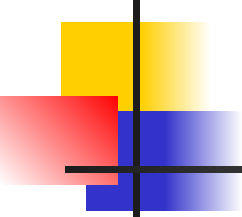


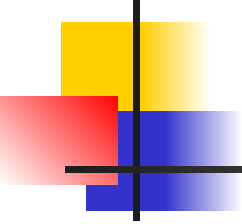
# Основные области применения DES-алгоритма

---

- хранение данных в ЭВМ;
- аутентификация сообщений;
- электронная система платежей;
- электронный обмен коммерческой информацией.

- 
- 
- Блок-схема алгоритма ГОСТ отличается от блок-схемы DES-алгоритма отсутствием начальной перестановки и числом циклов шифрования.

- 
- 
- Алгоритм расшифровки отличается от алгоритма зашифровки тем, что последовательность ключевых векторов используется в обратном порядке.



---

***Ключевые системы  
разграничения доступа и  
электронная цифровая  
ПОДПИСЬ***

# Ключевая система шифра



---

- Описание всех видов ключей, используемых шифром, и алгоритмы их применения.

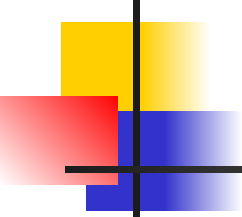




# Размер ключа

---

- Определяет число всевозможных ключевых установок шифра.

- 
- 
- Наличие закономерностей в ключе приводит к неявному уменьшению его размера и к понижению криптографической стойкости шифра.

# Основные меры по защите ключей

---

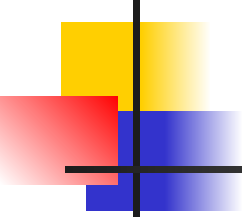
- ограничение круга лиц, допущенных к работе с ключами;
- регламентация рассылки, хранения и уничтожения ключей;
- установление порядка смены ключей;
- применение технических мер защиты ключевой информации от несанкционированного доступа.

# Электронная цифровая подпись



---

- Современное средство защиты конфиденциальности информации.

- 
- 
- При передаче сообщения по линиям связи или хранении его в памяти должны быть обеспечены вместе или по отдельности следующие требования:
    1. Соблюдение конфиденциальности сообщения;
    2. Удостоверение в подлинности полученного сообщения.

# Цели применения цифровой подписи



---

- гарантированное подтверждение подлинности информации, содержащейся в конкретном электронном документе,
- возможность неопровержимо доказать третьей стороне, что документ составлен именно этим конкретным лицом - автором данного документа.



# Контрольная функция

---

- код подлинности сообщения;
- квадратичный конгруэнтный алгоритм;
- Manipulation Detection Code;
- Message Digest Algorithm;
- контрольная сумма;
- символ контроля блока;
- циклический избыточный код;
- хеш-функция;
- имитовставка в ГОСТ 28147—89;
- алгоритм с усечением до  $n$  битов.



# Цифровая подпись

---

- Цифровое дополнение к передаваемому или же хранящемуся зашифрованному тексту, которое гарантирует целостность подписи и позволяет проверить авторство.