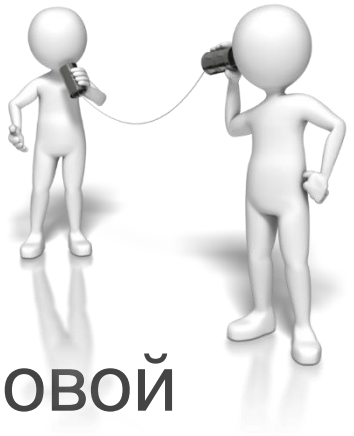
О криптографических проблемах, возникающих при реализации ПКЗ-2005

Докладчик: Н.С. Тыщенко

Средство криптографической защиты информации



а) средства шифрования

б) средства имитозащиты;

в) средства электронной цифровой подписи

г) средства кодирования;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

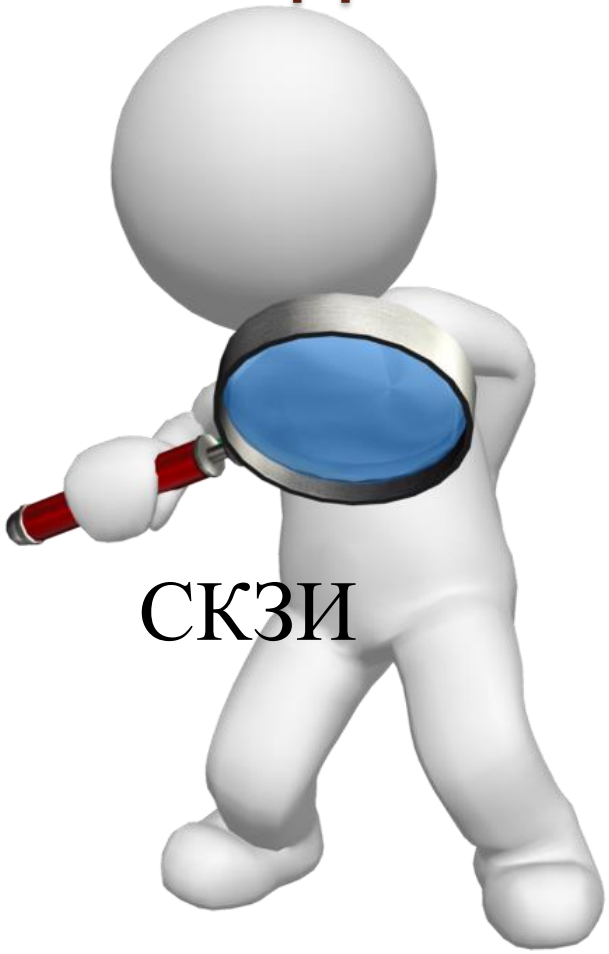
Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

разработка исследования экспертиза

Разработка

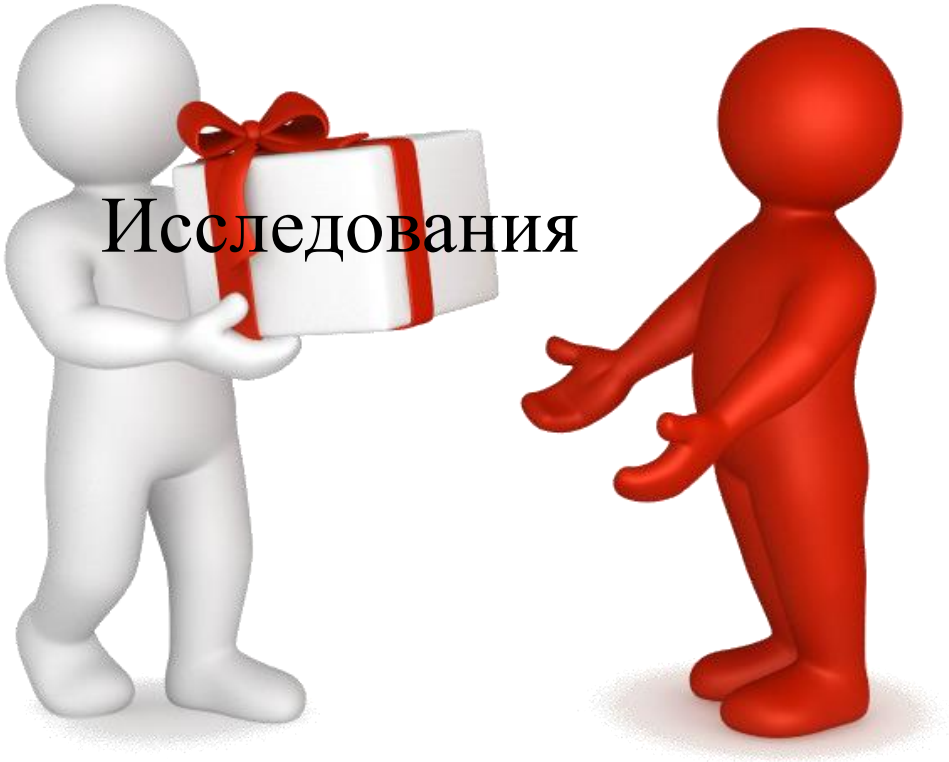
СКЗИ

Исследования



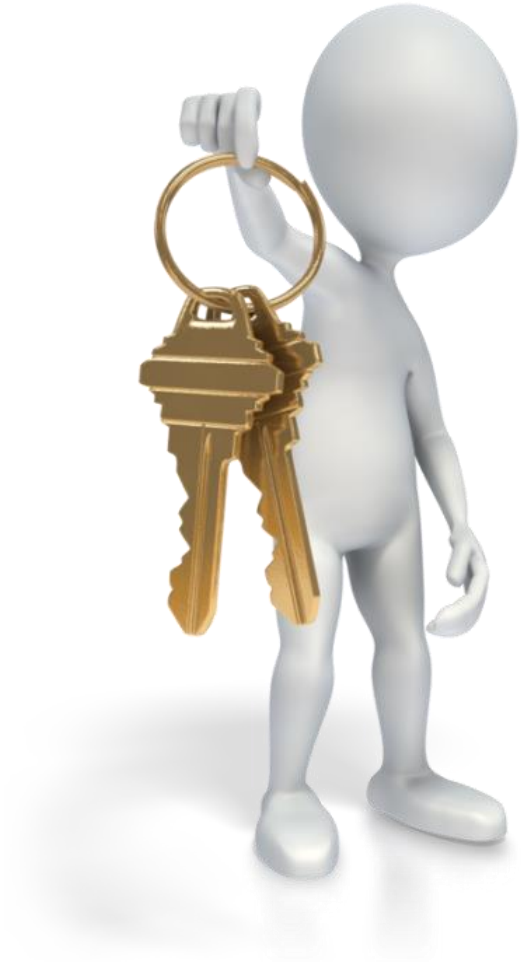
СКЗИ

Экспертиза



Кадровый вопрос

Ключевая система



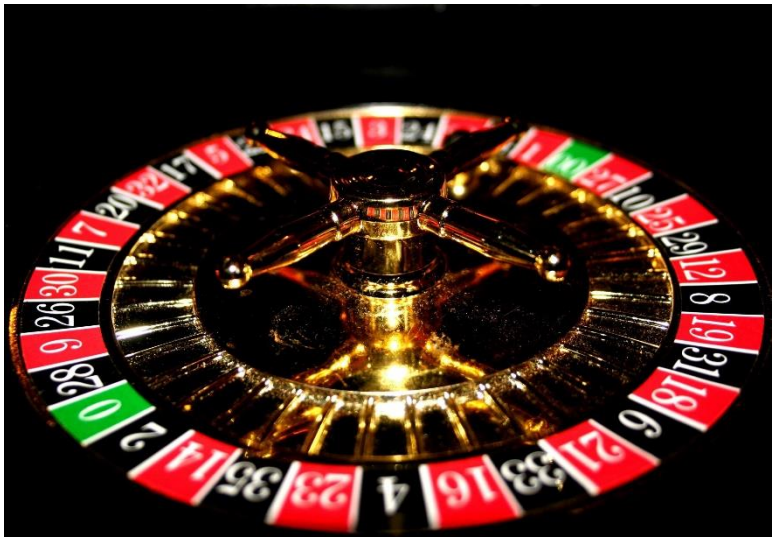
Алгоритмы и протоколы

Криптография

Ключи Алгоритмы

- Слабые ключи, стойкий алгоритм
- Хорошие ключи, слабый алгоритм

Датчики случайных чисел



Аутентификация пользователя

Итог

Спасибо за внимание!