

1. Знакомство с предметом криптографической защиты информации

- Основные понятия и определения.
- Алгоритмы симметричного шифрования.
- Алгоритмы асимметричного шифрования.
- Алгоритмы хеширования.
- Алгоритмы создания и проверки электронной (цифровой) подписи.

2. Концепция инфраструктуры открытых ключей (PKI)

- Основные понятия и определения.
- Архитектура PKI.
- Понятие о сертификате открытого ключа.
- Стандарт X.509

3. Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах

- Роль и место ЭП и других криптографических технологий обеспечения безопасности в системах управления, документооборота и электронной коммерции.
- Законы РФ, регулирующие использование СКЗИ и ЭП.
- Постановления Правительства РФ, регулирующие использование СКЗИ и ЭП.
- Нормативно-методические документы ФСБ России, регулирующие использование СКЗИ и ЭП.

4. Практическая реализация СКЗИ и ЭП на ОС

- Архитектура криптографической системы ОС
- Встраивание в ОС дополнительных СКЗИ и ЭП.
- Хранение информации об используемых криптографическими алгоритмами ключах и другой информации в ОС
- Использование криптографических методов защиты информации в протоколах защиты транспортного уровня SSL/TLS и электронной почты.
- Настройка приложений для использования ими криптографических методов защиты информации.
- Практическая работа: Работа с локальным хранилищем сертификатов в ОС.
- Практическая работа: Настройка приложений для использования СКЗИ в ОС.

5. СКЗИ «КриптоПро CSP»: установка, настройка, использование

- Общие сведения о СКЗИ «КриптоПро CSP».
- Установка СКЗИ «КриптоПро CSP».
- Настройка СКЗИ «КриптоПро CSP».
- Использование СКЗИ «КриптоПро CSP» в прикладных программах.
- Практическая работа: Установка СКЗИ «Крипто-Про CSP».
- Практическая работа: Настройка СКЗИ «Крипто-Про CSP».
- Практическая работа: Использование СКЗИ «КриптоПро CSP» совместно с MS Outlook Express для защиты сообщений электронной почты.