

Криптографическая защита информации, 104 часа (Программа)

1. Законодательная и нормативно-методическая база использования шифровальных (криптографических) средств.

- Введение. Актуальность проблемы обеспечения информационной безопасности. Термины и определения в области информационной безопасности.
- Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.
- Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств.

2. Теоретические основы использования шифровальных (криптографических) средств.

- Методы и способы криптографической защиты информации.
- Инфраструктура открытых ключей (ИОК/PKI).
- Обзор сертифицированных шифровальных (криптографических) средств защиты информации. Методика оценки и выбора СКЗИ.
- Практическая работа: Изучение базовых криптографических операций.
- Практическая работа: Изучение основных криптографических алгоритмов.

3. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

- Порядок обращения с СКЗИ и криптоключами к ним.
- Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.
- Лицензирование видов деятельности, связанных с шифровальными (криптографическими) средствами.

4. Практическое применение сертифицированных шифровальных (криптографических) средств.

- Назначение, состав и порядок применения аппаратных ключей в качестве функциональных ключевых носителей.
- Назначение и порядок применения СКЗИ, реализующих базовый функционал по криптографической защите информации ограниченного доступа.
- Назначение и порядок применения СКЗИ, используемых для обеспечения безопасности информации ограниченного доступа при передаче по каналам связи.
- Назначение и порядок применения СКЗИ для обеспечения защиты информации ограниченного доступа от несанкционированного доступа (НСД) при хранении в информационной системе.
- Назначение, состав и порядок применения программно-аппаратных средств автоматизации деятельности Удостоверяющих центров.
- Практическая работа: Работа с локальным хранилищем сертификатов в ОС MS Windows.
- Практическая работа: Порядок использования функциональных ключевых носителей на примере eToken.
- Практическая работа: Практическое применение цифровых сертификатов.
- Практическая работа: Установка, настройка СКЗИ «КриптоПро CSP». Работа с контейнерами закрытого ключа и сертификатами пользователя.
- Практическая работа: Практическое применение «КриптоПро CSP» и сертификатов для защиты сообщений электронной почты.
- Практическая работа: Защита информации при ее хранении в ИС с использованием ПО «Secret Disk 4».
- Практическая работа: Защита информации при ее хранении в корпоративной ИС с использованием ПО «Secret Disk Server NG».
- Практическая работа: Защита информации при передаче по каналам связи с использованием ПО «КриптоПро IPsec».
- Практическая работа: Установка и настройка ПАК «Удостоверяющий центр КриптоПро УЦ».
- Практическая работа: Практическая реализация регламентных процедур с использованием АРМ администратора ЦР.
- Практическая работа: Реализация процедур Технического регламента Удостоверяющего центра.