

Аннотация рабочей программы дисциплины (модуля)

ФТД.В.02 Сетевая безопасность

Цель дисциплины

Целью изучения дисциплины является формирование знаний об основных типах и способах защиты информации в компьютерных сетях, а также навыков по проектированию системы защиты информации и анализу защищенности вычислительных сетей.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- изучение основных принципов информационной безопасности сетевого оборудования;
- ознакомление с техническими и технологическими решениями, используемыми в данной области;
- выработка практических навыков аналитического и экспериментального исследования основных методов и средств, используемых в области, изучаемой в рамках данной дисциплины.

Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
УК - 1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает методы поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа. УК-1.2. Умеет применять методы поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач. УК-1.3. Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач

Содержание разделов дисциплины

Тема 1. Виды атак. Модель сетевой безопасности. Криптография и системы шифрования

Обобщенный сценарий атаки. Пассивная разведка. Активная разведка. Взлом целевой системы. Соккрытие следов взлома. Классификация атак. Модель сетевой безопасности. Криптография. Структура шифрования Фейстеля. Алгоритмы стандартного шифрования. Режимы работы блочных шифровальщиков. Расположение устройств шифрования. Распределение ключей. Криптография и аутентификация сообщений на основе общего ключа.

Тема 2. Механизмы обеспечения безопасности коммутируемых локальных сетей.

Ограничение количества управляющих компьютеров. Настройка безопасности индивидуального порта. Фильтрация MAC-адресов. Технология фильтрации IP-MAC

Binding. Списки контроля доступа. Сегментация трафика. Протокол IEEE 802.1x. Виртуальные сети. Аудит безопасности протокола связующего дерева STP.

Тема 3. Механизмы обеспечения безопасности беспроводных локальных сетей.

Классификация механизмов безопасности в сетях Wi-Fi. Механизмы шифрования. Принцип аутентификации абонента. Открытая аутентификация. Аутентификация с общим ключом. Аутентификация по MAC-адресу. Дополнительные механизмы защиты.

Тема 4. Механизмы межсетевой безопасности.

Межсетевые экраны. Фильтры пакетов. Фильтры инспекции состояний. Транслятор адресов. Транспортные шлюзы. Шлюзы приложений. Системы обнаружения атак и вторжений.

Тема 5. Системы туннелирования.

Протокол PPPoE. Виртуальные частные сети. Протокол IPSEC. Протокол SSL/TLS.

Тема 6. Безопасность удаленного управления.

Аудит безопасности протокола SNMP. Версии протокола SNMP. Протокол SNMPv3. Протокол SSH. Рекомендации по безопасности использования протокола SSH.