Аннотация рабочей программы дисциплины (модуля)

Б1.В.ДВ.09.02 Сетевая безопасность

Цель дисциплины

Целью изучения дисциплины является предоставление обучаемым 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

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ПКС-1	Способен разрабатывать, изменять и согласовывать архитектуры программного обеспечения с системным аналитиком и архитектором программного обеспечения	ПКС-1.1 Знать существующие архитектуры программного обеспечения. ПКС -1.2 Уметь использовать существующие архитектуры программного обеспечения. ПКС-1.3 Иметь навыки разработки и программного обеспечения различных архитектур.
ПКС-4	Способен проектировать программные интерфейсы	ПКС-4.1 Знать основные принципы проектирования программных интерфейсов. ПКС -4.2 Уметь использовать принципы проектирования программных интерфейсов. ПКС-4.3 Иметь навыки проектирования программных интерфейсов.

Содержание разделов дисциплины

7 семестр

Тема 1. Виды атак. Модель сетевой безопасности

Обобщенный сценарий атаки. Пассивная разведка. Активная разведка. Взлом целевой системы. Сокрытие следов взлома. Классификация атак. Модель сетевой безопасности.

Тема 2. Криптография и системы шифрования.

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 3. 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 4. 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 5. Механизмы межсетевой безопасности.
Межсетевые экраны. Фильтры пакетов. Фильтры инспекции состояний. Транслятор адресов. Транспортные шлюзы. Шлюзы приложений. Системы обнаружения атак и вторжений.

Тема 6. Системы тунелирования.
Протокол PPPoE. Виртуальные частные сети. Протокол IPSEC. Протокол SSL/TLS.

Тема 7. Безопасность удаленного управления.
Аудит безопасности протокола SNMP. Версии протокола SNMP. Протокол SNMPv3. Протокол SSH. Рекомендации по безопасности использования протокола SSH.