

Аннотация дисциплины С.1.1.27 Дисциплина. Безопасность вычислительных сетей

Дисциплина "Безопасность вычислительных сетей" изучается обучающимися по основной профессиональной образовательной программе "Безопасность автоматизированных систем критически важных объектов" направления подготовки "10.05.03 Информационная безопасность автоматизированных систем".

Дисциплина изучается в 5, 6 семестре. Общая трудоемкость дисциплины составляет 252/10 часов/з.ед. Самостоятельная работа заключается в выполнении работ, указанных в разделе 4.

В ходе изучения дисциплины осуществляется текущий контроль в форме технологии рейтингового контроля в соответствии с технологической карты дисциплины, размещенной на электронном курсе, а также промежуточный контроль в форме зачет, экзамен.

Целью изучения дисциплины является формирование следующих компетенций:

1. ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

В ходе изучения дисциплины последовательно рассматриваются темы:

1. Тема 1. Транспортная подсистема вычислительных сетей.
Транспортный уровень построения вычислительных сетей. Транспортные протоколы в Internet: TCP и UDP. Интерфейс Berkley Sockets. Угрозы безопасности и средства организации безопасного информационного взаимодействия в сетях TCP/IP.
2. Тема 2. Уровень приложений.
Представительский и прикладной уровни построения вычислительных сетей. Протоколы прикладного и представительского уровней сети Internet. Система DNS. Администрирование служб доменных имен.
3. Тема 3. Службы локальных вычислительных сетей.
Модель «клиент-сервер». Виды серверов и протоколы взаимодействия (HTTP, FTP, SMTP, RDP, SSH и другие). Основные сетевые службы прикладного уровня. Службы файлового обмена. Службы веб-серверов и электронной почты. Служба каталогов Active Directory. Политика безопасности и групповые политики. Решение задач администрирования Active Directory на базе ОС Windows Server. Решение задач администрирования Active Directory на базе ОС Windows Server. Решение задач администрирования веб-сервера, служб файлового обмена, сервера электронной почты, сервера баз данных.
4. Тема 4. Алгоритмы криптографической защиты информации в ЛВС.
Основные криптографические методы, используемые для защиты информации в вычислительных сетях. Понятие аутентификации. Виды аутентификации. Виды шифрования. Основные протоколы, используемые для защиты информации в вычислительных сетях. Протоколы аутентификации и шифрования с открытым ключом. Организация защищенного канала связи с использованием криптографических протоколов. Виртуальные частные сети. Протокол SSL.
5. Тема 5. Анализ защищенности ЛВС.
Методы и средства защиты информации в локальных вычислительных сетях. Понятие сетевая атака. Классификация сетевых атак. Виды сетевых атак и методы их реализации. Анализ защищенности и угроз безопасности ЛВС. Сетевое сканирование. Администрирование средств сетевого сканирования и реализации сетевых атак.
6. Тема 6. Средства контроля сетевого трафика в ЛВС.
Политика безопасности в локальной вычислительной сети. Понятие межсетевого экрана (МСЭ). Функции МСЭ. Классификация МСЭ. Способы реализации МСЭ. Модуль IPTables как средство реализации МСЭ. Настройка IPTables для решения

задач фильтрации и блокирования сетевого трафика. Средства контроля доступа к сетевым службам.

7. Тема 7. Средства обнаружения вторжений в ЛВС.
Классификация средств обнаружения вторжений (СОВ). Способы реализации СОВ. Сетевой анализатор Wireshark. Анализ сетевого трафика и угроз безопасности в ЛВС. Современные программно-аппаратные СОВ. Средства обеспечения безопасности внешнего периметра ЛВС (на примере модуля SNORT).

8. Тема 8. Безопасность в ЛВС.
Особенности эксплуатации локальных вычислительных сетей с учетом требований по обеспечению безопасности. Средства организации ложного информационного ресурса в ЛВС. Использование средств защиты информации в ЛВС с учетом требований по обеспечению безопасности. Защита информации в ЛВС на разных уровнях: физическом, канальном, сетевом, прикладном. Средства обнаружения несанкционированного доступа к информации на разных уровнях ЛВС. Администрирование ЛВС с учетом требований по обеспечению безопасности.

Основными стратегическими образовательными технологиями являются: лекционные занятия, практические и лабораторные занятия.

В рамках указанных технологий применяются тактические образовательные технологии: задания, классическая лекция.