

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

РЕКОМЕНДОВАНО К

УТВЕРЖДЕНИЮ:

Декан факультета КТ, ВТ и Э

председатель совета

 Ш.А. Юсуфов

17 10 2018 г.

УТВЕРЖДАЮ:

Проректор по учебной работе,
председатель методического совета

 ДГТУ
Н.С. Суракатов

24 10 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.Б22. Безопасность сетей ЭВМ
для специальности 10.05.03 Информационная безопасность автоматизированных систем
специализация Безопасность открытых информационных систем
факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина
кафедра Программного обеспечения вычислительной техники и автоматизированных систем
наименование кафедры, за которой закреплена дисциплина
Квалификация выпускника (степень) специалист
Форма обучения очная; курс 3; семестр(ы) 5,6;
Всего трудоемкость в зачетных единицах (часах) 8зет (288ч);
Лекции 51(час); Экзамен бсем; (1зет =36 часов);
Практические (семинарские) занятия- нет; Зачет - 5 (семестр);
Лабораторные занятия 68(час); Курсовая работа - нет (семестр);
Самостоятельная работа 133 (час).

Зав. кафедрой



/В.Б. Мелехин /

Начальник УО



/Э.В. Магомаева /

Махачкала – 2018 г.



Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по специальности 10.05.03-Информационная безопасность автоматизированных систем»

Программа одобрена на заседании выпускающей кафедры «Информационной безопасности» от 15.10.2018 г., протокол № 2

Зав. кафедрой ИБ 

Г.И. Качаева

ОДОБРЕНО:

Методической комиссией
по укрупненным группам специальностей
и направлений подготовки 10.00.00 –
«Информационная безопасность»

Председатель МК

В.Б. Мелехин.

подпись, И.О.Ф.

15.10

2018

АВТОР(Ы) ПРОГРАММЫ:

д.т.н., проф. В.Б.Мелехин
И.О.Ф., уч. степень, ученое звание


подпись

1. Цель освоения дисциплины

Целью изучения дисциплины «Безопасность сетей ЭВМ» является теоретическая и практическая подготовка специалистов в области построения сетей ЭВМ и обеспечения безопасности при эксплуатации сетей ЭВМ.

Задачи:

- изучение основных элементов теории построения сетей;
- изучение основных принципов функционирования сетевых протоколов;
- привитие навыков комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей;
- изучение основных угроз в сетях ЭВМ и методов противодействия им;
- овладение механизмами построения систем безопасности сетей ЭВМ.

2. Место дисциплины в структуре ООП

Дисциплина «Безопасность сетей ЭВМ» относится к числу дисциплин базовой части учебного плана.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

- «Информатика» – знать формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей;
- «Языки программирования» – знать язык программирования высокого уровня (объектно-ориентированное программирование), уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;
- «Основы информационной безопасности» – знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, владеть профессиональной терминологией в области информационной безопасности;
- «Сети и системы передачи информации» – знать основные характеристики сигналов электросвязи, спектры и виды модуляции, принципы построения и функционирования систем и сетей передачи информации, способы кодирования информации, основные телекоммуникационные протоколы.

Дисциплина «Безопасность сетей ЭВМ» является предшествующей для изучения следующих базовых дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», «Организация ЭВМ и вычислительных систем», «Безопасность систем баз данных», «Программно-аппаратные средства обеспечения информационной безопасности».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

Процесс изучения дисциплины направлен на формирование следующих компетенций:
-способностью проводить анализ защищенности автоматизированных систем (ПК-3);
-способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке

- программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);
 - способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

В результате изучения дисциплины студент должен:

знать:

- принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;
- основные протоколы сетей ЭВМ;
 - последовательность и содержание этапов построения компьютерных сетей;
 - эталонную модель взаимодействия открытых систем;
 - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ;

уметь:

- проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;
- эффективно использовать различные методы и средства защиты информации для компьютерных сетей;
- проводить мониторинг угроз безопасности компьютерных сетей;

владеть:

- навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
- навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;
- навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ.

4. Структура и содержание дисциплины (модуля) «Безопасность сетей ЭВМ»

Общая трудоемкость дисциплины составляет 8 зачетных единицы-288 часов, в том числе –лекционных 51 часов, лабораторных занятий 68 часов, СРС 133 часов, форма отчетности: 5 семестр- зачет, 6 семестр экзамен- (1зет =36 часов).

4.1. Содержание дисциплины

| № п/п | Раздел дисциплины Тема лекции и вопросы | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | | | Формы текущего контроля (по срокам текущей аттестации) |
|-------|---|---------|-----------------|--|----|----|-----|--|
| | | | | ЛК | ПЗ | ЛР | СРС | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | Лекция №1 Тема: Основы организации и функционирования сетей ЭВМ. Классификация сетей.1 1..Структура информационной сети. 2.Основные характеристики компьютерных сетей. 3. Система пакетной обработки. 4. Локальные вычислительные сети 5. Региональные вычислительные сети 6. Глобальные сети вычислительные сети. | 5 | 1 | 2 | | | 6 | Входная контрольная работа |
| 2 | ЛЕКЦИЯ №2 Тема: Среды передачи информации. 1. Витая пара. 2. Коаксиальный кабель. 3. Волоконно-оптический кабель. | 5 | 3 | 2 | | 4 | 6 | |
| 3 | ЛЕКЦИЯ №3 Тема: Уровни сетевой архитектуры и протоколы. 1. Эталонная модель взаимосвязи открытых систем OSI. 2. Структура пакета ЛВС | | 5 | 2 | | 4 | 6 | Аттестационная контрольная работа №1 |
| 4 | ЛЕКЦИЯ №4 Тема: стек протоколов TCP/IP 1. Протоколы уровня приложений 2. Протоколы транспортного уровня 3. Протоколы сетевого уровня. 4. Протоколы канального уровня. 5. Протоколы физического уровня | 5 | 7 | 2 | | 4 | 6 | |
| 5 | ЛЕКЦИЯ №5 Протоколы сетевого уровня IP, ARP 1. Функции протоколов IP, ARP. 2. Логические IP адреса. 3. Физические MAC адреса. | 5 | 9 | 2 | | 4 | 6 | Аттестационная контрольная работа №2 |

| | | | | | | | | |
|---------------------------|---|---|----|-----------|--|-----------|-----------|--------------------------------------|
| 6 | ЛЕКЦИЯ №6 Тема: Транспортные протоколы в Internet: TCP и UDP. 1. Установление соединения. 2. Порты. 3. Мультиплексирование. | 5 | 11 | 2 | | 4 | 6 | |
| 7 | ЛЕКЦИЯ №7 Маршрутизация и протоколы маршрутизации. 1. Принципы маршрутизации в сетях. 2. Протокол маршрутизации RIP. Построение таблицы маршрутизации. 3. Построение сетей с бесклассовой адресацией | 5 | 13 | 2 | | 4 | 7 | |
| 8 | ЛЕКЦИЯ №8 Тема: DNS-система доменных имен 1. Иерархические символьные имена. 2. Файлы зоны. Зона прямого и обратного просмотра. 3. Способы разрешения адресов. | 5 | 15 | 2 | | 4 | 7 | Аттестационная контрольная работа №3 |
| 9 | ЛЕКЦИЯ №2 Тема: Способы коммутации в сетях. 1. Коммутация каналов. Разделение каналов по времени и частоте. Коммутация пакетов. | 5 | 17 | 1 | | 6 | 7 | |
| Итого за 5 семестр | | | | 17 | | 34 | 57 | Зачет |
| 10 | ЛЕКЦИЯ №10 Тема: Сетевые операционные системы. 1. Архитектура СОС. 2. Характеристика сетевой ОС Windows 2012. 3. Настройка роли сервера 4. Служба каталогов Active Directory в ОС Windows 2012. 5. Настройка DNS в ОС Windows 2012. 6. Подключение к домену. 7. Настройка групповых политик в ОС. Windows 2012. 8. Службы. | 6 | 1 | 2 | | 4 | 4 | |
| 11 | ЛЕКЦИЯ №11 Сетевые информационные службы. 1. Информационные службы IP: Web-служба, почтовая служба, IP-телефония. 2. Сетевая файловая служба. 3. Служба управления сетью. | 6 | 2 | 2 | | 4 | 4 | |

| | | | | | | | | |
|----|--|---|---|---|--|---|---|-----------------------|
| 12 | ЛЕКЦИЯ №12 Тема: Стандартные локальные сети 1. Топологии сетей. 2. Аппаратура, структура пакета, метод доступа, среды передачи. 3. Стандартные сегменты Fast Ethernet и Gigabit Ethernet. | 6 | 3 | 2 | | | 4 | |
| 13 | ЛЕКЦИЯ №13 Тема: Стандартные локальные сети. 1. Сеть Token-Ring (аппаратура, структура пакета, метод доступа, среды передачи). 2. Сеть FDDI. | 6 | 4 | 2 | | | 4 | |
| 14 | ЛЕКЦИЯ №14 Тема: Методы доступа в сетях. 1. Маркерный метод доступа. 2. Метод доступа с контролем несущей и обнаружением коллизий- CSMA/CD | 6 | 5 | 2 | | | 4 | Аттестационная К/р №1 |
| 15 | ЛЕКЦИЯ №15 Тема: Активное сетевое оборудование 1. Сетевой «проводной» адаптер. 2. Сетевой беспроводной адаптер. 3. Концентратор. 4. Мост. 5. Коммутатор. 6. Маршрутизатор. | 6 | 6 | 2 | | 4 | 4 | |
| 16 | ЛЕКЦИЯ №16 Тема: Пассивное сетевое оборудование 1. Монтажный шкаф 2. Кросс-панель 3. Сетевой кабель 4. Патч-корд, кросс-корд 5. Коннекторы. | 6 | 7 | 2 | | | 4 | |
| 17 | ЛЕКЦИЯ №17 Тема: Виртуальные локальные сети VLAN 1. Коммутация и виртуальные 2. Локальные сети VLAN 3. Протокол Spanning-Tree и VLAN 4. Настройка VLAN по умолчанию 5. Настройка VLAN через домен 6. Группирование портов коммутатора в VLAN 7. Настройка транков. | 6 | 8 | 2 | | 4 | 4 | |
| 18 | ЛЕКЦИЯ №18 Тема: Глобальные сети | 6 | 9 | 2 | | | 4 | |

| | | | | | | | | |
|----|---|---|----|---|--|---|---|----------------------|
| | 1. Принципы организации ГВС. 2. Коммутируемые соединения по модему. 3. Постоянное соединение по выделенной линии: цифровые выделенные линии. 4. Сети ISDN и ADSL. | | | | | | | |
| 19 | ЛЕКЦИЯ №19 Технология виртуальных каналов. 1. Принцип работы виртуального канала 2. Технология X.25. 3. Технология Frame Relay. 4. Технология ATM. | 6 | 10 | 2 | | 4 | 5 | Аттестационная К/р№2 |
| 20 | ЛЕКЦИЯ №20 Тема: Правовое обеспечение информационной безопасности вычислительных сетей 1. Стандарты безопасности вычислительных сетей и их компонентов. 2. Показатели защищенности от НСД к информации. 3. Правовые основы защиты информации в компьютерных сетях. | 6 | 11 | 2 | | | 5 | |
| 21 | ЛЕКЦИЯ №21 Тема: Инструменты мониторинга и анализа сети. 1. Классификация средств мониторинга и анализа. 2. Анализаторы протоколов. 3. Сетевые анализаторы. 4. Кабельные сканеры. 5. Тестеры. | 6 | 12 | 2 | | 4 | 5 | |
| 22 | ЛЕКЦИЯ №22 Тема: Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия 1. Понятие и классификация атак на компьютерные сети. 2. Основные типы сетевых атак. Средства реализации атак. 3. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. 4. Технологии обнаружения компьютерных атак и их возможности. 5. Сигнатурный анализ и обнаружение аномалий. 6. Классификация систем | 6 | 13 | 2 | | 4 | 5 | |

| | | | | | | | | |
|----|--|---|----|---|--|---|---|----------------------|
| | обнаружения атак (СОА). | | | | | | | |
| 23 | ЛЕКЦИЯ №23 Тема: Технология межсетевого экранирования 1. Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. 2. Типы межсетевых экранов. Схемы межсетевого экранирования. 3. Фильтрация пакетов. 4. Понятие демилитаризованной зоны. Шлюзы прикладного уровня. 5. Контроль HTTP-трафика и электронной почты. | 6 | 14 | 2 | | 2 | 5 | |
| 24 | ЛЕКЦИЯ №24 Тема: Построение безопасности он основе VPN 1. Задачи, решаемые VPN. Туннелирование в VPN. 2. Организация VPN средствами протокола PPTP. 3. Установка и настройка VPN. 4. Анализ защищенности передаваемой информации. 5. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. | 6 | 15 | 2 | | 2 | 5 | Аттестационная К/р№3 |
| 25 | ЛЕКЦИЯ №25 Тема: Аудит информационной безопасности в компьютерных сетях. 1. Цели и задачи проведения аудита безопасности. Определение структуры информационно-телекоммуникационных сетей. 2. Программные средства анализа топологии вычислительной сети. 3. Определение маршрутов прохождения сетевых пакетов. 4. Обнаружение объектов сети. Построение схемы сети. 5. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. 6. Применение систем автоматизированного построения схемы сети. Цели и принципы зондирования узлов сети. | 6 | 16 | 2 | | 2 | 5 | |

| | | | | | | | | |
|----|--|---|----|-----------|--|-----------|------------|---------------------------------|
| 26 | ЛЕКЦИЯ №26 Тема: Подбор паролей к ресурсам 1. Способы удаленного подбора паролей. 2. Подбор паролей с локального хоста. 3. Подбор паролей с удаленного сервера. 4. Сборка программы hydra. Опции программы hydra 5. Подбор пароля к почтовому ящику. 6. Подбор пароля к общим ресурсам. | 6 | 17 | 2 | | 4 | 5 | |
| | Итого за 6 семестр | | | 34 | | 34 | 76 | Экзамен (1зет =36 часов) |
| | ИТОГО за 5, 6 семестры | | | 51 | | 68 | 133 | |

4.2 Содержание лабораторных занятий

| № п/п | № лекции из рабочей программы | Наименование лабораторного занятия | Кол-во часов | № литер. источника из списка литературы |
|------------------------------|-------------------------------|--|--------------|---|
| 1 | Лк.2 | Основные команды операционной системы Cisco IOS. Построение логической структуры сети с общей разделяемой средой в Cisco Packet Tracer и исследование ее пропускной способности. | 4 | 1-9 |
| 2 | Лк. 3 | Управление правами доступа. | 4 | 1-9 |
| 3 | Лк.4 | Конфигурирование IP адресов на интересах маршрутизаторов | 4 | 1-9 |
| 4 | Лк. 5 | Сетевые утилиты | 4 | 1-9 |
| 5 | Лк.6 | Построение сети с безклассовой адресацией. | 4 | 1-9 |
| 6 | Лк.7 | Настройка статической маршрутизации. Построение таблиц маршрутизации | 4 | 1-9 |
| 7 | Лк.8 | Настройка динамической маршрутизации. Протокол RIP. | 4 | 1-9 |
| 8 | Лк 9 | Настройка DNS | 4 | 1-9 |
| 9 | Лк. 9 | Настройка NAT | 2 | 1-9 |
| Итого за 5 семестр | | | 34 | |
| 1 | Лк.10 | Базовая настройка DHCP на маршрутизаторе Cisco. | 4 | 1-9 |
| 2 | Лк.11 | Анализ протоколов уровня приложения и транспорта. | 4 | 1-9 |
| 3 | Лк.15 | Конфигурирование port security на коммутаторах Cisco | 4 | 1-9 |
| 4 | Лк.17 | Настройка VLAN на коммутаторах Cisco | 4 | 1-9 |
| 5 | Лк.19 | Конфигурирование Frame Relay с подынтерфейсами "точка-точка". | 4 | 1-9 |
| 6 | Лк.21 | Изучение средств мониторинга и анализа сетевого трафика. Сниффер Wireshark | 4 | 1-9 |
| 7 | Лк.22 | Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer. | 4 | 1-9 |
| 8 | Лк.23 | Защита сети посредством установки и настройки межсетевого экрана. | 2 | 11-9 |
| 9 | Лк.24 | Создание VPN туннеля для удаленного подключения пользователей к защищенной сети | 2 | 1-9 |
| 10 | Лк.25 | Анализ топологии вычислительной сети | 2 | 1-9 |
| Итого за 6 семестр | | | 34 | |
| ИТОГО за 5,6 семестры | | | 68 | |

4.3 Тематика для самостоятельной работы студента

| № п/п | Тематика по содержанию дисциплины, выделенная для самостоятельного изучения | Кол-во часов из содержания дисциплины | Рекомендуемая литература и источники информации | Форма контроля СРС |
|------------------------------|---|---------------------------------------|---|-----------------------------|
| 1 | Понятие и виды телекоммуникационной сети. Кодирование информации в сетях. Корпоративные сети. Городские сети. | 6 | 1-7 | Устный опрос, аттест. к/р№1 |
| 2 | Беспроводные сети | 6 | 1-9 | |
| 3 | Стандартизация сетей. Понятие открытой системы взаимодействия. Стандартизация Интернета. | 6 | 1-9 | |
| 4 | Протоколы уровня представления. Протоколы сеансового уровня | 6 | 1-9 | Устный опрос, аттест. к/р№2 |
| 5 | Заголовки протоколов IP, ARP | 6 | 1-9 | |
| 6 | Управление потоком протокола TCP | 6 | | Устный опрос, аттест. к/р№3 |
| 7 | Протокол OSPF, BGP | 6 | 1-9 | |
| 8 | База данных DNS. Типы серверов DNS. | 6 | 1-9 | |
| 9 | Коммутация сообщений. Радиоканал, инфракрасный канал. | 6 | 1-9 | Зачетная к/р. |
| Итого за 5 семестр | | 57 | | Зачет |
| 10 | Ознакомление с ОС UNIX. | 4 | 1-9 | Устный опрос, аттест. к/р№1 |
| 11 | Сетевая служба DHCP | 4 | 1-9 | |
| 12 | Стандартные сегменты Gigabit Ethernet | 4 | 1-9 | |
| 13 | Сеть 100 VG Any Lan. | 4 | 1-9 | |
| 14 | Методы доступа | 4 | 1-9 | |
| 15 | Точка доступа. Модем. Антенна | 4 | 1-9 | Устный опрос, аттест. к/р№2 |
| 16 | Розетка RJ-45. Инструменты для работы с кабелем. | 4 | 1-9 | |
| 17 | Принципы создания сетей на основе VLAN | 4 | 1-9 | |
| 18 | Интернет провайдеры | 4 | 1-9 | |
| 19 | Сети Frame Relay, ATM. | 5 | | Устный опрос, аттест. к/р№3 |
| 20 | Политика сетевой защиты. | 5 | 1-9 | |
| 21 | Агенты SNMP Агенты RMON. | 5 | | |
| 22 | Угрозы межсетевого взаимодействия | 5 | 1-9 | |
| 23 | Обзор документов RFC, регламентирующих использование межсетевых экранов. | 5 | 1-9 | |
| 24 | Настройка политики межсетевого экранирования с использованием протокола IPSec. | 5 | 1-9 | |
| 25 | Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. | 5 | 1-9 | |
| 26 | Защита паролем | 5 | 1-9 | |
| Итого за 6 семестр | | 76 | | Экзамен |
| ИТОГО за 5,6 семестры | | 133 | | |

5. Образовательные технологии

В рамках учебных курсов должны быть предусмотрены встречи с представителями российских сетевых организаций, мастер-классы экспертов и специалистов.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 20% аудиторных занятий (определяется требованиями ГОС с учетом специфики ООП). Занятия лекционного типа для соответствующих групп студентов не могут составлять более 40% аудиторных занятий (определяется соответствующим ГОС).

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Входная контрольная

1. Понятие сети ЭВМ. Этапы развития сетей ЭВМ.
2. Какие задачи решает сеть?
3. Сервисы сети Интернет.
4. Основные характеристики компьютерных сетей.
5. Первые компьютерные сети.
6. Интернет как фактор развития сетевых технологий.
7. Простейшая сеть из двух компьютеров.
8. Как осуществляет связь компьютера с периферийными устройствами.
9. Совместное использование ресурсов.

Аттестационная контрольная работа №1 5 семестра

1. История развития ЛВС, ГВС.
 2. Проектирование сетей ЭВМ по принципу «Клиент-сервер».
3. Среды передачи информации.
4. Топологии сетей.
5. Конвергенция сетей. Сближение локальных и глобальных сетей.
6. Критерии классификации сетей ЭВМ.
7. Характеристики сетей ЭВМ. Средства построения сетей ЭВМ.
8. Логическая и физическая структуризация сетей ЭВМ.
9. Пакетная передача данных.
10. Модель ISO OSI.
11. Стандартные стеки коммуникационных протоколов.

Аттестационная контрольная работа №2 5 семестра

1. Протоколы прикладного уровня. Краткая характеристика HTTP, FTP, SMTP.
2. Протоколы сетевого уровня IP, ARP
3. Протоколы канального уровня.
4. Протоколы физического уровня.
5. Протоколы сетевого уровня IP, ARP
6. Физический адрес хоста.
7. Протокол автоматической конфигурации DHCP.

8. Протоколы маршрутизации.
9. Угрозы безопасности информации, передаваемой в сетях ЭВМ, на физическом и канальном уровнях. Методы их нейтрализации.

**Аттестационная контрольная работа №3
5 семестра**

1. Транспортные протоколы в Internet: TCP и UDP.
2. Архитектура сетевых операционных
3. Маршрутизация и протоколы маршрутизации.
4. Протоколы внешней маршрутизации.
5. Бесклассовая адресация.
6. Построение таблиц маршрутизации.
7. Доменная система имен.
8. Иерархическая структура доменных имен.
9. Коммутация каналов. Коммутация сообщений.
10. Пакетная коммутация.

**Аттестационная контрольная работа №1
6 семестра**

1. Структура сетевой операционной системы.
2. Сетевые службы.
3. Подключение к домену.
4. Методы доступа в сетях.
5. Метод доступа с контролем несущей и обнаружением коллизий-CSMA/CD.
6. Маркерный метод доступа
7. Настройка групповых политик.
8. Служба каталогов Active Directory.
9. IP-телефония.
10. Технологии локальных сетей.
11. Сеть Token-Ring.

**Аттестационная контрольная работа №2
6 семестра**

1. Активное сетевое оборудование.
2. Функции концентратора
3. Функции сетевого адаптера.
4. Функции маршрутизатора.
5. Коммутаторы VLAN
6. Локальные сети на основе VLAN.
7. Пассивное сетевое оборудование.
8. Коннекторы, сетевой кабель
9. Виртуальные локальные сети.
10. Глобальные вычислительные сети: принципы построения, структура.
11. Технологии глобальных сетей.
12. Интернет провайдер.

**Аттестационная контрольная работа №3
6 семестра**

1. Правовые основы защиты информации в компьютерных сетях.
2. Стандарты безопасности вычислительных сетей
3. Типы атак и способы защиты от них.
4. Технология межсетевого экранирования.
5. Основные типы сетевых атак.
6. Безопасность сетей на основе VPN.
7. Анализ и мониторинг сетей.
8. Технологии обнаружения компьютерных атак.
9. Понятие демилитаризованной зоны.

Вопросы проверки остаточных знаний

1. Агенты SNMP.
2. Агенты RMON.
3. Способы удаленного подбора паролей.
4. Подбор паролей с локального хоста.
5. Настройка маршрутизатора Cisco.
6. Буферизация пакетов.
7. Передача с установление виртуального канала.
8. Пропускная способность сети.
9. Методы обеспечения качества обслуживания.
10. Формат кадров технологии Ethernet.
11. Логическая структуризация сетей.
12. Архитектура коммутатор.

Вопросы к зачету

1. Понятие сети ЭВМ. Этапы развития сетей ЭВМ.
2. Критерии классификации сетей ЭВМ. Характеристики сетей ЭВМ.
3. Средства построения сетей ЭВМ. Логическая и физическая структуризация сетей ЭВМ.
4. Модель ISO OSI. Стандартные стеки коммуникационных протоколов. Технологии обеспечения безопасности в сетях ЭВМ.
5. Физический уровень построения вычислительных сетей.
6. Стандарты кабелей, используемых для построения сетей.
7. Структурированная кабельная система. Беспроводные сети.
8. Канальный уровень построения вычислительных сетей.
9. Методы доступа к разделяемой среде. Методы коммутации.
10. Угрозы безопасности информации, передаваемой в сетях ЭВМ, на физическом и канальном уровнях. Методы их нейтрализации.
11. Стандарты IEEE 802.x. Управление логическим каналом, метод доступа к разделяемой среде CSMA/CD.
12. Форматы кадров технологии Ethernet.
13. Стандарты физической среды технологии Ethernet. Методика расчета сетей Ethernet.
14. Технологии Token Ring, FDDI. Интерфейс Berkley Sockets. Высокоскоростные технологии построения ЛВС: 100VGAnyLan, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet.
15. Технологии VLAN.
16. Угрозы безопасности информации, передаваемой в локальных сетях ЭВМ. Методы их нейтрализации.

27. АТМ-сети.
28. Локальные сети на основе VLAN.
29. Правовые основы защиты информации в компьютерных сетях.
30. Безопасность сетей на основе VPN.
31. Стандарты безопасности вычислительных сетей
32. Типы атак и способы защиты от них.
33. Технология межсетевого экранирования.
34. Основные типы сетевых атак.
35. Безопасность сетей на основе VPN.
36. Анализ и мониторинг сетей.
37. Способы удаленного подбора паролей.
38. Подбор паролей с локального хоста.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Рекомендуемая литература и источники информации

(основная и дополнительная)

и. о. зав. каф. МЯ

| № | Виды занятий | Необходимая учебная, учебно-методическая литература, программное обеспечение и Интернет ресурсы | Автор (ы) | Издательство и год издания | Кол-во пособий, учебников и прочей литературы | |
|---------------------------|--------------|---|--|---|---|----------------|
| | | | | | в библи. | на кафедр. |
| Основная литература | | | | | | |
| 1 | лк | Сети TCP/IP. Принципы, протоколы и структура. | Камер Д.Э | Издат. Дом «Вильямс», 2003 | 3 | |
| 2 | лк | Безопасность глобальных сетевых технологий | Зима В.М. | БХВ-Петербург, 2003. | 3 | |
| 3 | лк | Телекоммуникационные системы и сети. | Шувалов В.П | Горячая линия. Телеком, 2004 | 3 | |
| 4 | лк | Информационная защита ПК | Бенкс М.А. | «Корона-Принт», 2001. | 3 | |
| 5 | лк | Локальные сети: архитектура, алгоритмы, проектирование. | Новиков Э.В. | ЭКОМ, 2000. | | 3 |
| 6 | лк | Компьютерные сети. Модернизация и поиск. | Закер К. | БХВ-Петербург. | - | 1 |
| 7 | лк | TCP/IP. Семейство протоколов передачи данных в сетях компьютеров. | Остерлох Хазер | ДиаСофт ЮП, 2002. | - | 1 |
| 8 | лк, лб | Основы информационной безопасности | Курс лекций : учебное пособие / Издание третье / Галатенко В.А. Под ред. Академика РАН В.Б. Бетелина | М.:ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. - 208 с. | - | - |
| 9 | лк | Безопасность сетей. | Брэгг Р. | М.: Эком, 2006. | | Сетевой ресурс |
| 10 | лк | Защита сетевого периметра | Норткат Стивен и др. | К.: ООО «ТИД «ДС», 2007. | | Сетевой ресурс |
| 11 | лк | Обнаружение нарушений безопасности в сетях | Норткат С., Новак Д. | М.: Издательский дом «Вильямс», 2008. | | Сетевой ресурс |
| Дополнительная литература | | | | | | |
| 12 | лк, лб | Брандмауэры в Linux | Зинглер Р.Л. | Вильямс, 2010. | 1 | 1 |
| 13 | лк | Сети Интранет, Серия «Стратегические технологии» | Грир Т. | Ченнел Трейдинг Лимитед, 2010 | 1 | - |
| 14 | лк, лб | Мультимедиа-системы | Мячев А. А. и др. | М.: Радио и связь. - 2005. | 1 | 1 |
| 15 | лк | Интерфейсы и сети ЭВМ: | Мячев А. А. | М.: Радио и связь. - 2004. | 1 | 1 |