МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа
и операторных уравнений

Каменский М.И.
25.05.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.03.02 Безопасность сетей ЭВМ

1. Код и наименование направления специальности: 10.05.04 информационно-аналитические системы безопасности

2. Профиль специализации: Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: функционального анализа и операторных уравнений

6. Составители программы: Завгородний Михаил Григорьевич, кандидат физико-математических наук.

7. Рекомендована: научно-методическим советом математического факультета, протокол от 25.05.2023, № 0500-06

8. Учебный год: 2024-2025, 2025-2026 **Семестр:** 4,5

9. Цели и задачи учебной дисциплины:

Цели изучения дисциплины:
- формирование у студентов компетентности в области информационной безопасности сетей ЭВМ;
- изучение методов и средств обеспечения защиты информации при передаче ее по каналам связи от нарушения конфиденциальности, целостности и доступности информации.
Задачи учебной дисциплины:
- изучение базовой инфраструктуры сетей ЭВМ, основных устройств и систем, требований к обеспечению информационной безопасности, соответствующих стандартов, технических спецификаций, протоколов и технологий;
- формирование умений по созданию, настройке и эксплуатации безопасных сетей ЭВМ
- овладение навыками по использованию компонентов защищенных сетей ЭВМ, способностью разрабатывать модели угроз и модели нарушителей ИБ на основе исходных данных о сети

10. Место учебной дисциплины в структуре ООП: дисциплина Безопасность сетей ЭВМ относится к обязательной части блока Б1.

Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Дискретная математика, Информатика, Математическая логика и теория алгоритмов, Языки программирования, Технология и методы программирования, Основы информационной безопасности. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при изучении курсов: Безопасность операционных систем (операционные системы и их безопасность), Безопасность программного обеспечения, Безопасность информационно-аналитических систем, Моделирование информационно-аналитических систем, Принципы построения, проектирования и эксплуатации информационно-аналитических систем, Безопасность программного обеспечения, Безопасность автоматизированных систем управления технологическим процессом, а также при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области информационной безопасности и защиты информации.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Коды	Индикаторы	Планируемые результаты обучения
ОПК-11	Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей	ОПК-11.3	Осуществляет меры противодействия нарушениям безопасности с использованием различных программных и	**знать:** основные возможности и принципы построения сетей ЭВМ; основные понятий по безопасности сетей ЭВМ требования, предъявляемые к системе защиты современных

	частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации		аппаратных средств защиты	ОС; **уметь:** оценивать эффективность и надежность сетей ЭВМ; выявлять имеющие место проблемные места в защите и использовать комплекс мероприятий для обеспечения защиты; **владеть:** навыками построения и настройки современных сетей ЭВМ;
ОПК-13	Способен производить настройку и обслуживание компонентов обеспечивающей части информационно-аналитических систем на всех этапах жизненного цикла, встроенных средств защиты информации, восстанавливать их работоспособность при внештатных ситуациях	ОПК-13.4	Настраивает, обслуживает и восстанавливает средства защиты информации на всех этапах жизненного цикла информационно-аналитических систем	**знать:** организацию управления доступом и защиты ресурсов сетей ЭВМ; основные механизмы безопасности; **уметь:** Настраивать, обслуживать и восстанавливать средства защиты информации на всех этапах жизненного цикла информационно-аналитических систем **владеть:** навыками применения методов обеспечения безопасности сетей ЭВМ;
		ОПК-13.5	Способен администрировать системы управления базами данных, операционные системы и компьютерные сети	**знать:** применяемые на практике критерии и методы оценивания эффективности и надежности средств защиты используемых сетей ЭВМ; **уметь:** администрировать системы управления базами данных, операционные системы и компьютерные сети; **владеть:** навыками администрирования систем управления базами данных, операционными системами и компьютерными сетями. применения действующую законодательную базу в области информационной безопасности;

12 Объем дисциплины в зачетных единицах/час.— 6/216

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость		
	Всего	По семестрам	
		сем. № 4	сем. № 5
Аудиторные занятия	*122*	*50*	*72*
в том числе: лекции	*68*	*34*	34
практические	-	-	-
лабораторные	*50*	*16*	34
Самостоятельная работа	*62*	*22*	40
Экзамен	*36*	-	36
Итого:	*216*	*72*	*144*

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Основные понятия компьютерных сетей. Определение локальных сетей и их топология	Основные понятия компьютерных сетей. История компьютерных сетей. Типы сетевых архитектур. Типы серверов. Отличия сетевых топологий. Требования, предъявляемые к современным вычислительным сетям.
2	Типы линий связи локальных сетей. Подключение линий связи и коды передачи информации	Типы, особенности, принципы функционирования, правила использования линий связи, применяемых в локальных сетях. Принципы подключения электрических линий связи в локальных сетях, методах их согласования, а также о кодах передачи информации. Методы цифрового кодирования. Способы модуляции
3	Пакеты, протоколы. Методы управления обменом	Принципы передачи информации по сети. Назначение и типы информационных пакетов, структура пакетов. Методы управления обменом в сетях с разной топологией. Стандартные стеки коммуникационных протоколов. Способы разделения канала по частоте и времени.
4	Сетевая модель OSI	Стандартная модель взаимодействия открытых систем OSI, уровни функций, выполняемых при взаимодействии по сети. Возможности сетевых адаптеров и промежуточных сетевых устройств. Функции модели OSI, реализуемых программно, стандартные протоколы обмена, их достоинствах и недостатках, типы сетевых программных средств и особенности сетевых программ крупнейших производителей. Принципы работы протоколов разных уровней
5	Физический уровень модели OSI. Технология Ethernet	Характеристики линий связи. Типы кабелей. Коннекторы. Модуляция. Методы кодирования. Формат кадра Ethernet. Передача данных. Физическая среда. Технологии Fast Ethernet, Gigabit Ethernet, 10G Ethernet.
6	Канальный уровень модели OSI. Коммутаторы	Подуровни канального уровня. MAC-адреса. Протокол ARP. Разделяемая среда, методы доступа. Неразделяемая среда. Беспроводные технологии. Принципы работы коммутатора. Алгоритм покрывающего дерева. Виртуальные сети (VLAN). Иерархическая сетевая модель.
7	Адресация в сетях IP	Типы IPv4-адресов. Формат IP-адреса. Классовая

		адресация. Бесклассовая адресация. Маска сети. Распределение адресов. Особые IP-адреса. Технология NAT. Адреса IPv6.
8	Транспортный и сетевой уровни модели OSI. Маршрутизация	Порты. Протокол UDP. Стек протоколов TCP/IP. Форматы пакетов TCP и IP. Протокол ICMP. Протокол IPv6. Сравнение и применение протоколов. Задачи, решаемые маршрутизатором. Таблица маршрутизации. Статическая маршрутизация. Виды протоколов динамической маршрутизации. Дистанционно-векторные протоколы: RIPv1 и RIPv2. Протоколы состояния каналов связи: OSPF.
9	Верхние уровни модели OSI	Клиент-серверная модель и одноранговые сети. Протокол Telnet. Система доменных имен. Протокол DHCP. Протокол HTTP. Электронная почта.
10	Беспроводные сети	Распространение электромагнитных волн. Лицензирование частот. Технология широкополосного сигнала. Физические уровни стандарта 802.11. Технология Bluetooth. Безопасность беспроводных сетей.
11	Стандарты информационной безопасности	Стандарты информационной безопасности. Роль стандартов информационной безопасности. Международный стандарт ISO 15408. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернете.
12	Обнаружение компьютерных атак	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.
13	Технология межсетевого экранирования	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows. Служба RRAS. Программа управления службой RRAS. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого.
14	Организация виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и

		настройка VPN. Анализ защищенности передаваемой информации. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения. Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server 2003. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.
15	Технологии защищенной обработки информации	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2003. Настройка сервера MSTS. Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
16	Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений. Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратно-программных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.

13.2. Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Основные понятия компьютерных сетей. Определение локальных сетей и их топология	2	-	1	3
2	Типы линий связи локальных сетей. Подключение линий связи и коды передачи информации	2	1	1	4
3	Пакеты, протоколы. Методы управления обменом	2	1	2	5
4	Сетевая модель OSI	2	-	2	4
5	Физический уровень модели OSI. Технология Ethernet	4	2	4	10
6	Канальный уровень модели OSI. Коммутаторы	4	2	2	8
7	Адресация в сетях IP	4	4	4	12
8	Транспортный и сетевой уровни модели OSI. Маршрутизация	6	2	2	10
9	Верхние уровни модели OSI	4	2	2	8
10	Беспроводные сети	4	2	2	8
11	Стандарты информационной безопасности	2	-	4	6
12	Обнаружение компьютерных атак	8	12	10	30
13	Технология межсетевого экранирования	6	6	6	18
14	Организация виртуальных частных сетей	6	6	6	18
15	Технологии защищенной обработки информации	6	6	6	18
16	Аудит информационной безопасности в компьютерных сетях	8	6	4	18
	Экзамен				36
	Итого	68	50	62	216

14. Методические указания для обучающихся по освоению дисциплины

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся. На лекциях рассказывается теоретический материал, на лабораторных занятиях решаются примеры по теоретическому материалу, прочитанному на лекциях.

При изучении курса «Безопасность сетей ЭВМ» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных

занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения, разобрать примеры, решенные на лекции. Перед следующей лекций обязательно повторить материал предыдущей лекции.

2. Перед лабораторным занятием обязательно повторить лекционный материал. После лабораторного занятия еще раз разобрать решенные на этом занятии примеры, после чего приступить к выполнению домашнего задания. Если при решении примеров, заданных на дом, возникнут вопросы, обязательно задать на следующем лабораторном занятии или в присутственный час преподавателю.

3. При подготовке к лабораторным занятиям повторить основные понятия по темам, изучить примеры. Решая задачи, предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить практические задачи.

4. Выбрать время для работы с литературой по дисциплине в библиотеке: каждый вторник с 15:00 до 18:00

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	*Таненбаум, Эндрю. Компьютерные сети = Computer Networks / Э. Таненбаум ; [пер. с англ. В. Шрага] .— 4-е изд. — СПб. [и др.] : Питер, 2009 .— 991 с. : ил., табл. — (Классика Computer Science) .— Библиогр.: с.952-970 .— Алф. указ.: с.971-991 .— ISBN 978-5-318-00492-6.*
2	*Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.*

б) дополнительная литература:

№ п/п	Источник
3	*Таненбаум, Эндрю. Компьютерные сети / Э. Таненбаум .— 4-е изд. — СПб. : Питер, 2005 .— 991 с. : ил., табл. — (Классика Computer Science) .— Парал. тит. л. англ. — ISBN 5-318-00492-X.*
4	*Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин .— Екатеринбург : Изд-во Уральского ун-та, 2003 .— 327 с. : ил .— Библиогр.:с.317-322 .— Алф.-предм. указ.: с.306-316 .— ISBN 5-86037-024-5.*
5	*Голуб, Владимир Александрович. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — ISBN 5-86026-020-2 : 37.00 .— <URL:http://www.lib.vsu.ru/elib/books/b102829.djvu>.*

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	*www.fstec.ru, www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .*

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	*Таненбаум, Эндрю. Компьютерные сети / Э. Таненбаум .— 4-е изд. — СПб. : Питер, 2005 .— 991 с. : ил., табл. — (Классика Computer Science) .— Парал. тит. л. англ. — ISBN 5-318-00492-X.*
2	*Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин .— Екатеринбург : Изд-во Уральского ун-та, 2003 .— 327 с. : ил .— Библиогр.:с.317-322 .— Алф.-предм. указ.: с.306-316 .— ISBN 5-86037-024-5.*
3	*Голуб, Владимир Александрович. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — ISBN 5-86026-020-2 : 37.00 .— <URL:http://www.lib.vsu.ru/elib/books/b102829.djvu>.*

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий. При проведении занятий в дистанционной форме используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ" (https://edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы в сети Интернет.

Перечень необходимого программного обеспечения : операционная система Windows , Linux, браузер Mozilla Firefox, Opera или Internet Expolorer, Denwer, PHP, MySQL, Экран, ноутбук.

18. Материально-техническое обеспечение дисциплины:

Проектор, ноутбук, экран. Для проведения лекционных и практических занятий используются аудитории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.

Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства

1.	Теоретические основы защиты ОС	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
2.	Методы защиты ОС	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
3.	Модель безопасности	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
4.	Контроль безопасности в ОС	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
5.	Безопасность серверных приложений	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
6.	Безопасность UNIX-систем	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
7.	Безопасность сетевых взаимодействий	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
8.	Безопасность приложений	ОПК-11, ОПК-13	ОПК-11.3; ОПК-13.4; ОПК-13.5	Домашнее задание, контрольная работа
Промежуточная аттестация форма контроля - экзамен				Перечень вопросов к экзамену

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: домашнее задание, контрольная работа, презентация.

Пример лабораторного задания (вариант задания)

Лабораторная работа № __
по дисциплине «Безопасность сетей ЭВМ»

Тема: «**Сканирование внутренней структуры сети**»

Задание. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров. По результатам выполнения подготовьте отчет.

Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Безопасность сетей ЭВМ»
Вариант №___

Разработайте файл конфигурации и настройте СОА Snort на обнаружение ICMP-пакетов большой длины.

20.2 Промежуточная аттестация Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Собеседование по билетам к зачету

Собеседование по экзаменационным билетам

Перечень вопросов к экзамену:

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.
2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
4. Создание защищенных сегментов сетей с использованием межсетевых экранов.
5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows XP.
6. Защита рабочих станций с использованием персональных сетевых фильтров.
7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
8. Электронные сертификаты. Понятие инфраструктуры открытых ключей.
9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.
10. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.
11. Преимущества технологии терминального доступа. Обеспечение безопасности.
12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.
13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.
14. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
15. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.
16. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки. Применение инструментальных средств аудита безопасности компьютерных систем.

17. Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности. Методика проведения инструментальных проверок.

18. Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799.

19. Назначение и основные функции программных комплексов «Гриф-специалист» и «Кондор-специалист». Построение модели защиты компьютерной системы с использованием комплексной экспертной системы «АванГард». Виды требований безопасности согласно ГОСТ Р ИСО/МЭК 15408-1-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

20. Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort».

Владение понятийным аппаратом данной области науки (теоретическими основами дисциплины), способность иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач в области информатики

Промежуточная аттестация, как правило, осуществляется в конце семестра. Результаты текущей аттестации обучающегося по решению кафедры могут быть учтены при проведении промежуточной аттестации. При несогласии студента, ему дается возможность пройти промежуточную аттестацию (без учета его текущих аттестаций) на общих основаниях.

При проведении экзамена учитываются результаты контрольных работ.

Для оценивания результатов обучения на экзамене (зачете с оценкой) используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами применять теоретические знания для решения практических задач	*Повышенный уровень*	*Отлично*
Обучающийся владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами, допускает ошибки при решении практических задачи или способен применять теоретические знания для решения практических задач в области информатики, но допускает неточности при применении понятийного аппарата данной области науки, но отвечает на дополнительные вопросы	*Базовый уровень*	*Хорошо*
Обучающийся владеет частично теоретическими основами дисциплины, фрагментарно способен иллюстрировать ответ примерами, фактами, не отвечает на	*Пороговый уровень*	*Удовлетворительно*

дополнительные вопросы *Не умеет применять теоретические знания для решения практических задач*		
Ответ на контрольно-измерительный материал не соответствует любым трем(четырем) из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	*Неудовлетворительно*