МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Бредихин А.В./

28.08.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Мониторинг защищенности сетевой инфраструктуры телекоммуникационных систем»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2025

Автор программы _____ Л.В. Паринова

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ С.С. Куликов

Воронеж 2025

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Бредихин А.В./

28.08.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Мониторинг защищенности сетевой инфраструктуры телекоммуникационных систем»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2025

Автор программы _____ Л.В. Паринова

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ С.С. Куликов

Воронеж 2025

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

является приобретение студентами знаний о методы контроля функционирования телекоммуникационных систем и сетей, принципах построения систем обнаружения компьютерных атак, методах обработки данных мониторинга безопасности телекоммуникационных систем и сетей

1.2. Задачи освоения дисциплины

сформировать у будущего специалиста в области безопасности телекоммуникационных систем знания, умения и навыки в области применения средств мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей; применения инструментальных средств проведения мониторинга защищенности сетевых ресурсов телекоммуникационных систем и сетей, а также составления отчетов по результатам проверок защищенности телекоммуникационных систем и сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Мониторинг защищенности сетевой инфраструктуры телекоммуникационных систем» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Мониторинг защищенности сетевой инфраструктуры телекоммуникационных систем» направлен на формирование следующих компетенций:

ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности;

ОПК-9.3 - Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-13	знать методы контроля функционирования телекоммуникационных систем и сетей; - принципы построения систем обнаружения компьютерных атак
	уметь применять средства мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей; применять инструментальные средства проведения мониторинга защищенности сетевых

	ресурсов телекоммуникационных систем и сетей
ОПК-9.3	знать методы обработки данных мониторинга безопасности телекоммуникационных систем и сетей;
	уметь составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей;
	владеть навыками анализа защищенности телекоммуникационных систем и сетей с использованием сканеров безопасности и средств автоматического реагирования на попытки несанкционированного доступа.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Мониторинг защищенности сетевой инфраструктуры телекоммуникационных систем» составляет 8 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	72	72
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Постановка задачи анализа защищенности компьютерной системы.	Корпоративная сеть как объект защиты Событие безопасности. Понятие уязвимости. Классификация уязвимостей. Источники информации по уязвимостям Принятые обозначения уязвимостей. National Vulnerabllity Database. Уязвимости и безопасность промышленных систем управления	6	6	12	24
2	Нормативная база и основы	Обзор международных и российских	6	6	12	24

	мониторинга безопасности телекоммуникационных систем и сетей	стандартов, регламентирующих мониторинг безопасности. Принципы непрерывности.				
3	Построение системы мониторинга	Принципы и критерии выбора параметров мониторинга. Подходы к построению мониторинга. Мониторинг с участием агентов и мониторинг при помощи конечных агентов. Иерархии систем мониторинга. Протоколы мониторинга телекоммуникационных систем и сетей. Инструменты для осуществления мониторинга.	6	6	12	24
4	Организация системы мониторинга безопасности.	Разбор существующих систем мониторинга, их сильные и слабые стороны. Документальное оформление процедуры мониторинга. Описание инструкции реагирование на инциденты (плейбук). Организация мониторинга безопасности телекоммуникационных систем и сетей.	6	6	12	24
5	Обнаружение атак в беспроводных сетях	IEEE 802.11i - нерешенные проблемы Несанкционированное использование беспроводных устройств Атаки на устройства и сервисы Атаки на механизм аутентификации 802.1x Атаки на клиентов Мониторинг безопасности Особенности обнаружения атак Атаки, характерные для беспроводных сетей	6	6	12	24
6	Выявление уязвимостей с помощью тестов	Эксплойты и их разновидности Использование техники запуска кода Простые эксплойты. Удаленный подбор пароля. Оценка стойкости паролей. Тестирование. Анализ результатов. Отказ в обслуживании	6	6	12	24
6						
		Итого	**36**	**36**	**72**	**144**

5.2 Перечень лабораторных работ

1. Работа с протоколами мониторинга. Мониторинг без участия агентов. Анализ работы протокола SNMP.

2. Процессный подход к организации мониторинга. Цикл непрерывности. Выбор критериев мониторинга для необходимы для непрерывности процессов.

3. Мониторинг при помощи агентов. Установка и настройка системы мониторинга Zabbix.

4. Работа с подсистемой WMI. Подключение хостов к системе мониторинга Zabbix. Настройка дашбордов для команды мониторинга.

5. Развертывание SIEM системы. Определение источников получения информации о событиях информационной безопасности. Разбор необходимости нормализации событий. Создание правил корреляции событий. Создание инцидентов на основе событий информационной безопасности

6. Методы хранения и анализа собранной информации. Формирование дашбордов в системах с открытым исходным кодом.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-13	знать методы контроля функционирования телекоммуникационных систем и сетей; - принципы построения систем обнаружения компьютерных атак	знание методов контроля функционирования телекоммуникационных систем и сетей; - принципы построения систем обнаружения компьютерных атак	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять средства мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей; применять инструментальные средства проведения мониторинга защищенности сетевых ресурсов телекоммуникационных систем и сетей	умение применять средства мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей; применять инструментальные средства проведения мониторинга защищенности сетевых ресурсов телекоммуникационных систем и сетей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-9.3	знать методы обработки данных мониторинга безопасности телекоммуникационных систем и сетей;	знание методов обработки данных мониторинга безопасности телекоммуникационных систем и сетей;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей;	умение составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками анализа защищенности телекоммуникационных систем и сетей с использованием сканеров без-	владение навыками анализа защищенности телекоммуникационных систем и сетей с использованием сканеров	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	опасности и средств автоматического реагирования на попытки несанкционированного доступа.	безопасности и средств автоматического реагирования на попытки несанкционированного доступа.		

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9, 10 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ОПК-13	знать методы контроля функционирования телекоммуникационных систем и сетей; - принципы построения систем обнаружения компьютерных атак	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь применять средства мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей; применять инструментальные средства проведения мониторинга защищенности сетевых ресурсов телекоммуникационных систем и сетей	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ОПК-9.3	знать методы обработки данных мониторинга безопасности телекоммуникационных систем и сетей;	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей;	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками анализа защищенности телекоммуникационных систем и сетей с использованием сканеров безопасности и средств автоматического реагирования на попытки несанкционированного доступа.	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

ИЛИ

«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-13	знать методы контроля функционирования телекоммуникационных систем и сетей; - принципы построения систем обнаружения компьютерных атак	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь применять средства мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей; применять инструментальные средства проведения мониторинга защищенности сетевых ресурсов телекоммуникационных систем и сетей	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-9.3	знать методы обработки данных мониторинга безопасности телекоммуникационных систем и сетей;	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей;	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками анализа защищенности телекоммуникационных систем и сетей с использованием сканеров безопасности и средств автоматического реагирования на попытки несанкционированного доступа.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Какие системы предназначены для обеспечения сетевого мониторинга, анализа и оповещения в случае обнаружения сетевой атаки?

IDP
AV
WCF
IPS

2. Чем системы IPS отличаются от систем IDS?

они способны обнаруживать атаки на сеть
они способны создавать оповещения в случае обнаружения сетевой атаки
они способны блокировать сетевую атаку
они способны осуществлять преобразование IP-адресов

3. Какие системы предназначены для обеспечения сетевого мониторинга, анализа, оповещения в случае обнаружения сетевой атаки, а также способны ее блокировать?

IDP
AV
WCF
IPS

4. Система IDP предназначена для обнаружения…

дефектов в программном обеспечении
спама
вторжений
нарушения целостности передаваемых данных

5. Какой протокол использует технология ZoneDefense для блокировки трафика зараженного компьютера?

IPSec
SSH
SNMP
UDP

6. Как называется протокол прикладного уровня для комплексного управления сетями?

IPSec
SSH
SNMP
UDP

7. Каковы причины проведения мониторинга Active Directory?

гарантия того, что изменения в сети и рабочей среде не будут отрицательно влиять на работу Active Directory

ежедневный профилактический мониторинг состояния службы каталога необходим для поддержания надежности Active Directory

мониторинг службы каталога является комбинацией задач, имеющих общую цель - измерение текущей характеристики некоторого ключевого ин-

дикатора по сравнению с текущим состоянием другого индикатора

мониторинг идентифицирует потенциальные проблемы прежде, чем они проявятся и закончатся длительными периодами простоя службы

мониторинг дает возможность поддерживать соглашение об уровне сервиса (Service-Level Agreement, SLA) с пользователем сети

необходимо отслеживать изменения инфраструктуры - увеличение размера базы данных Active Directory, функционирование серверов глобального каталога (GC) в интерактивном режиме, время репликации между географически разнесенными контроллерами доменов

8. С какими затратами, необходимыми для его эффективной реализации, связан мониторинг Active Directory, каковы причины их увеличения и сокращения?

для проектирования, развертывания и управления системой мониторинга нужны соответствующие людские ресурсы (человеко-часы), требующие оплаты

стоимость мониторинга быстро понижается при внедрении глобального мониторинга предприятия

часть пропускной способности сети будет использоваться для мониторинга Active Directory на всех контроллерах домена предприятия

для выполнения приложений-агентов на целевых серверах и на компьютере, являющемся центральным пультом мониторинга, используются память и ресурсы процессора

стоимость ресурсов, которые будут потрачены на систему мониторинга, не должна превышать ожидаемую от мониторинга экономию

9. Выберите верные высказывания об элементах мониторинга Active Directory

дисковые тома, которые содержат файл базы данных Active Directory и файлы журналов, должны иметь достаточно свободного пространства

если диск, на котором расположена база данных Active Directory, дефрагментирован, то необходимо его фрагментировать

служба FRS должна работать в пределах нормы, чтобы гарантировать, что общий системный том реплицируется по всему сайту

"здоровье" леса должно отслеживаться для того, чтобы проверить доверительные отношения и доступность сайта

необходимо отслеживать каждого хозяина операций, чтобы гарантировать "здоровье" сервера

следует проводить мониторинг для обеспечения доступности GC-каталога, позволяющего пользователям входить в систему и поддерживать членство универсальных групп

10. Выберите верные высказывания об элементах мониторинга Active Directory

дисковые тома, которые содержат файл базы данных Active Direc-

tory и файлы журналов, должны иметь достаточно свободного пространства

если диск, на котором расположена база данных Active Directory, дефрагментирован, то необходимо его фрагментировать

служба FRS должна работать в пределах нормы, чтобы гарантировать, что общий системный том реплицируется по всему сайту

"здоровье" леса должно отслеживаться для того, чтобы проверить доверительные отношения и доступность сайта

необходимо отслеживать каждого хозяина операций, чтобы гарантировать "здоровье" сервера

следует проводить мониторинг для обеспечения доступности GC-каталога, позволяющего пользователям входить в систему и поддерживать членство универсальных групп

7.2.2 Примерный перечень заданий для решения стандартных задач

1. В чем заключается отличие вторжений от вирусных атак?

вторжения обычно содержатся в отдельном загрузочном файле, который закачивается в систему пользователя

вторжения по характеру воздействия на атакуемую сеть могут быть как негативные, так и нейтральные

вторжения проявляются как образцы вируса, нацеленные на поиск путей преодоления механизмов обеспечения безопасности

вторжения могут осуществляться посредством сети

2. Как система IDP в NetDefend обнаруживает вторжения?

по сигнатурам вирусов и атак

по адресу отправителя трафика

на основе статистического анализа

с помощью поля ESP в составе передаваемых данных

3. Как называется определенные образцы вирусов и атак, с использованием которых IDP обнаруживает вторжения?

сертификаты

профили

сигнатуры

аутентификаторы

4. На каком принципе основано обнаружение неизвестных угроз в NetDefendOS IDP?

она не способна обнаруживать неизвестные угрозы

на основе статистического анализа

на использовании сертификатов открытых ключей

при создании вторжений за основу часто берется использовав-

шийся ранее код

5. Какая настройка в NetDefendOS IDP определяет действие, которое следует предпринять при обнаружении вторжения во входящем трафике?

Pipe Rules
Threshold Rules
IDP Rules
IP Rules

6. Какие сигнатуры обладают самой высокой точностью?

сигнатуры предотвращения вторжений
сигнатуры обнаружения вторжения
политики сигнатур

7. Какие сигнатуры обнаруживают различные типы приложений трафика и могут применяться для блокировки определенных приложений?

сигнатуры предотвращения вторжений
сигнатуры обнаружения вторжения
политики сигнатур

8. Какие сигнатуры способны обнаруживать события, которые могут оказаться вторжениями, но не обязательно ими являются?

сигнатуры предотвращения вторжений
сигнатуры обнаружения вторжения
политики сигнатур

9. Какие сигнатуры могут обнаружить попытки перехвата управления и сканеры сети с максимальной точностью?

сигнатуры предотвращения вторжений
сигнатуры обнаружения вторжения
политики сигнатур

10. Какова длительность триального периода подписки для опциональных сервисов IPS, AV и WCF?

30 дней
30 дней
90 дней
12 месяцев

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Какое действие рекомендуется выбрать для сигнатур обнаружения вторжений?

ignore
audit
protect

2. Какое действие рекомендуется выбрать для сигнатур предотвращения вторжений?

ignore
audit
protect

3. Что необходимо сделать для обновления локальной базы сигнатур в NetDefendOS?

ничего – эта опция подключена автоматически
зарегистрировать устройство на веб-ресурсе My D-Link
зарегистрировать устройство на веб-ресурсе и купить подписку на обновления
скачивать обновления вручную с официального сайта D-Link и устанавливать их на устройство

4. Как происходит обновление баз данных сигнатур в HA-кластере?

одновременно на обоих устройствах
поочередно
автоматическое обновление невозможно; базы данных на резервном межсетевом экране обновляются вручную
на резервном межсетевом экране базы данных не обновляются

5. Как называется функция в межсетевых экранах D-Link, которая автоматически изолирует инфицированные компьютеры локальной сети и предотвращает распространение ими вредоносного трафика?

Port Forwarding
Virtual Servers
ZoneDefense
Host Monitoring

6. На межсетевом экране NetDefend в настройках ZoneDefense установлен порог для TCP порт 445 «30 connections/second». Хост в сети создал 25 подключений в секунду. Что произойдет?

информация о событии будет записана в журнал
администратор получит email-уведомление о событии
передача трафика хостом будет заблокирована
ничего, так как количество соединений больше 20

7. Какая команда используется для того, чтобы на коммутаторе включить управление по SNMP ?

snmp on
create snmp
enable snmp
req snmp

8. Как называется компонент SNMP, представляющий собой программное обеспечение, установленное на рабочей станции управления, наблюдающее за сетевыми устройствами и управляющее ими?

менеджер SNMP

агент SNMP

база управляющей информации

мастер SNMP

9. Для чего нужен идентификатор объекта (Object IDentifier, OID)?

это компонент программного обеспечения, установленный на рабочей станции управления, который наблюдает за сетевыми устройствами и управляет ими

для обращения к управляемым объектам в базе управляющей информации MIB

это компонент, содержащий правила ограничения доступа, предназначенный для блокировки зараженного хоста в сети для аутентификации менеджера SNMP

10. Кто контролирует пространство имен OID?

администраторы сетевого оборудования

производители сетевого оборудования

агенство IANA

7.2.4 Примерный перечень вопросов для подготовки к зачету

Корпоративная сеть как объект защиты

Событие безопасности. Понятие уязвимости. Классификация уязвимостей. Источники информации по уязвимостям Принятые обозначения уязвимостей. National Vulnerabllity Database. Уязвимости и безопасность промышленных систем управления

Обзор международных и российских стандартов, регламентирующих мониторинг безопасности. Принципы непрерывности.

Принципы и критерии выбора параметров мониторинга. Подходы к построению мониторинга. Мониторинг с участием агентов и мониторинг при помощи конечных агентов. Иерархии систем мониторинга. Протоколы мониторинга телекоммуникационных систем и сетей. Инструменты для осуществления мониторинга.

7.2.5 Примерный перечень заданий для решения прикладных задач

Разбор существующих систем мониторинга, их сильные и слабые стороны. Документальное оформление процедуры мониторинга. Описание инструкции реагирование на инциденты (плейбук). Организация мониторинга безопасности телекоммуникационных систем и сетей.

IEEE 802.11i - нерешенные проблемы

Несанкционированное использование беспроводных устройств

Атаки на устройства и сервисы

Атаки на механизм аутентификации 802.1x
Атаки на клиентов
Мониторинг безопасности
Особенности обнаружения атак
Атаки, характерные для беспроводных сетей
Эксплойты и их разновидности
Использование техники запуска кода
Простые эксплойты. Удаленный подбор пароля. Оценка стойкости паролей. Тестирование. Анализ результатов. Отказ в обслуживании

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Постановка задачи анализа защищенности компьютерной системы.	ОПК-13, ОПК-9.3	Тест, защита лабораторных работ
2	Нормативная база и основы мониторинга безопасности телекоммуникационных систем и сетей	ОПК-13, ОПК-9.3	Тест, защита лабораторных работ
3	Построение системы мониторинга	ОПК-13, ОПК-9.3	Тест, защита лабораторных работ.
4	Организация системы мониторинга безопасности.	ОПК-13, ОПК-9.3	Тест, защита лабораторных работ.
5	Обнаружение атак в беспроводных сетях	ОПК-13, ОПК-9.3	Тест, защита лабораторных работ.
6	Выявление уязвимостей с помощью тестов	ОПК-13, ОПК-9.3	Тест, защита лабораторных работ.

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется про-

верка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2016. — 396 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110273

Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства : учебное пособие / В. В. Бондарев. — Москва : МГТУ им. Н.Э. Баумана, 2017. — 228 с. — ISBN 978-5-7038-4757-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103518

Дополнительная литература

Агеев, Е. Ю. Основы компьютерных сетевых технологий / Е. Ю. Агеев. — Москва : ТУСУР, 2011. — 83 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/11484

Давидюк, Н. В. Мониторинг безопасности информационных систем : учебное пособие / Н. В. Давидюк, И. М. Космачева. — Санкт-Петербург : Интермедия, 2020. — 116 с. — ISBN 978-5-4383-0204-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161352

Тимофеев, А. В. Проектирование и разработка информационных систем : учебное пособие для СПО / А. В. Тимофеев, З. Ф. Камальдинова, Н. С. Агафонова. — Саратов : Профобразование, 2022. — 91 с. — ISBN 978-5-4488-1416-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/116285.html

Сети и телекоммуникации : учебное пособие для бакалавров / составители И. В. Винокуров. — Москва : Ай Пи Ар Медиа, 2022. — 105 с. — ISBN 978-5-4497-1418-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/115699.html

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://www.eios.vorstu.ru (электронная информационно-обучающая система ВГТУ)
http://e.lanbook.com/ (ЭБС Лань)
http://znanium.com/ (ЭБС Знаниум)
http://IPRbookshop.ru/ (ЭБС IPRbooks (Айбукс))

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Мониторинг защищенности сетевой инфраструктуры телекоммуникационных систем» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная	Самостоятельная работа студентов способствует глубокому

работа	усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4