МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.02
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность компьютерных сетей
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость:6 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	**7**	**Итого**
Форма контроля / **Вид занятий**	**Экзамен**	
Лекции	32	32
Лабораторные	-	-
Практические	48	48
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,35	0,35
Контактная работа	80,35	80,35
Самостоятельная работа	100	100
Контроль	35,65	35,65
Итого	**216**	**216**

Рабочую программу составил(и):

Власов Игорь Анатольевич

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☒ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Дисциплина «Безопасность компьютерных сетей» обеспечивает приобретение знаний и умений в обеспечении безопасности вычислительных сетей, содействует формированию критичного и системного мышления; направлена на изучение современных стандартов обеспечения информационной безопасности, программно-аппаратных методов и средств защиты информации, критериев оценки обеспечения безопасности информационно-технологических систем и сетей.

Целью освоения учебной дисциплины является изучение программно-аппаратных методов и средств защиты информации, обеспечения безопасности информационно-технологических систем и сетей.

В результате изучения дисциплины студенты должны знать:

• технологии обнаружения компьютерных атак и их возможности;

• основные уязвимости и типовые атаки на современные компьютерные системы;

• возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;

• методы защиты компьютерных сетей;

• классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;

• основные принципы администрирования защищенных компьютерных систем;

• особенности реализации методов защиты информации современными программно-аппаратными средствам.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Основы управления информационной безопасностью;
- Программно-аппаратные средства защиты информации;
- Аудит защищенности информационных систем.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:

• Мониторинг событий информационной безопасности;

• Техническая защита информации.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-3 Способен оценивать угрозы безопасности информации операционных систем и сетей	ПК-3.1 Использует принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	Знать: - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		Уметь: - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Владеть: - навыками выявления и уничтожения компьютерных вирусов
	ПК-3.2 Применяет меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Знать: - средства защиты информации, функционал, настройки
		Уметь: - применять и проектировать СЗИ
		Владеть: - -навыками разработки, документирования вычислительных сетей с учетом требований по обеспечению информационной безопасности
	ПК-3.3 Демонстрирует владение методами количественного анализа процессов обработки, поиска и передачи информации и навыками разработки, документирования вычислительных сетей с учетом требований по обеспечению информационной безопасности	Знать: - математические методы обработки экспериментальных данных
		Уметь: - использовать математические методы и модели для решения прикладных задач;
		Владеть: -методами количественного анализа процессов обработки, поиска и передачи информации

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Эволюция компьютерных сетей 1.Вычислительная и телекоммуникационная технологии. 2.Системы пакетной обработки. 3.Многотерминальные системы — прообраз сети. Первые компьютерные сети. Первые глобальные сети. Первые локальные сети. Конвергенция сетей. 4. Общие принципы построения сетей	7	2		-	
Модуль 1	Пр	Тема 1 Эволюция компьютерных сетей Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.	7	2			Отчет по практическому занятию №1
Модуль 1	Ср	Тема 1 Эволюция компьютерных сетей	7	5			
Модуль 1	Лек	Тема 2 Архитектура и стандартизация сетей 2 Протокол и стек протоколов. 3. Модель OSI. Стандартизация сетей. 4.Понятие открытой системы. 5.Стандартизация Интернета. 6.Стандартные стеки коммуникационных протоколов 7.Классификация компьютерных сетей 8.Службы каталогов. 9.Общие сведения о службах каталогов. 10.Структура каталога LDAP. 11.Система единого входа в сеть на основе протокола Kerberos. 12.Создание единого пространства безопасности на базе Active Directory	7	2		-	
Модуль 1	Пр	Тема 2 Архитектура и стандартизация сетей Применение специализированных средств организации VPN на примере	7	2			Отчет по практическому занятию №2

		VipNet					
Модуль 1	Ср	Тема 2 Архитектура и стандартизация сетей	7	5			
Модуль 1	Лек	Тема 3 Технологии локальных сетей и Internet 1. Технологии локальных сетей на разделяемой среде. 2.Общая характеристика протоколов локальных сетей на разделяемой среде. 3.Стандартная топология и разделяемая среда. Стандартизация протоколов локальных сетей. Ethernet со скоростью 10 Мбит/с на разделяемой среде. 4.MAC адреса. Форматы кадров технологии Ethernet. 5.Доступ к среде и передача данных. Возникновение коллизии. 6.Спецификации физической среды. 7.Максимальная производительность сети Ethernet. 8.Технологии Token Ring и FDDI. 9.Беспроводные локальные сети IEEE 802.11. Проблемы и области применения беспроводных локальных сетей 10. Коммутируемые сети Ethernet. 11.Дуплексный режим работы. 12.Характеристики производительности коммутаторов. 13.Скоростные версии Ethernet. Fast Ethernet. Gigabit Ethernet. 10G Ethernet. 14.Архитектура коммутаторов	7	2			
Модуль 1	Пр	Тема 3 Технологии локальных сетей и Internet Настройка коммутатора	7	2			Отчет по практическому занятию №3
Модуль 1	Ср	Тема 3 Технологии локальных сетей и Internet	7	5			
Модуль 1	Лек	Тема 4 Сетевое управление в IP-сетях 1.Базовые протоколы TCP/IP. 2.Порты и сокеты. 3.Протокол UDP и UDP-дейтаграммы. 4.Протокол TCP и TCP-сегменты 5.Трансляция сетевых адресов 6.Адресация в стеке протоколов	7	2		-	

		TCP/IP 7.Архитектуры систем управления сетями. 8.Протокол SNMP. 9.Протокол DHCP.					
Модуль 1	Пр	Тема 4 Сетевое управление в IP-сетях Создание коммутируемой сети. Управление коммутатором через WEB-интерфейс. Изучение таблиц коммутации. Адресация канального уровня. MAC-адреса. Построение одноранговой сети	7	4			Отчет по практическому занятию №4,5
Модуль 1	Ср	Тема 4 Сетевое управление в IP-сетях	7	5			
Модуль 1	Лек	Тема 5 Проблемы функционирования межсетевых экранов. 1.Общая характеристика МСЭ и их функциональные свойства. 2.Проблемы разработки и внедрения МСЭ. 3.Роль МСЭ при реализации атак 4. Фильтрация пакетов. Критерии и правила фильтрации 5.Задачи ИБ при выборе и эксплуатации МСЭ 6. Шлюзы прикладного уровня 7. Контроль HTTP-трафика и электронной почты. 8. Написание правил фильтрации, возможности по анализу содержимого.	7	2		-	
Модуль 1	Пр	Тема 5 Проблемы функционирования межсетевых экранов. Адресация сетевого уровня. IP-адресация. Формирование подсетей Традиционная технология NAT. Базовая трансляция сетевых адресов. Трансляция сетевых адресов и портов	7	4			Отчет по практическому занятию №6,7
Модуль 1	Ср	Тема 5 Проблемы функционирования межсетевых экранов.	7	5			
Модуль 1	Лек	Тема 6 Обнаружение компьютерных атак 1.Понятие и классификация атак на компьютерные сети. 2. Основные типы сетевых атак. 3.Средства реализации атак.	7	2			

		4.Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. 5.Атаки на сетевые службы. 6.Атаки с использованием промежуточных узлов и территорий. 7.Каналы утечки информации из компьютерных систем 8.Технологии обнаружения компьютерных атак и их возможности. 9.Прямые и косвенные признаки атак. 10.Методы обнаружения атак. 11.Сигнатурный анализ и обнаружение аномалий. 12.Классификация систем обнаружения атак (СОА). 13.Сетевые и узловые СОА. 14.Требования, предъявляемые к СОА. 15.Стандартизация в области обнаружения атак. 16. 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.					
Модуль 1	Пр	Тема 6 Обнаружение компьютерных атак Моделирование компьютерной атаки	7	4			Отчет по практическому занятию №8
Модуль 1	Ср	Тема 6 Обнаружение компьютерных атак	7	5			

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 2	Лек	Тема 7 Информационное противоборство 1.Понятие “информационная война”. 2. Понятие “информационное оружие”. 3.Формы информационного противоборства 4. Компьютерный шпионаж, как следствие и способ информационного противоборства. 5.Модель атак типа “маскарад”. 6.Обнаружение атак типа “маскарад”	7	2		-	
Модуль 2	Пр	Тема 7 Информационное противоборство Обнаружение атаки типа Маскарад. Защита	7	2			Отчет по практическому занятию №9
Модуль 2	Ср	Тема 7 Информационное противоборство	7	6			
Модуль 2	Лек	Тема 8 Основные технические модели обеспечения информационной безопасности в ИТС 1 Цель и задачи обеспечения ИБ лвс. 2.Модель служб обеспечения ИБ лвс. 3.Решение задач обеспечения ИБ — распределённые системы 4.Защита топологии сети 5.Абонентское шифрование. 6.Виртуальные частные сети.	7	2		-	
Модуль 2	Пр	Тема 8 Основные технические модели обеспечения информационной безопасности в ИТС	7	2			Отчет по практическому занятию №10

		Разработка модели служб обеспечения ИБ лвс					
Модуль 2	Ср	Тема 8 Основные технические модели обеспечения информационной безопасности в ИТС	7				
Модуль 2	Лек	Тема 9 Принципы архитектуры безопасности в Internet-сети 1. Принципы архитектуры безопасности ISO. 2.Принципы архитектуры безопасности DOD. 3.Принципы архитектуры безопасности Internet (IETF). 4.Рекомендации IETF по использованию способов и средств обеспечения ИБ в Internet-сети (содержание архитектуры безопасности Internet)	7	2		-	
Модуль 2	Пр	Тема 9 Принципы архитектуры безопасности в Internet-сети Защита сетевого управления и сетевой аутентификации	7	4			Отчет по практическому занятию №11
Модуль 2	Ср	Тема 9 Принципы архитектуры безопасности в Internet-сети	7	6			
Модуль 2	Лек	Тема 10 Основные принципы и содержание топологических (заградительных) систем обеспечения ИБ 1.Задачи, решаемые NAT-модулями и СЭ. 2.NAT-модули и как системы распознавания образов. 3.Наличие принципиальной возможности NAT-модулей для распознования атак 4.Основные принципы и содержание NAT	7	2		-	
Модуль 2	Пр	Тема 10 Основные принципы и содержание топологических (заградительных) систем обеспечения ИБ Использование Nat модулей	7	2			Отчет по практическому занятию №12
Модуль 2	Ср	Тема 10 Основные принципы и содержание топологических	7				

		(заградительных) систем обеспечения ИБ					
Модуль 2	Лек	Тема 11 Защита сетевого трафика и компонентов сети 1.Защита компонентов сети от НСД. 2. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. 3.Электронная цифровая подпись и пакетное шифрование. 4.Криптографические сетевые протоколы. Управление ключами	7	2			
Модуль 2	Пр	Тема 11 Защита сетевого трафика и компонентов сети Разработка методов защиты ЛВС от НСД		4			Отчет по практическому занятию №13
Модуль 2	Ср	Тема 11 Защита сетевого трафика и компонентов сети		6			
Модуль 2	Лек	Тема 12 Средства повышения надежности функционирования сетей 1.Защита от сбоев электропитания, аппаратного и программного обеспечения. 2.Контроль и распределение нагрузки на вычислительную сеть 3. Физическая защита ЛВС. Содержание мероприятий 4.Разработка клиент-серверных приложений с элементами защиты. 5.Разработка приложения для аутентификации пользователей на основе сертификатов	7	2			
Модуль 2	Пр	Тема 12 Средства повышения надежности функционирования сетей Разработка клиент- серверных приложений с элементами	7	4			Отчет по практическому занятию №14

		защиты.					
Модуль 2	Ср	Тема 12 Средства повышения надежности функционирования сетей	7	6			
Модуль 2	Лек	Тема 13 Сети Wi-Fi 1.Построение локальной сети небольшого офиса на основе точек доступа и беспроводных адаптеров. 2. Настройка точки доступа и беспроводных адаптеров. 3.WEP-шифрование и его недостатки. 4. WAP-шифрование. Слабости алгоритмов шифрования на основе WAP. 5.Методы скрытия идентификатора беспроводной точки доступа.	7	2			
Модуль 2	Пр	Тема 13 Сети Wi-Fi Защита точек доступа, настройки, конфигурирование, методы взлома	7	4			Отчет по практическому занятию №15
Модуль 2	Ср	Тема 13 Сети Wi-Fi	7	6			
Модуль 2	Лек	Тема 14**.** Средства защиты протокола IP. Защита IP-пакетов с помощью IPSec. Защита WEB. Протоколы SSL/TLS. Протокол защищенных электронных транзакций SET 1.Средства защиты протокола IP. 2.IP-пакетов с помощью IPSec. 3.Основные задачи, решаемые IPSec. 4.Основные сервисы IPSec. 5.Транспортный и туннельный режимы IPSec. 6.Защищенные связи и их параметры. 7.Формат пакета ESP. 8.Управление ключами в IPSec. 9.Протокол Oakley.	7	2			

		10.Особенности применения протокола IPsec. 11.Использование протокола в маршрутизаторах и файерволах. 12. Организация демилиторизованных зон на основе протокола IPsec.					
Модуль 2	Пр	Тема 14. Средства защиты протокола IP. Защита IP-пакетов с помощью IPSec. Защита WEB. Протоколы SSL/TLS. Протокол защищенных электронных транзакций SET Защита сетевого трафика с использованием протокола IPSec	7	4			Отчет по практическому занятию №16
Модуль 2	Ср	Тема 14. Средства защиты протокола IP. Защита IP-пакетов с помощью IPSec. Защита WEB. Протоколы SSL/TLS. Протокол защищенных электронных транзакций SET	7	6			
Модуль 2	Лек	Тема 15 Организация виртуальных частных сетей 1. Задачи, решаемые VPN 2. Туннелирование в VPN 3. Защита данных на канальном уровне 4. Защита данных на сетевом уровне 5. Защита на транспортном уровне	7	2			
Модуль 2	Пр	Тема 15 Организация виртуальных частных сетей Организация VPN средствами протокола SSL в Windows Server	7	2			Отчет по практическому занятию №17

Модуль 2	Ср	Тема 15 Организация виртуальных частных сетей	7	6			
Модуль 2	Лек	Тема 16 Технологии терминального доступа 1 Общие сведения о технологии терминального доступа 2 Настройки сервера MSTS 3 Настройки протокола RDP	7	2			
Модуль 2	Пр	Тема 16 Технологии терминального доступа Настройка виртуальной сети	7	2			Отчет по практическому занятию №18
Модуль 2	Ср	Тема 16 Технологии терминального доступа	7	6			
	К	Подготовка к экзамену	7	35,65		-	
	ПА	Сдача Экзамена	7	0,35		-	Вопросы к экзамену
			Итого:	**216**			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. **CD-технология** – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
7	ПК-3	Протоколы практических заданий №1-18
		Вопросы к экзамену №№ 1-105
		Банк тестовых заданий №1-350

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.
2	Применение специализированных средств организации VPN на примере VipNet
3	Настройка коммутатора
4	Создание коммутируемой сети. Управление коммутатором через WEB-интерфейс. Изучение таблиц коммутации.
5	Адресация канального уровня. MAC-адреса. Построение одноранговой сети
6	Адресация сетевого уровня. IP-адресация. Формирование подсетей
7	Традиционная технология NAT. Базовая трансляция сетевых адресов. Трансляция сетевых адресов и портов
8	Моделирование компьютерной атаки
9	Обнаружение атаки типа Маскарад. Защита
10	Разработка модели служб обеспечения ИБ лвс.
11	Защита сетевого управления и сетевой аутентификации
12	Использование Nat модулей
13	Разработка методов защиты ЛВС от НСД
14	Разработка клиент- серверных приложений с элементами защиты.
15	Защита точек доступа, настройки, конфигурирование, методы взлома
16	Защита сетевого трафика с использованием протокола IPSec
17	Организация VPN средствами протокола SSL в Windows Server
18	Настройка виртуальной сети

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты проектируют защищенные сегменты сети, настраивают коммутатор, изучают технологии адресации, моделируют компьютерные атаки, проектируют защиту точек доступа, сетевого трафика, организуют VPN и контроль удаленного доступа

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 7

№ п/п	Вопросы к экзамену
1.	Общие принципы построения сетей
2.	Архитектуры информационных систем. Основные характеристики, достоинства и недостатки клиент-серверной архитектуры
3.	Одноранговые сетевые ОС и ОС с выделенными серверами
4.	Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей
5.	Контроль и распределение нагрузки на вычислительную сеть
6.	Стандарты безопасности вычислительных сетей и их компонентов
7.	Правовые основы защиты информации в сетях
8.	Роль службы ИБ в организации сетей и их защиты
9.	Влияние человеческого фактора на сетевую безопасность
10.	Цели создания системы защиты
11.	Идентификация и аутентификация абонентов сети
12.	Электронная цифровая подпись и пакетное шифрование
13.	Основные схемы применения МЭ
14.	Маршрутизаторы, межсетевые экраны
15.	Коммутаторы, характеристики, производительность, уязвимости, методы защиты
16.	Примеры типовых атак и рекомендаций по построению систем защиты
17.	Методы разделения ресурсов и технологии разграничения доступа
18.	Управление ключами
19.	Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных

20.	Классификация средств и информационных ресурсов в соответствии со стандартом ISO-17799
21.	Виды требований безопасности согласно ГОСТ Р ИСО/МЭК 15408-1-2002. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
22.	Виды протоколов и их характеристики
23.	Порты, сокеты, проблемы безопасности связанные с портами
24.	Организация вычислительных сетей на базе операционных систем Unix: основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение
25.	Преимущества и недостатки основных топологий сети
26.	Методы контроля сетевого трафика
27.	Механизмы типовых атак, основанных на уязвимостях сетевых протоколов
28.	Каналы утечки информации из компьютерных систем
29.	Методы обнаружения атак
30.	Сигнатурный анализ и обнаружение аномалий
31.	Протокол TCP и TCP-сегменты
32.	Трансляция сетевых адресов
33.	Архитектуры систем управления сетями
34.	Адресация в стеке протоколов TCP/IP
35.	Таблицы коммутации
36.	Фильтрация пакетов. Критерии и правила фильтрации
37.	Задачи ИБ при выборе и эксплуатации МСЭ
38.	Атаки на сетевые службы
39.	Атаки с использованием промежуточных узлов и территорий
40.	Классификация систем обнаружения атак (СОА)
41.	Сетевые и узловые СОА
42.	Архитектура СОА.
43.	Требования, предъявляемые к СОА
44.	Стандартизация в области обнаружения атак
45.	ПО для СОА
46.	Атаки на протоколы и службы Интернет. Методы и средства
47.	Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
48.	Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows
49.	Защита рабочих станций с использованием персональных сетевых фильтров.
50.	Критерии оценки безопасности сетевых ОС
51.	Примеры типовых атак и рекомендации по построению систем защиты
52.	Основы классификации сетевых угроз и атак
53.	Защита компонентов сети от НСД
54.	Защита от сбоев электропитания, аппаратного и программного обеспечения
55.	Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети
56.	Разработайте и реализуйте политику для пакетного фильтра, разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров
57.	Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec
58.	Разработайте и реализуйте политику для пакетного фильтра, запрещающего

	сканирование внутренней структуры сети. Реализуйте политику средствами протокола IPSec
59.	Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
60.	Настройте входящее подключение VPN с использованием протокола PPTP
61.	Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.
62.	Перехватите в локальной сети пакеты, убедитесь в шифровании трафика
63.	Преимущества технологии терминального доступа. Обеспечение безопасности
64.	Установить службу терминального доступа. Выполнить настройки протокола RDP, запрещающие использование ресурсов рабочей станции, включая буфер обмена, принтеры и накопители
65.	Установить службу терминального доступа. Выполнить настройки службы MSTS, разрешающие доступ к ресурсам терминального сервера только для учетных записей, зарегистрированных в созданной по умолчанию группе «Remote Desktop Users»
66.	Распределённые атаки на отказ от обслуживания, обнаружение, противодействие
67.	Способы взлома парольной защиты компонентов сети
68.	Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
69.	С помощью утилиты nmap проведите сканирование портов сетевого узла. Сформируйте списки открытых TCP- и UDP-портов, идентифицируйте версии ОС и запущенных сервисов. По результатам сделайте вывод о возможности обнаружения открытых портов и идентификации типа и версии ОС, а также сетевых сервисов
70.	Выявите сетевые узлы в локальном сегменте
71.	Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP
72.	Тестирование состояния защищенности компьютерных систем от несанкционированного доступа с использованием сканеров безопасности. Методика проведения инструментальных проверок
73.	Назначение и основные функции программных комплексов «Гриф-специалист» и «Кондор-специалист»
74.	Построение модели защиты компьютерной системы с использованием комплексной экспертной системы «Авангард»
75.	Назначение систем обнаружения атак. Классификация систем обнаружения атак. Использование системы обнаружения атак «Snort».
76.	Разработайте файл конфигурации и настройте СОА Snort на обнаружение ICMP пакетов большой длины
77.	Оценка показателей объектов зашиты
78.	Методика подготовки экспертного заключения по защите сети
79.	Механизмы типовых атак, основанных на уязвимостях сетевых протоколов
80.	Методы контроля сетевого трафика
81.	WireShark, описание, применение, принцип работы
82.	Анализ TCP-соединений
83.	Использование Wireshark для изучения сетевых протоколов
84.	Технологии виртуальных локальных сетей VLAN
85.	Преобразование сетевых адресов NAT
86.	Списки управления доступом ACL
87.	Конфигурирование и проверка IPsec VPN
88.	Обнаружение доступных сетевых служб
89.	Политика межсетевого экранирования

90.	Распределенные системы обнаружения атак
91.	Выявление факта сканирования портов
92.	Туннелирование в VPN
93.	Уровни защищенных каналов
94.	Защита данных на канальном уровне
95.	Организация VPN средствами протокола PPTP
96.	Анализ защищенности передаваемой информации по тунельному соединению
97.	Организация VPN средствами СЗИ VipNet
98.	Шифрование трафика с использованием протокола IPSec
99.	Методика Проверки защиты трафика
100.	Защита на транспортном уровне
101.	Методика настройки безопасности Windows серверов
102.	Организация демилиторизованных зон на основе протокола IPsec
103.	Анализ защищенности web-серверов
104.	Методика создания карт сети
105.	Сканеры безопасности сети, типы, применение

7.3.2. Критерии и нормы оценки

Семестр	**Форма проведения промежуточной аттестации**	**Критерии и нормы оценки**	
7	Экзамен (по накопительному рейтингу)	«отлично»	80-100 баллов
		«хорошо»	60-79 баллов
		«удовлетворительно»	40-59 баллов
		«неудовлетворительно»	0-39 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Нестеров С.А.	Основы информационной безопасности	учебное пособие	2022г.	https://e.lanbook.com/books/1545
2	Прохорова О.В.	Информационная безопасность и защита информации	учебное пособие	2022г.	https://e.lanbook.com/book/217445?category=1545
3	Никифоров С.Н.	Методы защиты информации. Защищенные сети	учебное пособие	2021 г	https://e.lanbook.com/book/171868?category=1545

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	А. И. Бирюков	Информационная безопасность: защита и нападение 2-е изд.)	учебно-методическое пособие	2019г.	
2	А.В. Моргунов	Информационная безопасность:	учебно-	2019г.	https://

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
			методическое пособие		e.lanbook.com/book/152227?category=1545

8.3. Перечень профессиональных баз данных и информационных справочных систем

1.Информационная безопасность. Защита информации
Адрес ресурса: http://all-ib.ru/
2. CNEWS безопасность
Адрес ресурса: https://safe.cnews.ru/
3. ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU
Адрес ресурса: http://www.iso27000.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф