

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: 2026

Общая трудоемкость: 63Е

Распределение часов дисциплины по семестрам

Семестр	7	Итого
Форма контроля	Экзамен	
Вид занятий		
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):

Доцент ИИиЭБ, к.э.н., доцент, Фрезе Т.Ю.

(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 31.08.2030

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 1 от 01.09.2025).

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 средствами.

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	Знать: - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
		Уметь:

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
	системы и системы передачи информации	- 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 Основы архитектуры, технологий и управления компьютерными сетями	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	-	-	Банк тестовых заданий
	Пр	Практическая работа 1. Анализ эволюции сетевых архитектур	7	2	-	-	Отчет по практической работе
	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	7	2	-	--	Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		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					
	Пр	Практическая работа 2 Исследование стека протоколов OSI и TCP/IP	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 3 Настройка и тестирование службы каталогов LDAP	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 4 Реализация единого входа на основе Kerberos	7	2	-	-	Отчет по практической работе
	Лек	Тема 3. Технологии локальных сетей и Internet 1. Технологии локальных сетей на разделяемой среде.	7	2			Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		<p>2.Общая характеристика протоколов локальных сетей на разделяемой среде.</p> <p>3.Стандартная топология и разделяемая среда. Стандартизация протоколов локальных сетей. Ethernet со скоростью 10 Мбит/с на разделяемой среде.</p> <p>4.MAC адреса. Форматы кадров технологии Ethernet.</p> <p>5.Доступ к среде и передача данных. Возникновение коллизии. 6.Спецификации физической среды.</p> <p>7.Максимальная производительность сети Ethernet.</p> <p>8.Технологии Token Ring и FDDI. 9.Беспроводные локальные сети IEEE 802.11. Проблемы и области применения беспроводных локальных сетей</p> <p>10. Коммутируемые сети Ethernet. 11.Дуплексный режим работы.</p> <p>12.Характеристики производительности</p>					

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		коммутаторов. 13.Скоростные версии Ethernet. Fast Ethernet. Gigabit Ethernet. 10G Ethernet. 14.Архитектура коммутаторов					
	Пр	Практическая работа 5 Анализ кадров Ethernet и MAC-адресов	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 6 Исследование работы коммутатора и дуплексного режима	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 7 Настройка и анализ производительности VLAN	7	2	-	-	Отчет по практической работе
	Лек	Тема 4. Сетевое управление в IP-сетях 1.Базовые протоколы TCP/IP. 2.Порты и сокетты. 3.Протокол UDP и UDP-дейтаграммы. 4.Протокол TCP и TCP-сегменты 5.Трансляция сетевых адресов 6.Адресация в стеке протоколов TCP/IP	7	2		-	Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		7.Архитектуры систем управления сетями. 8.Протокол SNMP. 9.Протокол DHCP.					
	Пр	Практическая работа 8 Изучение протоколов TCP и UDP	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 9 Настройка DHCP-сервера и анализ опций	7	2	-	-	Отчет по практической работе
	Пр	Практическая работ 10 Настройка SNMP для мониторинга сети	7	2	-	-	Отчет по практической работе
	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	7	2		-	Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		6. Шлюзы прикладного уровня 7. Контроль HTTP-трафика и электронной почты. 8. Написание правил фильтрации, возможности по анализу содержимого.					
	Пр	Практическая работа 11 Разработка правил фильтрации для межсетевого экрана	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 12. Анализ HTTP-трафика и настройка шлюза прикладного уровня	7	2	-	-	Отчет по практической работе
	Лек	Тема 6. Обнаружение компьютерных атак 1.Понятие и классификация атак на компьютерные сети. 2. Основные типы сетевых атак. 3.Средства реализации атак. 4.Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. 5.Атаки на сетевые службы. 6.Атаки с использованием промежуточных узлов и территорий.	7	2			Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		<p>7.Каналы утечки информации из компьютерных систем</p> <p>8.Технологии обнаружения компьютерных атак и их возможности. 9.Прямые и косвенные признаки атак.</p> <p>10.Методы обнаружения атак. 11.Сигнатурный анализ и обнаружение аномалий.</p> <p>12.Классификация систем обнаружения атак (СОА).</p> <p>13.Сетевые и узловые СОА.</p> <p>14.Требования, предъявляемые к СОА.</p> <p>15.Стандартизация в области обнаружения атак.</p> <p>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.</p>					

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
	Пр	Практическая работа 13 Обнаружение атаки «ARP-spoofing» средствами COA	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 14 Сигнатурный анализ и обнаружение аномалий	7	2	-	-	Отчет по практической работе
	Ср	Самостоятельное изучение материала, чтение электронного учебника	7	50	-	-	Банк тестовых заданий
Модуль 2 Информационное противоборство, архитектура безопасности и средства защиты сетей	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		-	Банк тестовых заданий
	Пр	Практическая работа 15. Моделирование атаки «маскарад» и ее обнаружение	7	2	-	-	Отчет по практической работе

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
	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	-	-	Отчет по практической работе
	Пр	Практическая работа 16. Построение виртуальной частной сети (VPN) на основе OpenVPN	7	2	-	-	Отчет по практической работе
	Лек	Тема 9. Принципы архитектуры безопасности в Internet-сети 1. Принципы архитектуры безопасности ISO. 2.Принципы архитектуры безопасности DOD.	7	2		-	Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		3.Принципы архитектуры безопасности Internet (IETF). 4.Рекомендации IETF по использованию способов и средств обеспечения ИБ в Internet-сети (содержание архитектуры безопасности Internet)					
	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 распознавания атак 4.Основные принципы и содержание NAT	7	2		-	Банк тестовых заданий
	Пр	Практическая работа 17. Настройка NAT и анализ его влияния на безопасность	7	2	-	-	Отчет по практической работе
	Лек	Тема 11. Защита сетевого трафика и компонентов сети	7	2			Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		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					
	Пр	Практическая работа 18. Реализация аутентификации с использованием сертификатов	7	2	-	-	Отчет по практической работе
	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	7	2			Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		3. Физическая защита ЛВС. Содержание мероприятий 4.Разработка клиент-серверных приложений с элементами защиты. 5.Разработка приложения для аутентификации пользователей на основе сертификатов					
	Пр	Практическая работа 19. Разработка клиент-серверного приложения с аутентификацией и шифрованием	7	2	-	-	Отчет по практической работе
	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	7	2			Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		беспроводной точки доступа.					
	Пр	Практическая работа 20. Настройка защищенного Wi-Fi (WPA2-Enterprise)	7	2	-	-	Отчет по практической работе
	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. 10.Особенности применения протокола IPsec. 11.Использование протокола в	7	2			Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		маршрутизаторах и файерволах. 12. Организация демилитаризованных зон на основе протокола IPsec.					
	Пр	Практическая работа 21 Исследование SSL/TLS: захват и дешифрование защищенного трафика	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 22 Настройка IPsec в транспортном и туннельном режимах	7	2	-	-	Отчет по практической работе
	Пр	Практическая работа 23 Организация демилитаризованной зоны (DMZ) на базе IPsec	7	2	-	-	Отчет по практической работе
	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			Банк тестовых заданий
	Лек	Тема 16. Технологии терминального доступа	7	2			Банк тестовых заданий

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
		1 Общие сведения о технологии терминального доступа 2 Настройки сервера MSTS 3 Настройки протокола RDP					
	Пр	Практическая работа 24 Исследование протокола RDP и его защита	7	2	-	-	Отчет по практической работе
	Ср	Самостоятельное изучение материала, чтение электронного учебника	7	50	-	-	Банк тестовых заданий
	К	Контроль	7	35,65	-	-	Банк тестовых заданий / Вопросы к экзамену
	ПА	Промежуточная аттестация	7	0,35	-	-	Банк тестовых заданий / 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	Отчет по практическим работам №№1-24
		Вопросы к экзамену №№ 1-105
		Б а

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

7.2.1. Практическая работа

(наименование оценочного средства)

Практическая работа 1. Анализ эволюции сетевых архитектур
 Практическая работа 2 Исследование стека протоколов OSI и TCP/IP
 Практическая работа 3 Настройка и тестирование службы каталогов LDAP
 Практическая работа 4 Реализация единого входа на основе Kerberos
 Практическая работа 5 Анализ кадров Ethernet и MAC-адресов
 Практическая работа 6 Исследование работы коммутатора и дуплексного режима
 Практическая работа 7 Настройка и анализ производительности VLAN
 Практическая работа 8 Изучение протоколов TCP и UDP
 Практическая работа 9 Настройка DHCP-сервера и анализ опций
 Практическая работ 10 Настройка SNMP для мониторинга сети
 Практическая работа 11 Разработка правил фильтрации для межсетевого экрана
 Практическая работа 12. Анализ HTTP-трафика и настройка шлюза прикладного уровня
 Практическая работа 13 Обнаружение атаки «ARP-spoofing» средствами COA
 Практическая работа 14 Сигнатурный анализ и обнаружение аномалий
 Практическая работа 15. Моделирование атаки «маскарад» и ее обнаружение
 Практическая работа 16. Построение виртуальной частной сети (VPN) на основе OpenVPN
 Практическая работа 17. Настройка NAT и анализ его влияния на безопасность
 Практическая работа 18. Реализация аутентификации с использованием сертификатов
 Практическая работа 19. Разработка клиент-серверного приложения с аутентификацией и шифрованием
 Практическая работа 20. Настройка защищенного Wi-Fi (WPA2-Enterprise)
 Практическая работа 21 Исследование SSL/TLS: захват и дешифрование защищенного трафика
 Практическая работа 22 Настройка IPsec в транспортном и туннельном режимах
 Практическая работа 23 Организация демилитаризованной зоны (DMZ) на базе IPsec
 Практическая работа 24 Исследование протокола RDP и его защита

Типовой(ые) пример(ы) задания(ий)

Таблица 1 - Поколения сетей

параметр/система пакетной обработки					
многотерминальная					
первые ГВС					

первые ЛВС					
конвергентные сети					

Темы письменных работ

№	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

Краткое описание и регламент выполнения

1. Заполнить таблицу «Поколения сетей» (5 строк: параметр/система пакетной обработки, многотерминальная, первые ГВС, первые ЛВС, конвергентные сети).
2. Построить временную диаграмму конвергенции (ось времени — годы, области — технологии).
3. Сформулировать 3 ключевых вывода об эволюции..

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.

7.2.4 Типовой пример тестового задания

Администратор сети настраивает защищённый канал между двумя офисами через интернет. Требуется обеспечить конфиденциальность, целостность и аутентификацию всех IP-пакетов, включая скрытие оригинальных IP-адресов отправителя и получателя. Дополнительное условие — трафик внутри каждого офиса не должен шифроваться (только при передаче по открытой сети).

Какой стек технологий и режим работы наиболее полно соответствует этим требованиям?

Варианты ответов:

1. IPsec в транспортном режиме с протоколом AH — позволяет скрыть IP-адреса, но AH не обеспечивает конфиденциальность (шифрование данных).
2. SSL/TLS поверх TCP — обеспечивает шифрование и аутентификацию, но работает только для конкретного приложения (порта) и не скрывает исходные IP-адреса пакетов на сетевом уровне.
3. IPsec в туннельном режиме с протоколом ESP — инкапсулирует весь исходный IP-пакет в новый, шифрует его (конфиденциальность), добавляет аутентификацию, а внешние IP-адреса (шлюзов) скрывают внутреннюю топологию.
4. OpenVPN в режиме bridge на транспортном уровне — шифрует трафик, но не может скрыть исходные IP-адреса при передаче через интернет без дополнительной настройки NAT.
5. Протокол L2TP без IPsec — обеспечивает туннелирование, но не шифрует данные (только инкапсуляция), нарушая требование конфиденциальности.

Критерии оценки:

Баллы начисляются автоматически пропорционально правильным ответам.

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, сокет, 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 COA Snort на обнаружение ICMP пакетов большой длины
77.	Оценка показателей объектов защиты
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 туннельному 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 демилитаризованных 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»	85-100 баллов
		«хорошо»	70-84 баллов
		«удовлетворительно»	55-69 баллов
		«неудовлетворительно»	0-54 баллов

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
7	Экзамен	«отлично»	85-100 баллов практические работы выполнены грамотно или имеют несущественные замечания; обучающийся владеет теоретическим материалом, отвечает на дополнительные вопросы
		«хорошо»	70-84 балла практические работы выполнены грамотно или имеют несущественные замечания; обучающийся владеет основным теоретическим материалом, отвечает на дополнительные вопросы, с неточностями
		«удовлетворительно»	55-69 баллов практические работы выполнены, имеют замечания; обучающийся владеет теоретическим материалом, не отвечает на дополнительные вопросы
		«неудовлетворительно»	0-54 баллов практические работы не выполнены или имеют существенные замечания; обучающийся не владеет теоретическим материалом, не отвечает на дополнительные вопросы или отвечает с грубыми ошибками

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	Фаронов, А. Е.	Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 с. — ISBN 978-5-4497-2418-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133957.html	учебное пособие	2024	Цифровой образовательный ресурс IPR SMART
2	Мельников, А. В.	Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : Российский государственный университет правосудия имени В.М. Лебедева, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/152309.html	учебное пособие	2025	Цифровой образовательный ресурс IPR SMART
3	Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М.	Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е.	учебное пособие	2025	Цифровой образовательный ресурс IPR SMART

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
	Суровов	В. Смирнова, А. М. Суровов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/146404.html			
4	Мэйволд, Э.	Безопасность сетей : учебное пособие / Э. Мэйволд. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/146327.html	учебное пособие	2025	Цифровой образовательный ресурс IPR SMART
5	Куликов, С. С.	Информационная безопасность локальных компьютерных сетей : практикум / С. С. Куликов. — Воронеж : Воронежский государственный технический университет, ЭБС АСБ, 2021. — 57 с. — ISBN 978-5-7731-0969-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL:	практикум	2021	Цифровой образовательный ресурс IPR SMART

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		https://www.iprbookshop.ru/118614.html			

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	М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг, К. А. Ахrameева	Безопасность беспроводных локальных сетей : учебное пособие / М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг, К. А. Ахrameева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2021. — 71 с. — ISBN 978-5-89160-227-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/279623	учебное пособие	2021	Лань : электронно-библиотечная система
2	Костин, В. Н.	Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART :	учебное пособие	2018	Цифровой образовательный ресурс IPR SMART

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		[сайт]. — URL: https://www.iprbookshop.ru/98200.html			

8.3. Перечень профессиональных баз данных и информационных справочных систем

№ пп	Наименование	Ссылка
1	Springer Nature (Полнотекстовая коллекция журналов)	https://www.springernature.com/gp/products
2	Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature)	https://link.springer.com/
3	«Кодекс»	https://kodeks.ru/
4	Техэксперт	https://cntd.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Консультант+	Договор №1522 от 25.12.2015, срок действия - бессрочно
2	Windows: WinPro 10 RUS Upgrd OLP NL Acdmc	договор № 757 от 04.07.2018, срок действия – бессрочно; контракт № 1653 от 14.12.2018, срок действия – бессрочно
3	Office Standard: ⁴ Office Stdandard 2013 Russian OLP NL AcademicEdition	договор № 690 от 19.05.2015, 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	Помещение для самостоятельной работы обучающихся Д -409	Стол-ы-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
2	Помещение для самостоятельной работы обучающихся Г-401	Стол-ы, стулья, компьютеры
3	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа.	Стол-ы ученические двухместные, стулья, стол преподавательский, стул

№ 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
	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. Д-402	преподавательский, доска аудиторная (меловая), кафедра напольная
4	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. Д-413	Стол ученические двухместные, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая) , кафедра напольная
5	Лаборатория кибербезопасности. Лаборатория «Автоматизированные системы в защищенном исполнении». Лаборатория «Программно-аппаратные средства защиты информации». Лаборатория «Безопасность вычислительных сетей» Лаборатория «Техническая защита информации». Лаборатория «Сети и системы передачи информации». Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования. Аудитория для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну Э-101в	Стол компьютерные, стол преподавательский, стулья, шкаф металлический, телевизор на передвижной тумбе, стойка телекоммуникационная, коммутатор оптический Qtech QSW-6910-26F, коммутатор Qtech QSW-4610-28T-AC, система хранения данных Русский щит Alpha DF5045, сервер Русский щит Gamma SX6302, ноутбук Digma Pro Sprint M DN15P3-8CXW02, осциллограф АКИП-4115/1А, анализатор низкочастотных сигналов СКМ-21, генератор сигналов АКИП-3407/1А, антенна дипольная активная Е-3000А1, антенна рамочная Н-30А1, акустический излучатель АС-1 Лайт Арт.001, рефлектометр ТОПА3-7317-ARX, измерительный пробник напряжения ШИП, анализатор спектра АКИП-4211/1, межсетевой экран ССПТ-2

