МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

«Утверждаю»
Декан естественнонаучного факультета
_____ Пещукович А.И.
«____»_____2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита сетевых информационных технологий

Направление подготовки - 10.03.01 «Информационная безопасность»
Профиль подготовки – Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Форма подготовки – Очная
Уровень подготовки – Бакалавриат

ДУШАНБЕ - 2026

Рабочая программа составлена на основе требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» **(**уровень Бакалавриат), утвержденного приказом Министерства образования и науки РФ №524 от 08.06.2017 г., Концепции преподавания Защита сетевых информационных технологий для специальностей и направлений подготовки, реализуемых в образовательных организациях высшего образования, утвержденной протоколом Экспертного совета по развитию исторического образования Минобрнауки РФ от 06.08.2024 г. №ВФ/35-ПР

При разработке рабочей программы учитываются

- содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры Кафедра информатики и информационных технологий протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена УМС естественнонаучного факультета протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена Ученым советом естественнонаучного факультета, протокол № 1 от «___» _____ 2025 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Актуальность изучения дисциплины «Защита сетевых информационных технологий»

1.1 Цели изучения дисциплины Целью освоения дисциплины «Защита сетевых информационных технологий» является формирование у студентов теоретических знаний и практических навыков в области обеспечения безопасности компьютерных сетей. Дисциплина направлена на изучение современных угроз информационной безопасности, методов и средств защиты сетевых ресурсов, а также на формирование умений по разработке и внедрению эффективных решений для защиты сетей. В результате освоения дисциплины студенты должны быть готовы к решению задач по обеспечению безопасности сетевой инфраструктуры в различных организациях.

1.2 Задачи изучения дисциплины Изучение основных принципов и концепций информационной безопасности. Освоение методов анализа уязвимостей и оценки рисков в сетевых системах. Изучение современных сетевых атак и способов противодействия им. Формирование практических навыков по настройке и администрированию средств защиты сетевой безопасности. Развитие умений по разработке и реализации стратегий защиты сетевых информационных технологий.

1.3 В результате изучения дисциплины «Защита сетевых информационных технологий» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Индикаторы достижения компетенции	Вид оценки
УК-2.	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из	"ИУК-2.1 Формулирует совокупность взаимосвязанных задач. ИУК-2.2 Определяет ресурсное обеспечение. ИУК-2.3 Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач.	

	действующих правовых норм, имеющихся ресурсов и ограничений	ИУК-2.4 Выполняет задачи в рамках своей ответственности и при необходимости корректирует способы их решения."	
ПК-2.	Способен разрабатывать и адаптировать прикладное программное обеспечение	ИПК-2.1 Применяет современные технологии разработки и адаптации прикладного ПО. ИПК-2.2 Разрабатывает и адаптирует ПО на современных языках программирования. ИПК-2.3 Применяет современные технологии для разработки веб-приложений.	
ПК-3.	Способен проектировать информационные системы по видам обеспечения	ИПК-3.1 Обосновывает выбор проектных решений по видам обеспечения ИС. ИПК-3.2 Участвует в проектировании экономических ИС и их модулей.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Защита сетевых информационных технологий»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.07).** В процессе преподавания данного курса учитываются знания студентов по таким дисциплинам, как история таджикского народа, история первобытного общества, история древнего мира и средних веков, изучавшихся ими в общеобразовательной средней школе.

2.2 Преподавание данной дисциплины является необходимым для дальнейшего освоения студентами дисциплин в структуре ОПОП бакалавриата по направлению **«Информационная безопасность».**

Таблица 2.

№ п/п	Название дисциплины	Семестр	Место дисциплины в структуре ОПОП

-	—	—	Предшествующая дисциплина
-	—	—	Последующая дисциплина

При освоении данной дисциплины необходимы умения и готовность («входные» знания) обучающегося по дисциплинам, указанных в Таблице 2. Дисциплины взаимосвязаны с данной дисциплиной, они изучаются параллельно. Теоретическими дисциплинами, для которых освоение данной дисциплины необходимо как предшествующее являются:

3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА, КРИТЕРИИ НАЧИСЛЕНИЯ БАЛЛОВ

Преподавание курса «Защита сетевых информационных технологий» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 126 часа, из которых: лекции – 20 часов, практические занятия – 14 часов, лабораторные работы 20 часов, иная контактная работа – 32 часа, самостоятельная работа – 56. Всего часов аудиторной нагрузки – 70 часа.

По итогам 1 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в защиту сетевых информационных технологий. Основные понятия и определения.

Обзор дисциплины, цели и задачи. Понятие информационной безопасности, актуальность защиты сетевых технологий. Угрозы, уязвимости, атаки.

Лекция 2 Основы сетевых технологий и модели OSI/TCP/IP.

Обзор сетевых протоколов. Уровни модели OSI. Адресация, маршрутизация. Уязвимости на разных уровнях.

Лекция 3 Угрозы информационной безопасности в сетях. Типы атак.

Классификация угроз. Социальная инженерия. Атаки на пароли. DDoS-атаки. Вредоносное ПО.

Лекция 4 Методы аутентификации и авторизации в сетях.

Парольная защита. Многофакторная аутентификация. Криптография и ее применение в сетях.

Лекция 5 Межсетевые экраны (Firewall). Принципы работы и типы.

Stateful inspection, Proxy Firewall. Настройка и конфигурация межсетевых экранов.

Лекция 6 Системы обнаружения и предотвращения вторжений (IDS/IPS).

Принципы работы. Методы обнаружения атак. Ловушки (honeypots).

Лекция 7 Защита беспроводных сетей (Wi-Fi).

Стандарты безопасности. WEP, WPA, WPA2/3. Аудит безопасности Wi-Fi сетей.

Лекция 8 Правовые аспекты защиты информации. Стандарты и нормативные документы.

Федеральные законы в области защиты информации. Рекомендации по обеспечению безопасности.

Лекция 9 Разработка политики безопасности организации.

Разработка политики безопасности, основные разделы. Практические рекомендации по разработке.

Лекция 10 VPN технологии. Обзор и применение в сетевой безопасности.

Типы VPN. Настройка и конфигурация VPN. Обеспечение безопасного удаленного доступа.

Структура и содержание практической части курса

Практическое занятие 1 Настройка сетевых устройств и сетевого оборудования. (Практика)

Настройка сетевых интерфейсов, маршрутизаторов, коммутаторов. Базовые команды.

Практическое занятие 2 Использование инструментов для анализа сетевого трафика (Wireshark). (Практика)

Перехват и анализ пакетов. Фильтрация трафика. Выявление аномалий.

Практическое занятие 3 Практическое применение межсетевых экранов (Firewall). (Практика)

Настройка правил фильтрации. Создание правил для различных типов трафика.

Практическое занятие 4 Настройка и использование систем обнаружения вторжений (IDS/IPS). (Практика)

Установка и настройка Snort или Suricata. Анализ журналов событий. Реакция на атаки.

Практическое занятие 5 Аудит безопасности беспроводных сетей. (Практика)

Сканирование Wi-Fi сетей. Анализ безопасности. Выявление уязвимостей.

Практическое занятие 6 Настройка и использование VPN-сервисов (OpenVPN, WireGuard). (Практика)

Настройка сервера и клиентов. Обеспечение безопасного удаленного доступа.

Практическое занятие 7 Защита от DDoS-атак. Применение инструментов и техник. (Практика)

Использование инструментов для противодействия DDoS. Настройка защиты.

Практическое занятие 8 Практикум по анализу уязвимостей сетевого оборудования. (Практика)

Сканирование уязвимостей. Анализ отчетов. Рекомендации по устранению.

Практическое занятие 9 Настройка безопасного удаленного доступа к сети. (Практика)

Использование SSH, VPN. Настройка двухфакторной аутентификации.

Практическое занятие 10 Создание и настройка политик безопасности. (Практика)

Разработка шаблонов политик безопасности. Реализация политик безопасности.

Структура и содержание лабораторной части курса

Лабораторная работа 1 Установка и настройка виртуальной среды для проведения лабораторных работ.

Установка и настройка виртуальных машин (VirtualBox, VMware).

Лабораторная работа 2 Практическое использование Wireshark для анализа сетевого трафика.

Перехват и анализ сетевых пакетов. Анализ протоколов.

Лабораторная работа 3 Настройка и использование межсетевого экрана (Firewall) на базе Linux.

Настройка iptables/nftables. Фильтрация трафика.

Лабораторная работа 4 Настройка и использование системы обнаружения вторжений (IDS) на базе Snort.

Установка, настройка правил, анализ журналов.

Лабораторная работа 5 Настройка и использование системы обнаружения вторжений (IPS) на базе Suricata.

Установка, настройка правил, анализ журналов.

Лабораторная работа 6 Настройка и использование VPN-сервера на базе OpenVPN.

Установка, настройка сертификатов, подключение клиентов.

Лабораторная работа 7 Защита беспроводной сети Wi-Fi.

Настройка WPA/WPA2/WPA3. Анализ безопасности.

Лабораторная работа 8 Практическое применение инструментов для сканирования уязвимостей (Nmap, Nessus).

Сканирование хостов, анализ результатов, отчеты.

Лабораторная работа 9 Использование Kali Linux для тестирования на проникновение.

Обзор инструментов, базовые атаки.

Лабораторная работа 10 Настройка и использование системы SIEM (Security Information and Event Management).

Установка и настройка, анализ событий безопасности.

Структура и содержание КСР

КСР 1 Разработка плана защиты сети небольшой организации.

Анализ рисков, выбор средств защиты, документирование.

КСР 2 Анализ уязвимостей веб-приложения и рекомендации по устранению.

Выявление уязвимостей, предложения по защите, отчет.

КСР 3 Создание отчета по аудиту безопасности Wi-Fi сети.

Сканирование, анализ, выводы, рекомендации.

КСР 4 Разработка политики безопасности для выбранной организации.

Выбор отрасли, написание документа, обоснование.

КСР 5 Разработка сценария реагирования на инцидент ИБ.

Выбор инцидента, план действий, документация.

Структура и содержание СРС

СРС 1 Изучение современных сетевых атак и методов защиты.

Самостоятельное изучение материалов по теме, подготовка презентации.

СРС 2 Анализ уязвимостей в конкретном сетевом оборудовании.

Поиск информации, анализ, составление отчета.

СРС 3 Подготовка обзора по методам обнаружения вторжений.

Изучение литературы, создание презентации или реферата.

СРС 4 Изучение стандартов и нормативных документов по ИБ.

Самостоятельное изучение, конспектирование.

СРС 5 Подготовка доклада по теме "Защита облачных сервисов".

Поиск информации, подготовка доклада, презентация.

СРС 6 Изучение современных систем SIEM.

Обзор различных систем SIEM, их возможностей.

СРС 7 Подготовка реферата по теме "Криптографические алгоритмы и их применение".

Изучение алгоритмов, анализ применения, написание реферата.

СРС 8 Изучение методик анализа вредоносного ПО.

Самостоятельное изучение, подготовка обзора.

СРС 9 Подготовка к контрольным точкам.

Повторение пройденного материала, подготовка к тестированию.

СРС 10 Изучение вопросов правового регулирования ИБ.

Анализ нормативных актов, подготовка обзора.

СРС 11 Подготовка презентации по теме "Современные угрозы веб-приложениям".

Поиск информации, анализ, подготовка.

СРС 12 Изучение способов защиты от DDoS-атак.

Анализ методов защиты, подготовка доклада.

СРС 13 Разработка плана реагирования на инцидент.

Самостоятельная работа.

СРС 14 Исследование методов обеспечения безопасности IoT устройств.

Анализ актуальных угроз и методов защиты.

СРС 15 Подготовка презентации: "Безопасность облачных вычислений".

Изучение безопасности облачных платформ, подготовка презентации.

СРС 16 Анализ конкретного инцидента информационной безопасности.

Анализ произошедшего инцидента, выводы и рекомендации.

СРС 17 Изучение средств защиты виртуализации.

Самостоятельное изучение, подготовка реферата или презентации.

СРС 18 Исследование применения машинного обучения в ИБ.

Изучение материалов, подготовка обзора.

СРС 19 Подготовка к промежуточной аттестации.

Повторение пройденного материала, подготовка к экзамену.

СРС 20 Изучение уязвимостей в современных операционных системах.

Самостоятельное изучение.

СРС 21 Анализ существующих стандартов в области ИБ.

Изучение стандартов (ISO 27001 и др.), подготовка реферата.

СРС 22 Подготовка к экзамену.

Обобщение знаний по всему курсу.

СРС 23 Подготовка реферата по теме: "Использование систем обнаружения и предотвращения вторжений".

Самостоятельный поиск информации, анализ, подготовка отчета.

СРС 24 Анализ методик пентеста и их применения.

Изучение различных методик пентеста, составление отчета.

СРС 25 Обзор инструментов для анализа вредоносного ПО.

Обзор инструментов для анализа вредоносного ПО.

СРС 26 Анализ существующих политик безопасности.

Изучение политики безопасности.

СРС 27 Обзор инструментов для анализа безопасности веб-приложений.

Изучение методов тестирования и анализа веб-приложений.

СРС 28 Практическое использование инструментария для анализа безопасности сети.

Практический анализ и тестирование на основе инструментария.

Структура и содержание теоретической, лабораторной части курса, КСР и СРС

Таблица 3.

№ п/п	Наименование темы	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Литра	Количество баллов
		Лек	Прак	КСР	Лаб	СРС	ИКР		
1	Введение в защиту сетевых информационных технологий. Основные по-ня-тия и определения.	2		2		4		1	10
	Настройка сетевых устройств и сетевого оборудования.		2					4	
2	Установка и настройка виртуальной среды для проведения лаборатор-ных работ.				2	4		3	10
3	Основы сетевых технологий и модели OSI/TCP/IP.	2						6	10
	Использование инструментов для анализа сетевого трафика (Wireshark)		2			4		5	
4	Практическое использование Wireshark для анализа сетевого трафика.				2			4	10
5	Угрозы информационной безопасности в сетях. Типы атак.	2		2		4		2	10
	Практическое применение межсетевых экранов (Firewall).		2					5	
6	Настройка и использование межсетевого экрана (Firewall) на базе Linux.				2	4		7	10
7	Методы аутентификации и авторизации в сетях.	2						2	10
	Настройка и использование систем обнаружения вторжений (IDS/IPS).		2					2	
8	Настройка и использование системы обнаружения вторжений (IDS) на базе Snort.				2	4		1	10
9	Межсетевые экраны (Firewall). Принципы работы и типы.	2		2				4	10
	Аудит безопасности беспроводных сетей.		2			2		5	
10	Настройка и использование системы обнаружения вторжений (IPS) на базе Suricata.				2			3	10

11	Системы обнаружения и предотвращения вторжений (IDS/IPS).	2				4		2	10
	Настройка и использование VPN-сервисов (OpenVPN, WireGuard).		2					5	
12	Настройка и использование VPN-сервера на базе OpenVPN.				2	4		6	10
13	Защита беспроводных сетей (Wi-Fi).	2		2				5	10
14	Защита от DDoS-атак. Применение инструментов и техник.		2			4		6	10
15	Защита беспроводной сети Wi-Fi.				2			5	10
	Правовые аспекты защиты информации. Стандарты и нормативные до-кументы.	2				2		4	
16	Практикум по анализу уязвимостей сетевого оборудования.		2					5	10
17	Практическое применение инструментов для сканирования уязвимостей (Nmap, Nessus).				2				10
	Разработка политики безопасности организации.	2		2					
18	Настройка безопасного удаленного доступа к сети.		2						10
19	Использование Kali Linux для тестирования на проникновение.				2				10
	VPN технологии. Обзор и применение в сетевой безопасности.	2							
20	Создание и настройка политик безопасности.		2						10
	Настройка и использование системы SIEM (Security Information and Event Management).				2				
Итого:		20	20	10	20	40	0		200

Формы контроля и критерии начисления баллов

Контроль усвоения студентом каждой темы осуществляется в рамках балльно-рейтинговой системы (БРС), включающей текущий, рубежный и

итоговый контроль. Студенты **1 -го курса**, обучающиеся по кредитно-рейтинговой системе обучения, могут получить максимально возможное количество баллов - 300. Из них на текущий и рубежный контроль выделяется 200 баллов или 49% от общего количества.

На итоговый контроль знаний студентов выделяется 51% или 100 баллов.

Порядок выставления баллов: 1-й рейтинг (1-7 недели до 12,5 баллов+12,5 баллов (8 неделя – Рубежный контроль №1) = 100 баллов), 2-й рейтинг (9-15 недели до 12,5 баллов+12,5 баллов (16 неделя – Рубежный контроль №2) = 100 баллов), итоговый контроль 100 баллов.

К примеру, за текущий и 1-й рубежный контроль выставляется 100 баллов: лекционные занятия – 21 балл, за практические занятия (КСР, лабораторные) – 31,5 балл, за СРС – 17,5 баллов, требования ВУЗа – 17,5 баллов, рубежный контроль – 12,5 баллов.

В случае пропуска студентом занятий по уважительной причине (при наличии подтверждающего документа) в период академической недели деканат факультета обращается к проректору по учебной работе с представлением об отработке студентом баллов за пропущенные дни по каждой отдельной дисциплине с последующим внесением их в электронный журнал.

Итоговая форма контроля по дисциплине (зачет, экзамен) проводится как в форме тестирования, так и в традиционной (устной) форме. Тестовая форма итогового контроля по дисциплине предусматривает: для естественнонаучных направлений – 10 тестовых вопросов на одного студента, где правильный ответ оценивается в 10 баллов, для гуманитарных направлений – 25 тестовых вопросов, где правильный ответ оценивается в 4 балла. Тестирование проводится в электронном виде, устный экзамен на бумажном носителе с выставлением оценки в ведомости по аналогичной системе с тестированием.

Таблица 4.

Неделя	Активное участие на лекционных занятиях, написание конспекта и выполнение других видов работ*	Активное участие на практических (семинарских) занятиях, КСР	СРС Написание реферата, доклада, эссе Выполнение других видов работ	Выполнение положения высшей школы (установленная форма одежды, наличие рабочей папки, а также других пунктов устава высшей школы)	РК №1	Всего
1	2	3	4	5	6	7
1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Первый рейтинг	21	31,5	17,5	17,5	12,5	100
1	2	3	4	5	6	7
1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Второй рейтинг	21	31,5	17,5	17,5	12,5	100
Итог						200

Формула вычисления результатов дистанционного контроля и итоговой формы контроля по дисциплине за семестр для студентов 1 -го курсов:

$$ИБ = \left[\frac{(P_1 + P_2)}{2}\right] \cdot 0{,}49 + Эи \cdot 0{,}51 \ ,$$

где ИБ –итоговый балл, P_1- итоги первого рейтинга, P_2- итоги второго рейтинга, *Эи*– результаты итоговой формы контроля (экзамен).

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы обработки информации» включает в себя:

1. план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

2. характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

3. требования к представлению и оформлению результатов самостоятельной работы;

4. критерии оценки выполнения самостоятельной работы.

План-график выполнения самостоятельной работы по дисциплине

4.1. План-график выполнения самостоятельной работы по дисциплине

№	Объем СРС, ч.	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля
1	4	Основы защиты сетевых информационных технологий	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	Архитектура компьютерных сетей и уязвимости	Вопросы 5–8. Презентация методов	Выступление
3	6	Модель угроз и атак в сетях передачи данных	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Сетевые атаки и методы их реализации	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Политика безопасности компьютерных сетей	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Межсетевые экраны и системы фильтрации трафика	Выполнение задания 2	Защита работы
7	6	Системы обнаружения и предотвращения вторжений (IDS/IPS)	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Криптографическая защита сетевых соединений	Вопросы 16–17. Выполнение задания 4	Защита работы
9	4	Защита беспроводных сетей	Выполнение задания 5	Защита работы
10	4	Безопасность сетевых протоколов и сервисов	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Аутентификация и управление доступом в сетях	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы

12	4	Мониторинг и журналирование сетевых событий безопасности	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы
13	4	Реагирование на сетевые инциденты безопасности	Вопросы 32–37. Презентация	Опрос, выступление
14	4	Виртуальные частные сети и защищённые каналы связи	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Защита корпоративных и распределённых сетей	Вопросы 41–44. Выполнение задания 9	Защита работы
16	4	Комплексная система защиты сетевых ИТ	Вопросы 45–46. Выполнение задания 8 (4–10)	Защита работы

4.2 Характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

Для выполнения задания, прежде всего, необходимо ознакомиться и изучить основные положения теоретических материалов соответствующей темы из литературных источников. Они указаны в разделе «Содержание и структура дисциплины». Конспекты и задания можно выполнить в отдельном тетради или в лекционной (практической) тетради в произвольной форме.

4.3 Критерии оценки выполнения самостоятельной работы.

Критерии оценки выполнения самостоятельной работы является полнота освещения вопроса, логичность изложения, проявления самостоятельность в обработке материала.

4.4. Критерии оценки выполнения самостоятельной работы.

Самостоятельная работа прививает студентам навыки работы с источниками и учебной литературой, помогает повысить уровень знаний по предмету, которые можно использовать на практике.

Оценка «отлично» выставляется студенту, если индивидуальное задание выполнено полностью и по данной теме защищена лабораторная работа.

Оценка «хорошо» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено с отдельными замечаниями.

Оценка «удовлетворительно» выставляется студенту, если лабораторная

работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

Оценка «неудовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания не защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕ- ЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература:

1. 1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — 5-е изд. — СПб.: Питер, 2020. — 992 с.

2. Гусев А.В. Защита информации в компьютерных системах и сетях: Учебник. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2020. – 384 с.

3. Галатенко В.А. Сетевая безопасность. – М.: Интернет-Университет Информационных технологий, 2020. – 288 с.

4. Федоров А.В. Безопасность компьютерных сетей: учебное пособие / А.В. Федоров. - М.: ФОРУМ, 2020. - 384 с.

5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2019. – 608 с.

6. Щербаков А.Ю. Безопасность информационных систем. Учебное пособие. - М.: КУРС: ИНФРА-М, 2019. – 272 с.

7. Ларин И.В. Безопасность сетей TCP/IP. - СПб.: БХВ-Петербург, 2019. - 464 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Столлингс В. Криптография и защита сетей. – М.: Вильямс, 2017.

2. Слюсарь Н.В., Яковлев С.А. Безопасность компьютерных сетей: Учебное пособие. – М.: Юрайт, 2018.

3. Баранов В.В., Попов А.Н., Прокофьев А.В. Технические средства защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2017.

4. Васильев А.А. Защита информации в компьютерных системах. – М.: ЭКОМ, 2018.

5. Петров М.В. Безопасность компьютерных сетей: Учебное пособие. – СПб.: Питер, 2019.

6. Бойко А.В. Безопасность информационных систем: учеб. пособие / А.В. Бойко. - М.: ИНФРА-М, 2019.

7. Голубцов С.А. Информационная безопасность: учебник и практикум для вузов / С.А. Голубцов, А.В. Басаев. - М.: Юрайт, 2020.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. Сайт ФСТЭК России: https://fstec.ru/

2. Сайт CERT-RU: https://cert.gov.ru/

3. OWASP (Open Web Application Security Project): https://owasp.org/

4. NIST (National Institute of Standards and Technology): https://www.nist.gov/

5. SecurityLab.ru: https://www.securitylab.ru/

5.4. Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для обеспечения систематической и регулярной работы по изучению дисциплины «Защита сетевых информационных технологий» и успешного прохождения текущих и итоговых контрольных испытаний студенту рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.

2. Регулярно изучать каждую тему дисциплины, используя различные формы индивидуальной работы.

3. Согласовывать с преподавателем виды работы по изучению дисциплины.

4. По завершении отдельных тем передавать выполненные работы (рефераты) преподавателю.

Обучение по дисциплине «Защита сетевых информационных технологий» строится следующим образом. На лекциях преподаватель дает общую характеристику рассматриваемого вопроса, различные научные концепции или позиции, которые есть по данной теме. Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме. Во время лекционного занятия необходимо фиксировать все спорные моменты и проблемы, на которых останавливается преподаватель. Потом именно эти аспекты станут предметом самого пристального внимания и изучения на практических занятиях.

При подготовке к практическому занятию обязательно требуется изучение дополнительной литературы по теме занятия. Без использования нескольких источников информации невозможно проведение дискуссии на занятиях, обоснование собственной позиции, построение аргументации. Если обсуждаемый аспект носит дискуссионный характер, следует изучить существующие точки зрения и выбрать тот подход, который вам кажется наиболее верным. При этом следует учитывать необходимость обязательной аргументации собственной позиции. Во время практических занятий рекомендуется активно участвовать в обсуждении рассматриваемой темы, выступать с подготовленными заранее рефератами, докладами и презентациями.

Самостоятельная работа должна соответствовать графику прохождения программы дисциплины. Самостоятельная работа по дисциплине «Защита сетевых информационных технологий» включает:

а) работу с литературой;

б) подготовку устного выступления на практическом занятии;

в) подготовку к занятию в интерактивной форме;

г) подготовку реферата с презентацией;

д) подготовку к дискуссии;

е) заполнение хронологической таблицы;

ж) подготовку к текущей и итоговой аттестации по дисциплине.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, которая может осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа студентов предполагает самостоятельное изучение отдельных тем, дополнительную подготовку студентов к каждому практическому занятию.

Самостоятельная работа студентов является важной формой образовательного процесса. Она реализуется непосредственно в процессе аудиторных занятий, в контакте с преподавателем, а также в библиотеке, дома, при выполнении студентом учебных и творческих задач.

Цель самостоятельной работы студентов - научить студента осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию.

При изучении дисциплины организация самостоятельной работы студентов форм представлена следующим образом:

1) внеаудиторная самостоятельная работа;

2)аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя.

Аудиторная самостоятельная работа может реализовываться при проведении практических занятий и во время чтения лекций.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

Для проведения занятий необходимо иметь большой банк заданий, причем эти задания могут быть дифференцированы по степени сложности.

На каждом этапе самостоятельной работы следует разъяснять цели работы, контролировать понимание этих целей студентами, постепенно формируя у них

умение самостоятельной постановки задачи и выбора цели.

При чтении лекционного курса непосредственно в аудитории необходимо контролировать усвоение материала основной массой студентов

путем проведения экспресс-опросов по конкретным темам.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

На практических занятиях нужно не менее 1 часа из двух (50% времени) отводить на самостоятельное рассмотрение заданий.

По результатам самостоятельного рассмотрения задания следует выставлять по каждому занятию оценку. Оценка предварительной подготовки студента к практическому занятию может быть сделана путем экспресс-опроса в течение 5, максимум - 10 минут.

По материалам раздела целесообразно выдавать студенту домашнее задание и на последнем практическом занятии по разделу подвести итоги его изучения (например, провести контрольную работу), обсудить оценки каждого студента, выдать дополнительные задания тем студентам, которые хотят повысить оценку.

Результативность самостоятельной работы студентов во многом определяется наличием активных методов ее контроля. Существуют следующие виды контроля:

- входной контроль знаний и умений студентов при начале изучения очередной дисциплины;

- текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических занятиях;

- самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;

- итоговый контроль по дисциплине в виде зачета, зачета с оценкой (в устной форме).

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИТ РТСУ

имеются 4 компьютерных классов. Для занятий используются лицензионное программное обеспечение ОС Windows -7/8/10/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

В Университете созданы специальные условия для обучающихся с ограниченными возможностями здоровья - специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение дисциплины обучающимися с ограниченными возможностями здоровья.

Обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также обеспечивается:

- наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проёмов, лифтов).

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ

ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Промежуточная аттестации осуществляется: для зачета – контрольная работа и опрос. Экзамен проводится в форме тестирования. Защита курсового проекта: представляется пояснительная записка и презентация выступления.

Текущий контроль студентов осуществляется путем защиты лабораторных работ, выполнения самостоятельного задания, обсуждения теоретических вопросов.

Контролирующие материалы по дисциплине содержат:

Контрольные вопросы и задания для текущего контроля знаний по дисциплине.

Тестовые задания для промежуточного контроля знаний по дисциплине;

Методические рекомендации и тематика курсового проектирования.

Также указаны критерии оценки курсового проекта.

Итоговая система оценок по кредитно-рейтинговой системе с использованием буквенных символов

Оценка по буквенной системе	Диапазон соответствующих наборных баллов	Численное выражение оценочного балла	Оценка по традиционной системе
A	10	95-100	Отлично
A-	9	90-94	
B+	8	85-89	Хорошо
B	7	80-84	
B-	6	75-79	
C+	5	70-74	Удовлетворительно
C	4	65-69	
C-	3	60-64	
D+	2	55-59	
D	1	50-54	
Fx	0	45-49	Неудовлетворительно
F	0	0-44	

Содержание текущего контроля, промежуточной аттестации, итогового контроля раскрываются в фонде оценочных средств, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС ВО.

ФОС по дисциплине является логическим продолжением рабочей программы учебной дисциплины. ФОС по дисциплине прилагается.