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
_____ Лешукович А.И.
«____» _____2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Введение в специальность

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 Введение в специальность "Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)"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 информатики и информационных технологий протокол №6 от «30» _____ 2026 г.

Рабочая программа утверждена УМС естественнонаучного факультета протокол №1 от «29» _____ 2025 г.

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

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1.1 Цели изучения дисциплины Целью освоения дисциплины "Введение в специальность "Безопасность компьютерных систем" является формирование у студентов базовых знаний и представлений о профессии, её роли в современном мире, а также развитие навыков, необходимых для успешного обучения и будущей профессиональной деятельности. Дисциплина призвана сформировать у студентов понимание основных принципов и концепций безопасности компьютерных систем, помочь им осознать важность данной области и подготовить к дальнейшему изучению профильных дисциплин.

1.2 Задачи изучения дисциплины Ознакомление студентов с основными понятиями и терминологией в области безопасности компьютерных систем. Формирование представлений о структуре и организации отрасли безопасности компьютерных систем, а также о профессиональных ролях и обязанностях. Развитие навыков поиска и анализа информации, необходимой для решения задач в области безопасности. Формирование у студентов понимания этических и правовых аспектов деятельности в области безопасности компьютерных систем. Развитие у студентов навыков планирования и организации собственной учебной деятельности и саморазвития.

1.3 В результате изучения дисциплины «Введение в специальность "Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)"» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Перечень планируемых результатов обучения	Вид оценочного знания
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИУК-1.1 Анализирует задачу, выделяя её базовые составляющие. ИУК-1.2 Демонстрирует знание особенностей системного и критического мышления и готовность к нему. ИУК-1.3 Аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение.	

		ИУК-1.4 Предлагает возможные варианты решения задачи, оценивая их достоинства и недостатки.	
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	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. ИУК-2.4 Выполняет задачи в рамках своей ответственности и при необходимости корректирует способы их решения.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Введение в специальность»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.01).** 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
1	Информатика	1 семестр	Предшествующая дисциплина
2	Основы информационной безапасности	1 семестр	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 «Введение в специальность "Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)"» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет 72 зачетные единицы. Всего запланировано 72 часа, из которых: лекции – 16 часов, практические занятия – 14 часов, лабораторные работы 0 часов, иная контактная работа – 32 часа, самостоятельная работа – 40. Всего часов аудиторной нагрузки – 32 часа.

По итогам 1 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в специальность. Актуальность и роль безопасности компьютерных систем.

Основные понятия и термины. Место безопасности компьютерных систем в современном мире. Обзор современных угроз и вызовов.

Лекция 2 История развития информационной безопасности.

Эволюция подходов к обеспечению безопасности. Этапы развития и основные вехи. Вклад различных научных школ и специалистов.

Лекция 3 Основные понятия информационной безопасности. Угрозы, уязвимости, риски.

Классификация угроз. Типы уязвимостей. Оценка рисков и методы управления ими.

Лекция 4 Нормативно-правовая база в области информационной безопасности.

Законодательство РФ в области защиты информации. Международные стандарты и рекомендации. Основные документы и их роль.

Лекция 5 Организационные аспекты обеспечения информационной безопасности.

Политики безопасности. Роли и обязанности в области ИБ. Обучение и повышение осведомленности.

Лекция 6 Технические средства защиты информации: обзор и классификация.

Межсетевые экраны, системы обнаружения вторжений, антивирусные программы. Криптографические методы защиты.

Лекция 7 Безопасность сетей и сетевых протоколов.

Атаки на сети. Методы защиты сетевого трафика. Безопасные протоколы.

Лекция 8 Профессиональные роли и карьерные перспективы в области безопасности компьютерных систем.

Обзор востребованных профессий. Необходимые навыки и компетенции. Перспективы развития карьеры.

3.2 Структура и содержание лабораторной части курса

Структура и содержание КСР

КСР 1 Анализ угроз и уязвимостей конкретной организации (кейс-задача). Студенты работают в группах, анализируя заданную организацию и разрабатывая рекомендации по улучшению информационной безопасности.

КСР 2 Организационные аспекты обеспечения информационной безопасности. Разработка политики безопасности для малого предприятия (пример). Настройка политик безопасности операционных систем.

КСР 3 Технические средства защиты информации: обзор и классификация. Настройка межсетевого экрана (на примере виртуальной машины). Использование антивирусного программного обеспечения.

КСР 4 Безопасность сетей и сетевых протоколов. Анализ сетевого трафика с помощью сниффера. Настройка VPN-соединения.

Структура и содержание СРС

СРС 1. История развития защиты информации Подготовка реферата или презентации об эволюции методов защиты: от шифра Цезаря и Скиталы до современных криптографических систем.

СРС 2. Нормативно-правовое регулирование в сфере ИБ Анализ основных законов РФ (ФЗ «О персональных данных», ФЗ «Об информации...», Доктрина информационной безопасности) и составление конспекта по их ключевым положениям.

СРС 3. Классификация угроз информационной безопасности Изучение видов угроз (антропогенные, техногенные, стихийные) и каналов утечки информации. Подготовка сравнительной таблицы по типам вредоносного ПО.

СРС 4. Методы и средства защиты информации Обзор и сравнительный анализ программных, аппаратных и организационных методов защиты. Подготовка к коллоквиуму по теме «Комплексные системы защиты информации».

СРС 5. Основы криптографии и стеганографии Изучение принципов работы симметричного и асимметричного шифрования, электронной подписи. Решение простейших задач по шифрованию данных.

СРС 6. Защита информации в компьютерных сетях Изучение принципов работы межсетевых экранов (Firewall), систем обнаружения вторжений (IDS) и VPN. Подготовка глоссария по сетевой безопасности.

СРС 7. Идентификация, аутентификация и биометрия Анализ современных методов подтверждения личности пользователя: парольная защита, токены, биометрические сканеры. Подготовка доклада о преимуществах и недостатках биометрии.

СРС 8. Профессиональная этика и карьера в ИБ Изучение профессиональных стандартов специалиста по информационной безопасности. Анализ рынка труда и требований работодателей к начальным компетенциям (Hard & Soft Skills).

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	Лекция 1. Введение в специальность. Актуальность и роль безопасности компьютерных систем.	2				5		5	12,50
2	Практическое занятие 1. Введение в специальность. Актуальность и роль безопасности компьютерных систем.		2					2	12,50
3	Лекция 2. История развития информационной безопасности.	2				5		7	12,50
4	КСР 1 Анализ угроз и уязвимостей конкретной организации			2				3	12,50

5	Лекция 3. Основные понятия информационной безопасности. Угрозы, уязвимости, риски.	2				5		2	12,50
6	Практическое занятие 3. Основные понятия информационной безопасности. Угрозы, уязвимости, риски.		2					4	12,50
7	Лекция 4. Нормативно-правовая база в области информационной безопасности.	2				5		6	12,50
8	КСР 2 Организационные аспекты обеспечения информационной без-опасности.			2				1	12,50
9	Лекция 5. Организационные аспекты обеспечения информационной безопасности.	2				5		3	12,50
10	Практическое занятие 5. Организационные аспекты обеспечения информационной безопасности.		2					6	12,50
11	Лекция 6. Технические средства защиты информации: обзор и классификация.	2				5		7	12,50
12	КСР 3 Технические средства защиты информации: обзор и классифика-ция.			2				4	12,50
13	Лекция 7. Безопасность сетей и сетевых протоколов.	2				5		2	12,50
14	Практическое занятие 7. Безопасность сетей и сетевых протоколов.		2					3	12,50
15	Лекция 8. Профессиональные роли и карьерные перспективы в области безопасности компьютерных систем.	2				5		1	12,50
16	КСР 4 Безопасность сетей и сетевых протоколов.			2				2	12,50
Итого:		**16**	**8**	**8**		**40**			**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 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 3-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 в ч.	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля
1.	5	Вот 8 тем для самостоятельной работы студентов (СРС), составленных в соответствии с логикой курса «Введение в специальность» и вашим примером оформления:	Вопросы 1-4. Описание технологии разработки, реферат	Опрос
2.	5	СРС 1. История развития защиты информации Подготовка реферата или презентации об эволюции методов защиты: от шифра Цезаря и Скиталы до современных криптографических систем.	Вопросы 8-10. Презентация, доклад	Выступление
	5	СРС 2. Нормативно-правовое регулирование в сфере ИБ Анализ основных законов РФ (ФЗ «О персональных данных», ФЗ «Об информации...», Доктрина информационной безопасности) и составление конспекта по их ключевым положениям.	Выполнение задания 1 (1-10).	Защита работы.
3.	5	СРС 3. Классификация угроз информационной безопасности Изучение видов угроз (антропогенные, техногенные, стихийные) и каналов утечки информации. Подготовка сравнительной таблицы по типам вредоносного ПО.	Выполнение задания 2	Защита работы.
4.	5	СРС 4. Методы и средства защиты информации Обзор и сравнительный анализ программных, аппаратных и организационных методов защиты. Подготовка к коллоквиуму по теме «Комплексные системы защиты информации».	Выполнение задания 3	Защита работы.
5.	5	СРС 5. Основы криптографии и стеганографии Изучение принципов работы симметричного и асимметричного шифрования, электронной подписи. Решение простейших задач по шифрованию данных.	Выполнение задания 4	Защита работы.

6.	5	СРС 6. Защита информации в компьютерных сетях Изучение принципов работы межсетевых экранов (Firewall), систем обнаружения вторжений (IDS) и VPN. Подготовка глоссария по сетевой безопасности.	Вопросы 18-25.	Защита работы.
7.	5	СРС 7. Идентификация, аутентификация и биометрия Анализ современных методов подтверждения личности пользователя: парольная защита, токены, биометрические сканеры. Подготовка доклада о преимуществах и недостатках биометрии.	Вопросы 26-29.	Опрос. Защита работы
8.	5	СРС 8. Профессиональная этика и карьера в ИБ Изучение профессиональных стандартов специалиста по информационной безопасности. Анализ рынка труда и требований работодателей к начальным компетенциям (Hard & Soft Skills).	Вопросы 30-31. Реферат. Выполнение задания 7	Защита реферата. 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. Гайдамакин, Н. А. Безопасность компьютерных сетей. Учебник и практикум для вузов / Н. А. Гайдамакин, Е. С. Столяров. — М.: Издательство Юрайт, 2023. — 257 с.
2. Гусев, А. В. Информационная безопасность: учебник для вузов / А. В. Гусев, А. А. Гришин. — М.: Издательство Юрайт, 2023. — 217 с.
3. Еськов, В. Г. Безопасность компьютерных систем и сетей: учебник и практикум для вузов / В. Г. Еськов, А. В. Разумовский. — М.: Издательство Юрайт, 2023. — 207 с.
4. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы. Учебное пособие / А. А. Малюк. – СПб.: ВУС, 2021. – 416 с.
5. Минин, Д. И. Основы информационной безопасности: Учебник / Д. И. Минин. – М.: ИНТУИТ, 2019. – 300 с.
6. Щербаков, А. Ю. Основы информационной безопасности. Учебное пособие / А. Ю. Щербаков. — М.: ФЛИНТА, 2021. — 224 с.
7. Ситников, А. И. Безопасность компьютерных систем. Практикум / А. И. Ситников, А. В. Коваленко, С. В. Лебедев. – СПб.: Питер, 2019. – 288 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Ларин, М. В. Информационная безопасность: Учебное пособие. — М.: КноРус, 2022. — 352 с.
2. Хорев, А. А. Защита информации в компьютерных системах: учеб. пособие / А. А. Хорев. – 2-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА-М, 2018. – 304 с.
3. Федотов, А. П. Основы информационной безопасности: Учебник для бакалавров / А. П. Федотов. – М.: Дашков и К, 2019. – 336 с.

4. Концепция информационной безопасности Российской Федерации. Утверждена Указом Президента РФ от 05.12.2016 N 646.
5. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных".
6. Курбатов С.В., Мельников В.П., Михеев А.Н. Информационная безопасность организации: Учебное пособие. – М.: Горячая линия – Телеком, 2017. – 352 с.
7. Соколов А.В. Безопасность информационных систем: Учебное пособие. – СПб.: СПбГУТ, 2017. – 123 с.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Нет данных.

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 «Введение в специальность "Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)"» 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 «Введение в специальность "Безопасность

компьютерных систем (по отрасли или в сфере профессиональной деятельности)"» 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 «Введение в специальность "Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)"» 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.