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

Основы информационной безопасности

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 Основы информационной безопасности 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 «Основы информационной безопасности»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Основы информационной безопасности" является формирование у студентов фундаментальных знаний и практических навыков в области защиты информации. Дисциплина направлена на изучение основных угроз информационной безопасности, методов и средств защиты информации, а также на развитие навыков анализа уязвимостей и разработки эффективных мер защиты. В результате изучения дисциплины студенты должны быть готовы к решению практических задач по обеспечению информационной безопасности в различных сферах.

1.2 Задачи изучения дисциплины Изучение основных понятий, принципов и концепций информационной безопасности. Рассмотрение различных угроз информационной безопасности и методов противодействия им. Освоение методов защиты информации, включая криптографические методы, контроль доступа и сетевую безопасность. Формирование навыков анализа уязвимостей информационных систем и разработки рекомендаций по их устранению. Приобретение знаний об организации процессов обеспечения информационной безопасности в организациях.

1.3 В результате изучения дисциплины «Основы информационной безопасности» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Перечень планируемых результатов обучения	Вид оценочного знания
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		
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности		
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты		
ОПК-1.4	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями		

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Основы информационной безопасности»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.О.11).** 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 «Основы информационной безопасности» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 90 часа, из которых: лекции – 32 часов, практические занятия – 14 часов, лабораторные работы 0 часов, иная контактная работа – 32 часа, самостоятельная работа – 26. Всего часов аудиторной нагрузки – 64 часа.

По итогам 1 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в информационную безопасность. Основные понятия и определения

Обзор дисциплины. Актуальность информационной безопасности. Основные определения: информация, данные, информационная система, угроза, уязвимость, атака. Классификация угроз и атак.

Лекция 2 Политики безопасности и управление рисками

Разработка и реализация политик безопасности. Управление рисками: идентификация, анализ, оценка и обработка рисков. Стандарты информационной безопасности.

Лекция 3 Криптографические методы защиты информации. Симметричное шифрование

Основные принципы криптографии. Симметричные алгоритмы шифрования: DES, 3DES, AES. Режимы работы шифров.

Лекция 4 Криптографические методы защиты информации. Асимметричное шифрование и цифровые подписи

Асимметричные алгоритмы шифрования: RSA, ElGamal. Цифровые подписи. Электронная подпись.

Лекция 5 Аутентификация и авторизация. Контроль доступа

Методы аутентификации: пароли, биометрия, многофакторная аутентификация. Принципы авторизации. Модели контроля доступа.

Лекция 6 Безопасность операционных систем

Защита операционных систем: принципы, средства. Уязвимости операционных систем. Настройка безопасности ОС.

Лекция 7 Безопасность компьютерных сетей. Межсетевые экраны

Сетевые атаки и методы защиты. Межсетевые экраны: принципы работы, типы, настройка.

Лекция 8 Обнаружение и предотвращение вторжений. Системы обнаружения вторжений

Принципы работы систем обнаружения вторжений (IDS). Методы анализа трафика. Системы предотвращения вторжений (IPS).

Лекция 9 Вирусы и вредоносное ПО

Типы вредоносного ПО: вирусы, трояны, черви, шпионское ПО. Методы защиты от вредоносного ПО.

Лекция 10 Безопасность веб-приложений

Уязвимости веб-приложений: XSS, SQL injection, CSRF. Методы защиты веб-приложений.

Лекция 11 Безопасность баз данных

Защита баз данных: контроль доступа, шифрование данных, аудит. Уязвимости баз данных.

Лекция 12 Безопасность беспроводных сетей

Угрозы в беспроводных сетях. Стандарты безопасности беспроводных сетей (WEP, WPA, WPA2, WPA3).

Лекция 13 Социальная инженерия. Человеческий фактор в информационной безопасности

Методы социальной инженерии. Защита от атак социальной инженерии. Обучение пользователей.

Лекция 14 Правовые аспекты информационной безопасности

Законодательство в области информационной безопасности. Персональные данные. Ответственность за нарушения в области ИБ.

Лекция 15 Аудит информационной безопасности

Цели и задачи аудита ИБ. Методы аудита. Составление отчетов об аудите.

Лекция 16 Управление инцидентами информационной безопасности

Процесс реагирования на инциденты. Методы расследования инцидентов. Восстановление после инцидентов.

Структура и содержание КСР

КСР 1 Разработка политики безопасности организации

Разработка проекта политики безопасности для конкретной организации. Определение целей, задач и основных положений политики.

КСР 2 Анализ рисков информационной безопасности

Проведение анализа рисков для заданного сценария. Оценка вероятности угроз и их последствий.

КСР 3 Шифрование данных и защита информации

Решение задач, связанных с выбором оптимальных методов шифрования для различных ситуаций.

КСР 4 Оценка эффективности механизмов аутентификации и авторизации

Анализ различных методов аутентификации и авторизации. Выбор наиболее подходящих методов для конкретных информационных систем.

КСР 5 Анализ уязвимостей операционной системы

Проведение анализа уязвимостей операционной системы. Разработка рекомендаций по устранению уязвимостей.

КСР 6 Настройка межсетевого экрана и защита сети

Решение задач по настройке межсетевых экранов для защиты сети от различных угроз.

КСР 7 Анализ атак на веб-приложения

Анализ распространенных атак на веб-приложения. Разработка рекомендаций по защите от этих атак.

КСР 8 Аудит информационной безопасности

Проведение аудита информационной безопасности на основе заданного сценария. Составление отчета об аудите.

Структура и содержание СРС

СРС 1 Изучение истории развития информационной безопасности

Подготовка реферата по истории развития информационной безопасности, от древних времен до наших дней.

СРС 2 Анализ современных угроз информационной безопасности

Подготовка презентации о современных киберугрозах, включая APT-атаки, целевые атаки, вредоносное ПО.

СРС 3 Исследование криптографических алгоритмов

Изучение одного из криптографических алгоритмов (DES, AES, RSA, ECC и др.) и подготовка доклада.

СРС 4 Разработка модели управления рисками информационной безопасности

Разработка модели управления рисками для конкретной организации или проекта. Подготовка отчета.

СРС 5 Изучение стандартов и нормативных документов в области ИБ

Анализ одного из стандартов или нормативных документов (ISO 27001, PCI DSS, GDPR и др.).

СРС 6 Анализ уязвимостей в конкретном программном обеспечении

Поиск и анализ уязвимостей в определенном программном обеспечении (веб-браузер, операционная система).

СРС 7 Разработка мер по защите от социальной инженерии

Разработка мер по защите от атак социальной инженерии. Подготовка презентации.

СРС 8 Изучение правовых аспектов информационной безопасности

Подготовка реферата по теме правового регулирования информационной безопасности в России.

СРС 9 Разработка сценария реагирования на инциденты

Разработка сценария реагирования на конкретный инцидент ИБ (например, утечка данных).

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)						Лит-ра	Количество
		Лек	Прак	КСР	Лаб	СРС	ИКР		

									баллов
1	Лекция 1 Введение в информационную безопасность. Основные понятия и определения	2						1,5	12,5
	Анализ угроз и уязвимостей информационных ресурсов организации		2					2,6	
2	Лекция 2 Политики безопасности и управление рисками	2						2,4	12,5
	КСР 1 Разработка политики безопасности организации			2				3,2,1,5,6	
3	Лекция 3 Криптографические методы защиты информации. Симмет-ричное шифрование	2						2	12,5
	Разработка и структура политики информационной безопасности		2					5	
4	Лекция 4 Криптографические методы защиты информации. Асиммет-ричное шифрование и цифровые подписи	2						3	12,5
	КСР 2 Анализ рисков информационной безопасности			2				5	
5	Лекция 5 Аутентификация и авторизация. Контроль доступа	2						7	12,5
	Настройка и использование средств симметричного шифрования		2					8,5,4	
6	Лекция 6 Безопасность операционных систем	2						6,5,	12,5
	КСР 3 Шифрование данных и защита информации			2				3,2,4	
7	Лекция 7 Безопасность компьютерных сетей. Межсетевые экраны	2						5,2,3	12,5
	Использование асимметричных алгоритмов и цифровых подписей		2					2,3,1	
8	Лекция 8 Обнаружение и предотвращение вторжений. Системы обнару-жения вторжений	2				3		1,2,3	12,5
	КСР 4 Оценка эффективности механизмов аутентификации и авториза-ции			2				8,5,4	
9	Лекция 9 Вирусы и вредоносное ПО	2				3		6,5,	12,5

	Настройка механизмов аутентификации и разграничения доступа		2					3,2,4	
10	Лекция 10 Безопасность веб-приложений	2				3		5,2,3	12,5
	КСР 5 Анализ уязвимостей операционной системы			2				2,3,1	
11	Лекция 11 Безопасность баз данных	2				3		2	12,5
	Обеспечение безопасности операционной системы		2					5	
12	Лекция 12 Безопасность беспроводных сетей	2				3		3	12,5
	КСР 6 Настройка межсетевого экрана и защита сети			2				5	
13	Лекция 13 Социальная инженерия. Человеческий фактор в информаци-онной безопасности	2				2		5	12,5
	Обнаружение и удаление вредоносного программного обеспечения		2					2	
14	Лекция 14 Правовые аспекты информационной безопасности	2				3		7	12,5
	КСР 7 Анализ атак на веб-приложения			2				8	
15	Лекция 15 Аудит информационной безопасности	2				3		4	12,5
	Обеспечение безопасности беспроводных сетей		2					5	
16	Лекция 16 Управление инцидентами информационной безопасности	2				3		2	12,5
	КСР 8 Аудит информационной безопасности			2				1	
Итого:		32	16	16	0	26	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	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля
1.		СРС 1 Изучение истории развития информационной безопасности	Вопросы 1-4. Описание технологии разработки, реферат	Опрос
2.		СРС 2 Анализ современных угроз информационной безопасности	Вопросы 5-8. Презентация методов	Выступление
3.		СРС 3 Исследование криптографических алгоритмов	Вопросы 8-10. Презентация, доклад	Выступление
4.		СРС 4 Разработка модели управления рисками информационной безопасности	Вопросы 11-13. Выполнение задания 1 (1-10).	Защита работы. Выступление
5.		СРС 5 Изучение стандартов и нормативных документов в области ИБ	Выполнение задания 1. Конспект, презентация (вопросы 14-15)	Опрос, Выступление
6.		СРС 6 Анализ уязвимостей в конкретном программном обеспечении	Выполнение задания 2	Защита работы.
7.		СРС 7 Разработка мер по защите от социальной инженерии	Вопросы 16-17. Выполнение задания 3	Защита работы.
8.		СРС 8 Изучение правовых аспектов информационной безопасности	Вопросы 16-17. Выполнение задания 4	Защита работы.
9.		СРС 9 Разработка сценария реагирования на инциденты	Выполнение задания 5	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. Информационная безопасность: учебник и практикум для вузов. — М.: Юрайт, 2023. — 352 с.

2. Губин А.В. Защита информации: учебник для вузов. — М.: Юрайт, 2021. — 363 с.
3. Мельников В.В. Защита информации в компьютерных системах: учебник для вузов. — М.: Финансы и статистика, 2019. — 368 с.
4. Хорошко В.А., Чечулин А.А. Защита информации в компьютерных системах: учебник для вузов. — М.: Гелиос АРВ, 2018. — 560 с.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях: учебное пособие. — М.: ДМК Пресс, 2019. — 616 с.
6. Липов А.В. Информационная безопасность: учебник для бакалавров. — М.: Издательство Юрайт, 2018. — 429 с.
7. Гостев Р.Г., Калашников А.В., Толстых А.П. Основы информационной безопасности: учебное пособие. — СПб.: Лань, 2019. — 208 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Смирнов А.В. Безопасность компьютерных сетей: учебное пособие.
2. Федотов А.П. Компьютерная криминалистика.
3. Кузьмин А.В. Основы защиты информации.
4. Щербаков А.Ю. Аудит информационной безопасности.
5. Дьяконов А.В. Социальная инженерия в информационной безопасности.
6. Касперски Е.В. Компьютерные вирусы: что это такое?
7. Ковтун Д.В. Правовое регулирование информационной безопасности.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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 «Основы информационной безопасности» 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 «Основы информационной безопасности» 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 «Основы информационной безопасности» 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.