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

Информационная безопасность

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 Информационная безопасность 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 №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

1.1 Цели изучения дисциплины Целью освоения дисциплины "Информационная безопасность" является формирование у студентов теоретических знаний и практических навыков в области защиты информации, ознакомление с правовыми и нормативными основами обеспечения информационной безопасности, а также развитие компетенций, необходимых для разработки, внедрения и сопровождения систем защиты информации. Дисциплина направлена на подготовку специалистов, способных эффективно противостоять угрозам информационной безопасности в различных сферах деятельности.

1.2 Задачи изучения дисциплины Задачи дисциплины:

1. Изучение основных принципов и концепций информационной безопасности.

2. Ознакомление с нормативно-правовыми актами и стандартами в области защиты информации.

3. Освоение методов и средств защиты информации от различных угроз.

4. Формирование навыков анализа уязвимостей и разработки мер по их устранению.

5. Развитие умений по организации и управлению процессами обеспечения информационной безопасности.

1.3 В результате изучения дисциплины «Информационная безопасность» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Перечень планируемых результатов обучения	Вид оценочного знания
УК-5	Способен воспринимать межкультурное разнообразие общества в социально-историческом,	Знать: основные культурные и этические принципы, влияющие на информационную	Реферат

	этическом и философском контекстах	безопасность. Уметь: анализировать влияние межкультурных различий на проблемы информационной безопасности. Владеть: навыками этичного поведения в информационном пространстве.	
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	Знать: нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. Уметь: применять нормативные документы для обеспечения информационной безопасности. Владеть: навыками анализа и применения нормативно-правовой базы.	Тестирование
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации,	Знать: нормативные и методические документы ФСБ и ФСТЭК. Уметь: организовывать защиту информации ограниченного доступа в соответствии с требованиями регуляторов. Владеть: навыками практического применения требований по защите информации ограниченного доступа.	Кейс-задача

	Федеральной службы по техническому и экспортному контролю		
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	Знать: принципы формирования политики информационной безопасности. Уметь: разрабатывать и реализовывать комплекс мер по обеспечению информационной безопасности. Владеть: навыками управления процессом реализации мер защиты.	Проект
ОПК-1.4	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	Знать: принципы оценки уровня безопасности компьютерных систем и сетей. Уметь: оценивать уровень безопасности в соответствии с нормативными требованиями. Владеть: навыками анализа и оценки защищенности компьютерных систем.	Устный опрос
ПК-1	Способен проектировать системы и средства обеспечения информационной безопасности компьютерных систем	Знать: принципы проектирования систем и средств обеспечения информационной безопасности. Уметь: проектировать системы защиты информации.	Курсовая работа

		Владеть: навыками разработки проектной документации.	
ПК-3	Способен сопровождать и совершенствовать системы обеспечения информационной безопасности компьютерных систем	Знать: принципы сопровождения и совершенствования систем обеспечения информационной безопасности. Уметь: сопровождать и совершенствовать системы защиты информации. Владеть: навыками администрирования и оптимизации систем защиты.	Кейс-задача

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Информационная безопасность»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.О.30).** 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 «Информационная безопасность» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 90 часа, из которых: лекции – 10 часов, практические занятия – 14 часов, лабораторные работы 20 часов, иная контактная работа – 32 часа, самостоятельная работа – 50. Всего часов аудиторной нагрузки – 40 часа.

По итогам 6 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

№ 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 информационную безопасность	2				4		1,5	
	Основные понятия и определения.		2			4		2,3	12,5
2	Угрозы информационной безопасности.				2	4		6,5	12,5
3	Рассмотрение базовых понятий, классификации угроз, анализ актуальных проблем.	2				4		7,2	
	Правовые основы информационной безопасности.		2			4		2,3	12,5
4	Законодательство РФ и РТ в области защиты информации.				2	4		2,1	12,5
5	Методы и средства защиты информации.	2				4		6,2	
	Криптография. Шифрование данных.		2			4		4,3	12,5

6	Основы криптографических алгоритмов и их применения для защиты информации.				2			5,1,3,5	12,5
7	Защита компьютерных сетей.	2				4		5,6	
	Межсетевые экраны.		2			4		2,3	12,5
8	Системы обнаружения вторжений.				2	4		6,5	12,5
9	Принципы работы и настройка сетевых экранов, IDS/IPS.	2				4		7,2	
	Безопасность операционных систем.		2			4		2,3	12,5
10	Аудит безопасности.				2	4		2,1	12,5
11	Разграничение доступа.	2				4		6,2	
	Организация безопасной работы операционных систем, аудит событий, управление доступом.		2			4		2,3	12,5
12	Аудит безопасности операционной системы (например, Linux) с использова-нием инструментов, таких как Nessus, и настройка политик безопасности.				2			6,5	12,5
13	Обеспечение безопасности баз данных.	2				4		7,2	
	Резервное копирование и восстановление.		2			4		2,3	12,5
14	Организация и обеспечение безопасности веб-приложений.				2	4		2,1	12,5
15	Анализ уязвимостей веб-приложений и применение методов защиты.	2						6,2	
	Управление доступом и аутентификация пользователей. Парольная за-щита.		2			4		4,3	12,5
16	Безопасность мобильных устройств.				2			5,1,3,5	12,5
Итог		16	16	0	16	80	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 **3 -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 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, ч.	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля
1	4	Понятие и цели информационной безопасности	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	Основные угрозы информационной безопасности	Вопросы 5–8. Презентация методов	Выступление
3	6	Модели и принципы обеспечения ИБ	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Классификация уязвимостей информационных систем	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Политика информационной безопасности организации	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Организационные меры защиты информации	Выполнение задания 2	Защита работы
7	6	Технические средства защиты информации	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Программные средства защиты информации	Вопросы 16–17. Выполнение задания 4	Защита работы
9	4	Криптографические методы защиты информации	Выполнение задания 5	Защита работы
10	4	Защита информации в компьютерных сетях	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Контроль и аудит информационной безопасности	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы
12	4	Правовое обеспечение информационной безопасности	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы
13	4	Управление рисками информационной безопасности	Вопросы 32–37. Презентация	Опрос, выступление

14	4	Реагирование на инциденты ИБ	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Обеспечение непрерывности и восстановление после сбоев	Вопросы 41–44. Выполнение задания 9	Защита работы
16	4	Комплексная система обеспечения ИБ в организации	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. Галатенко В.А. Информационная безопасность. Учебник. М.: Изд-во Инфра-М, 2019. – 544 с.

2. Герасимов А.В., Миронов С.В., Яковлев Д.В. Информационная безопасность. Учебник и практикум. М.: Изд-во Юрайт, 2019. – 411 с.

3. Еськов А.А. Защита информации в компьютерных системах и сетях. Учебное пособие. М.: Изд-во ДМК Пресс, 2019. – 280 с.

4. Караяннис А.А., Федорова С.Ю. Информационная безопасность. Учебное пособие. М.: Изд-во КноРус, 2019. – 320 с.

5. Либерман А.С. Информационная безопасность: учебное пособие. М.: Изд-во РУТ (МИИТ), 2019. – 152 с.

6. Щербаков А.Ю. Безопасность компьютерных сетей. Учебник. М.: Изд-во Форум, 2019. – 352 с.

7. Петров М.Ю. Информационная безопасность: Теоретические основы. – СПб.: Питер, 2018. – 416 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

2. Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

3. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.

4. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Общие положения.

5. Концепция информационной безопасности Российской Федерации (утверждена Президентом РФ).

6. Методика оценки эффективности защиты информации в информационных системах персональных данных (ФСТЭК России).

7. Сборник материалов по информационной безопасности (под ред. Иванова А.В.).

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 «Информационная безопасность» 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 «Информационная безопасность» 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 «Информационная безопасность» 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.