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 автоматизированных систем

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 автоматизированных систем 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 «Информационная безопасность автоматизированных систем»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Информационная безопасность автоматизированных систем" является формирование у студентов теоретических знаний и практических навыков в области защиты информации в автоматизированных системах. Дисциплина направлена на изучение принципов построения, функционирования и анализа угроз безопасности информационных систем, а также на овладение методами и средствами защиты информации. В результате изучения дисциплины студенты должны быть готовы к разработке и внедрению эффективных мер по обеспечению информационной безопасности.

1.2 Задачи изучения дисциплины Изучение основных понятий, принципов и стандартов информационной безопасности. Рассмотрение угроз и уязвимостей информационных систем различных типов. Овладение методами анализа защищенности информационных систем. Изучение средств и способов защиты информации (криптография, межсетевые экраны, системы обнаружения вторжений и т.д.). Формирование практических навыков разработки и реализации мер по обеспечению информационной безопасности.

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

Код	Результаты освоения ООП	Индикаторы достижения компетенции	Вид оценочного знания
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	

	действующих правовых норм, имеющихся ресурсов и ограничений	задач. ИУК-2.4 Выполняет задачи в рамках своей ответственности и при необходимости корректирует способы их решения."	
ПК-1.	Способен проводить обследование организаций и формировать требования к информационной системе	ИПК-1.1 Использует методики обследования организации и выявления информационных потребностей пользователей. ИПК-1.2 Анализирует деятельность предприятия и выявляет участки, нуждающиеся в автоматизации. ИПК-1.3 Выбирает класс ИС, способы автоматизации, оценивает совокупную стоимость владения ИС, планирует стратегическое и оперативное развитие ИС.	
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 **«Информационная безопасность автоматизированных систем»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.08).** 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 автоматизированных систем» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 90 часа, из которых: лекции – 20 часов, практические занятия – 14 часов, лабораторные работы 20 часов, иная контактная работа – 32 часа, самостоятельная работа – 30. Всего часов аудиторной нагрузки – 60 часа.

По итогам 6 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в информационную безопасность. Основные понятия, термины и определения.

Обзор дисциплины. Актуальность информационной безопасности. Типы угроз и уязвимостей. Правовое регулирование.

Лекция 2 Политики безопасности и управление рисками.

Разработка и внедрение политик безопасности. Анализ рисков и оценка уязвимостей.

Лекция 3 Аутентификация и авторизация. Управление доступом.

Методы аутентификации. Системы управления доступом. Ролевая модель доступа.

Лекция 4 Криптографические методы защиты информации.

Основные принципы криптографии. Симметричное и асимметричное шифрование. Электронная подпись.

Лекция 5 Межсетевые экраны (Firewall).

Принципы работы и типы межсетевых экранов. Настройка и администрирование.

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

Принципы работы и классификация IDS/IPS. Методы обнаружения атак.

Лекция 7 Безопасность операционных систем.

Защита ОС Windows и Linux. Настройка безопасности. Аудит безопасности.

Лекция 8 Безопасность баз данных.

Защита баз данных. Методы защиты данных от несанкционированного доступа. Аудит БД.

Лекция 9 Безопасность веб-приложений.

Уязвимости веб-приложений. Методы защиты от атак. Анализ безопасности веб-приложений.

Лекция 10 Безопасность беспроводных сетей.

Стандарты безопасности Wi-Fi. Методы защиты беспроводных сетей. Атаки на беспроводные сети.

Структура и содержание практической части курса

Практическое занятие 1 Практическое применение политик безопасности. (Практика)

Разработка и реализация политик безопасности для организации.

Практическое занятие 2 Анализ рисков и оценка уязвимостей. (Практика)

Применение методик анализа рисков. Оценка уязвимостей информационных систем.

Практическое занятие 3 Настройка средств аутентификации и авторизации. (Практика)

Практическое использование различных методов аутентификации. Настройка прав доступа.

Практическое занятие 4 Практикум по криптографии. (Практика)

Применение различных алгоритмов шифрования. Работа с электронной подписью.

Практическое занятие 5 Настройка и администрирование межсетевых экранов. (Практика)

Настройка правил фильтрации трафика. Мониторинг работы межсетевого экрана.

Структура и содержание лабораторной части курса

Лабораторная работа 1 Введение в лабораторный практикум по информационной безопасности.

Ознакомление с лабораторным оборудованием и программным обеспечением. Техника безопасности.

Лабораторная работа 2 Анализ угроз и уязвимостей.

Использование инструментов для анализа уязвимостей. Создание отчета об уязвимостях.

Лабораторная работа 3: Настройка межсетевого экрана.

Практическое применение межсетевых экранов для защиты сети.

Лабораторная работа 4: Настройка системы обнаружения вторжений.

Настройка и тестирование системы обнаружения вторжений.

Лабораторная работа 5 Криптографические методы защиты информации.

Практическое применение криптографических методов (шифрование, цифровая подпись).

Лабораторная работа 6: Защита операционных систем.

Настройка безопасности операционных систем. Аудит безопасности.

Лабораторная работа 7 Безопасность веб-приложений.

Анализ уязвимостей веб-приложений. Практическое применение средств защиты.

Лабораторная работа 8 Безопасность беспроводных сетей.

Анализ безопасности беспроводных сетей. Поиск и устранение уязвимостей.

Лабораторная работа 9 Защита баз данных.

Настройка безопасности СУБД. Аудит баз данных.

Лабораторная работа 10 Расследование компьютерных инцидентов.

Сбор и анализ данных. Восстановление информации.

Структура и содержание КСР

КСР 1 Разработка политики безопасности организации.

Разработка документа политики безопасности.

КСР 2 Анализ рисков информационной системы.

Проведение анализа рисков информационной системы.

КСР 3 Разработка плана защиты информационной системы.

Разработка плана защиты информационной системы.

КСР 4 Проектирование безопасной сетевой инфраструктуры.

Разработка проекта безопасной сетевой инфраструктуры.

КСР 5 Аудит безопасности информационной системы.

Проведение аудита безопасности информационной системы.

Структура и содержание СРС

СРС 1 Изучение нормативных документов в области информационной безопасности.

Самостоятельное изучение нормативных документов.

СРС 2 Подготовка рефератов и презентаций по темам курса.

Подготовка рефератов и презентаций.

СРС 3 Анализ практических задач в области информационной безопасности.

Решение практических задач.

СРС 4 Изучение современных угроз информационной безопасности.

Анализ актуальных угроз.

СРС 5 Подготовка к тестированию.

Подготовка к тестированию.

СРС 6 Разработка кейс-задач.

Разработка кейс-задач.

СРС 7 Самостоятельная работа с литературой.

Изучение дополнительной литературы.

СРС 8 Поиск и анализ информации в сети Интернет.

Поиск и анализ информации в сети Интернет.

СРС 9 Разработка презентаций по тематике курса.

Разработка презентаций.

СРС 10 Выполнение индивидуальных заданий.

Выполнение индивидуальных заданий.

СРС 11 Подготовка к экзамену.

Подготовка к экзамену.

СРС 12 Анализ инструментов для пентеста.

Анализ инструментов для пентеста.

СРС 13 Анализ актуальных киберугроз

Анализ актуальных киберугроз

СРС 14 Разработка стратегии защиты от киберугроз.

Разработка стратегии защиты от киберугроз.

СРС 15 Поиск уязвимостей в различных системах.

Поиск уязвимостей в различных системах.

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 информационную безопасность. Основные понятия, термины и определения.	2				4		1	10
	Практическое применение политик безопасности.		2					4	
2	Введение в лабораторный практикум по информационной безопасности.				2	4		3	10
3	Политики безопасности и управление рисками.	2						6	10
				2		4		5	
4	Анализ угроз и уязвимостей.				2			4	10
5	Аутентификация и авторизация. Управление доступом.	2				4		2	10
	Анализ рисков и оценка уязвимостей.		2					5	
6	Настройка межсетевого экрана.				2	4		7	10
7	Криптографические методы защиты информации.	2						2	10
	Разработка политики безопасности организации.			2				2	

8	Настройка системы обнаружения вторжений.				2	4		1	10
9	Межсетевые экраны (Firewall).	2						4	10
	Практикум по криптографии.		2			2		5	
10	Анализ рисков информационной системы.				2			3	10
11	Системы обнаружения и предотвращения вторжений (IDS/IPS).	2				4		2	10
	Разработка плана защиты информационной системы.			2				5	
12	Криптографические методы защиты информации.				2	4		6	10
13	Безопасность операционных систем.	2						5	10
14	Настройка и администрирование межсетевых экранов.		2			4		6	10
15	Защита операционных систем.				2			5	10
	Безопасность баз данных.	2				2		4	
16	Проектирование безопасной сетевой инфраструктуры.			2				5	10
17	Безопасность веб-приложений.				2			7	10
	Безопасность веб-приложений.	2						5	
18	Настройка средств аутентификации и авторизации.		2					5	10
19	Защита баз данных.				2			3	10
	Безопасность беспроводных сетей.	2						1	
20	Аудит безопасности информационной системы.			2				5	10
	Безопасность беспроводных сетей.				2			4	
Итого:		20	10	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 **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 особенности автоматизированных систем и их безопасности	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	Классификация автоматизированных систем и угроз	Вопросы 5–8. Презентация методов	Выступление
3	6	Архитектура автоматизированных систем и уязвимости	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Модель угроз и нарушителя для АС	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Политика информационной безопасности АС	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Идентификация и аутентификация в АС	Выполнение задания 2	Защита работы
7	6	Разграничение доступа и управление правами	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Защита программного обеспечения АС	Вопросы 16–17. Выполнение задания 4	Защита работы
9	4	Защита данных и резервное копирование	Выполнение задания 5	Защита работы
10	4	Защита АС в компьютерных сетях	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Контроль и аудит безопасности АС	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы
12	4	Аттестация и сертификация автоматизированных систем	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы
13	4	Реагирование на инциденты в АС	Вопросы 32–37. Презентация	Опрос, выступление
14	4	Управление рисками безопасности АС	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Обеспечение непрерывности функционирования АС	Вопросы 41–44. Выполнение задания 9	Защита работы

16	4	Комплексная система защиты автоматизированной системы	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. 3-е изд., перераб. и доп. М.: Изд-во МГТУ им. Н.Э. Баумана, 2018. 512 с.
2. Щербаков А. Ю. Информационная безопасность. Учебник. М.: Юрайт, 2019. 420 с.
3. Федотов А. П. Информационная безопасность. Курс лекций. СПб.: Питер, 2019. 400 с.
4. Липов А. В. Информационная безопасность автоматизированных систем. Учебник. М.: Академия, 2018. 352 с.
5. Малюк А. А. Информационная безопасность: концептуальные и методологические основы. Учебное пособие. М.: Горячая линия - Телеком, 2018. 592 с.
6. Баранов В. В., Василенко В. А., Конявский В. А. Обеспечение информационной безопасности автоматизированных систем. М.: Гелиос АРВ, 2019. 320 с.
7. Горелик А. С., Зайцев С. А., Радин В. И. Защита информации в компьютерных системах. М.: Гелиос АРВ, 2020. 256 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Официальные документы ФСТЭК России по вопросам безопасности информации.
2. Стандарты ISO/IEC 27000.
3. Специализированная литература по криптографии.
4. Руководства по настройке и администрированию систем защиты информации (Firewall, IDS/IPS).
5. Книги по расследованию компьютерных инцидентов и цифровой криминалистике.
6. Научные статьи в области информационной безопасности.
7. Материалы конференций по информационной безопасности.

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. Сайт OWASP: https://owasp.org/
4. Ресурсы по информационной безопасности от Microsoft: https://learn.microsoft.com/ru-ru/security/
5. Сайт 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 «Информационная безопасность автоматизированных систем» 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 автоматизированных систем» 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 автоматизированных систем» 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.