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

Проектирование систем защиты информации

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 Проектирование систем защиты информации 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 «Проектирование систем защиты информации»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Проектирование систем защиты информации" является формирование у студентов теоретических знаний и практических навыков в области проектирования и реализации эффективных систем защиты информации. Дисциплина направлена на обучение методам анализа угроз, выбора адекватных средств защиты и разработки проектной документации для информационных систем различного масштаба. В результате изучения дисциплины студенты должны уметь разрабатывать проекты систем защиты информации, соответствующие требованиям безопасности и актуальным стандартам.

1.2 Задачи изучения дисциплины {Изучение основных принципов и концепций защиты информации.} {Овладение методами анализа рисков и угроз информационной безопасности.} {Ознакомление с различными типами средств защиты информации (СЗИ) и их применением.} {Формирование навыков разработки проектной документации для систем защиты информации.} {Изучение нормативных правовых актов и стандартов в области информационной безопасности.}

1.3 В результате изучения дисциплины «Проектирование систем защиты информации» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Индикаторы достижения компетенции	Вид оценочного знания
УК-3.	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	"ИУК-3.1 Определяет свою роль в команде. ИУК-3.2 Учитывает особенности поведения и интересы других участников. ИУК-3.3 Осуществляет обмен информацией и опытом. ИУК-3.4 Соблюдает нормы	

		внутригруппового взаимодействия и несёт ответственность за результат."	
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.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Проектирование систем защиты информации»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.ДВ.01.01).** 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
-	—	—	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 «Проектирование систем защиты информации» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 162 часа, из которых: лекции – 32 часов, практические занятия – 14 часов, лабораторные работы 0 часов, иная контактная работа – 32 часа, самостоятельная работа – 98. Всего часов аудиторной нагрузки – 64 часа.

По итогам 7 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в проектирование систем защиты информации. Основные понятия и определения

Обзор дисциплины. Цели и задачи проектирования СЗИ. Актуальность информационной безопасности. Классификация угроз информационной безопасности.

Лекция 2 Анализ рисков информационной безопасности

Методы анализа рисков (ISO 27005, OCTAVE). Оценка вероятности возникновения угроз и ущерба от них. Выбор мер по снижению рисков.

Лекция 3 Нормативно-правовое регулирование в области информационной безопасности

Законодательство РФ в области ИБ. Стандарты и нормативные документы (ФЗ-152, ГОСТы). Международные стандарты (ISO 27001).

Лекция 4 Технологии защиты информации. Криптографические методы защиты

Криптографические алгоритмы (симметричные, асимметричные). Электронная подпись. Хеширование. Сертификаты.

Лекция 5 Технологии защиты информации. Средства защиты информации

Межсетевые экраны. Системы обнаружения и предотвращения вторжений (IDS/IPS). Антивирусное ПО. Системы резервного копирования.

Лекция 6 Защита сетевой инфраструктуры

Безопасность беспроводных сетей. VPN. Защита от DDoS-атак. Мониторинг сетевой активности.

Лекция 7 Защита баз данных

Принципы защиты баз данных. Методы аутентификации и авторизации. Контроль доступа. Аудит событий.

Лекция 8 Разработка проектной документации по защите информации

Этапы разработки проекта СЗИ. Требования к проектной документации. Оформление отчетов.

Лекция 9 Современные тенденции в области защиты информации. Обзор

Искусственный интеллект в ИБ. Облачные технологии и ИБ. Управление уязвимостями. Кибербезопасность.

Лекция 10 Анализ защищенности корпоративных сетей. Средства защиты

Обзор современного инструментария и методик, применяемых для анализа защищенности корпоративных сетей. Обзор основных классов средств защиты

Лекция 11 Управление информационной безопасностью в организации

Формирование политики безопасности. Организационные меры по обеспечению ИБ. Управление инцидентами.

Лекция 12 Обеспечение безопасности при работе с облачными технологиями

Риски безопасности в облачных средах. Практические рекомендации по обеспечению безопасности облачных сервисов.

Лекция 13 Безопасность мобильных устройств

Угрозы безопасности мобильных устройств. Рекомендации по защите мобильных устройств. Реализация безопасности мобильных устройств

Лекция 14 Защита информации в условиях пандемии

Обзор угроз и уязвимостей, связанных с удаленной работой и использованием различных онлайн-сервисов.

Лекция 15 Аудит информационной безопасности

Виды аудита ИБ. Методы и инструменты аудита. Составление отчетов по результатам аудита.

Лекция 16 Практические аспекты обеспечения информационной безопасности

Обзор подходов к управлению рисками информационной безопасности. Рекомендации по созданию и внедрению эффективной системы ИБ

Структура и содержание практической части курса

Практическое занятие 1 Анализ угроз и уязвимостей информационной системы (Практика)

Практическое применение методов анализа угроз и уязвимостей. Использование инструментов сканирования.

Практическое занятие 2 Разработка модели угроз (Практика)

Практическое применение различных методик моделирования угроз. Построение модели угроз для конкретной информационной системы

Практическое занятие 3 Применение криптографических методов защиты (Практика)

Настройка и использование криптографических алгоритмов (шифрование, электронная подпись).

Практическое занятие 4 Настройка межсетевых экранов (Практика)

Практическое конфигурирование межсетевых экранов. Создание правил фильтрации трафика.

Практическое занятие 5 Установка и настройка системы обнаружения вторжений (IDS) (Практика)

Настройка и использование IDS. Анализ журналов событий. Реагирование на инциденты.

Практическое занятие 6 Развертывание и настройка VPN (Практика)

Настройка VPN-сервера и клиентов. Обеспечение безопасности VPN-соединений.

Практическое занятие 7 Защита баз данных (Практика)

Практическое применение мер защиты баз данных. Настройка ролей и привилегий. Аудит событий.

Практическое занятие 8 Разработка проектной документации СЗИ (Практика)

Составление технического задания. Разработка схемы защиты. Написание отчета по результатам анализа рисков.

Структура и содержание КСР

КСР 1 Разработка ТЗ на систему защиты информации для предприятия малого бизнеса

Разработка технического задания, выбор СЗИ, обоснование решения.

КСР 2 Разработка схемы защиты информационной системы банка

Разработка схемы защиты с учетом специфики банковской деятельности. Анализ рисков.

КСР 3 Анализ уязвимостей веб-приложения

Практическое применение методик и инструментов для выявления уязвимостей в веб-приложениях.

КСР 4 Разработка плана реагирования на инциденты информационной безопасности

Составление плана реагирования на различные типы инцидентов. Определение ролей и обязанностей.

КСР 5 Разработка политики информационной безопасности

Создание политики информационной безопасности для организации. Определение основных разделов.

КСР 6 Анализ соответствия требованиям законодательства по защите персональных данных

Анализ соответствия требованиям ФЗ-152. Разработка рекомендаций.

КСР 7 Разработка стратегии защиты от DDoS-атак

Разработка плана защиты от DDoS-атак для конкретной организации. Выбор средств защиты.

КСР 8 Разработка рекомендаций по улучшению информационной безопасности компании

Подготовка отчета с рекомендациями по улучшению ИБ на основе проведенного анализа. Оценка экономической эффективности предлагаемых мер.

Структура и содержание СРС

СРС 1 Подготовка к лекциям

Изучение теоретического материала, подготовка к контрольным точкам и самостоятельным работам.

СРС 2 Подготовка к практическим занятиям

Решение задач, подготовка к выполнению практических заданий, изучение дополнительных материалов.

СРС 3 Подготовка к лабораторным работам

Выполнение лабораторных работ, изучение документации к ПО, подготовка отчетов.

СРС 4 Работа над рефератом (по выбору)

Подготовка реферата по выбранной теме, изучение дополнительной литературы, анализ актуальных проблем.

СРС 5 Подготовка к контрольной работе

Повторение изученного материала, решение задач, подготовка к контрольной работе.

СРС 6 Изучение дополнительных материалов по отдельным темам

Работа с дополнительной литературой, анализ статей, подготовка презентаций.

СРС 7 Подготовка к экзамену

Систематизация изученного материала, повторение основных понятий, подготовка к ответам на вопросы.

СРС 8 Самостоятельное изучение материалов по теме: "Применение искусственного интеллекта в защите информации"

Изучение современных подходов к применению искусственного интеллекта в области информационной безопасности, включая анализ уязвимостей, обнаружение аномалий и автоматизацию реагирования на инциденты.

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 проектирование систем защиты информации. Основные по-нятия и определения	2						5	12,5
	Анализ угроз и уязвимостей информационной системы		2			3		4	
2	Анализ рисков информационной безопасности	2						7	12,5
	Разработка ТЗ на систему защиты информации для предприятия малого бизнеса			2					
3	Нормативно-правовое регулирование в области информационной без-опасности	2						6	12,5
	Разработка модели угроз		2			3		7	
4	Технологии защиты информации. Криптографические методы защиты	2						5	12,5
	Разработка схемы защиты информационной системы банка			2					
5	Технологии защиты информации. Средства защиты информации	2						3	12,5
	Применение криптографических методов защиты		2			4		2	
6	Защита сетевой инфраструктуры	2						1	12,5

	Анализ уязвимостей веб-приложения			2					
7	Защита баз данных	2						5	12,5
	Настройка межсетевых экранов		2			3		2	
8	Разработка проектной документации по защите информации	2						7	12,5
	Разработка плана реагирования на инциденты информационной без-опасности			2					
9	Современные тенденции в области защиты информации. Обзор	2						5	12,5
	Установка и настройка системы обнаружения вторжений (IDS)		2			4		4	
10	Анализ защищенности корпоративных сетей. Средства защиты	2						6	12,5
	Разработка политики информационной безопасности			2					
11	Управление информационной безопасностью в организации	2						4	12,5
	Развертывание и настройка VPN		2			3		7	
12	Обеспечение безопасности при работе с облачными технологиями	2						5	12,5
	Анализ соответствия требованиям законодательства по защите персо-нальных данных			2					
13	Безопасность мобильных устройств	2						1	12,5
	Защита баз данных		2			4		2	
14	Защита информации в условиях пандемии	2						3	12,5
	Разработка стратегии защиты от DDoS-атак			2					
15	Аудит информационной безопасности	2						2	12,5
	Разработка проектной документации СЗИ		2			4		4	
16	Практические аспекты обеспечения информационной безопасности	2						6	12,5
	Разработка рекомендаций по улучшению информационной безопасности компании			2					
Итого:		**32**	**16**	**16**	**0**	**28**	**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 **4 -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 4 -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 проектирования систем защиты информации	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	Нормативные требования и стандарты в области защиты информации	Вопросы 5–8. Презентация методов	Выступление
3	6	Этапы проектирования системы защиты информации	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Анализ объекта защиты и его характеристик	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Формирование модели угроз и нарушителя	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Выбор принципов и методов защиты информации	Выполнение задания 2	Защита работы
7	6	Проектирование подсистемы организационной защиты	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Проектирование подсистемы технической защиты	Вопросы 16–17. Выполнение задания 4	Защита работы
9	4	Проектирование подсистемы программной защиты	Выполнение задания 5	Защита работы
10	4	Проектирование подсистемы криптографической защиты	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Интеграция подсистем в единую систему защиты	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы

12	4	Разработка проектной документации	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы
13	4	Оценка эффективности проектных решений	Вопросы 32–37. Презентация	Опрос, выступление
14	4	Тестирование и аттестация системы защиты информации	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Сопровождение и модернизация системы защиты	Вопросы 41–44. Выполнение задания 9	Защита работы
16	4	Комплексный проект системы защиты информации	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. Основы информационной безопасности. Учебное пособие. – М.: Изд-во Фолиант, 2020. – 512 с.
2. Каратаев А.В. Защита информации в компьютерных системах. Учебное пособие. – СПб.: Изд-во СПбГЭТУ "ЛЭТИ", 2020. – 180 с.
3. Петров М.В. Информационная безопасность: Теория и практика. – М.: ДМК Пресс, 2019. – 480 с.
4. Хорошко А.В., Чечулин А.А. Защита информации в информационных системах. Учебник. – М.: Гелиос АРВ, 2020. – 504 с.
5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы. – М.: Горячая линия – Телеком, 2018. – 640 с.
6. Щербаков А.Ю. Безопасность компьютерных сетей. – СПб.: Питер, 2019. – 384 с.
7. Баранова Н.В., Иванов Д.В. Безопасность информационных технологий: учебник для вузов. — М.: Юрайт, 2020. — 254 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Кузин А.В. Информационная безопасность. – М.: Академия, 2017. – 368 с.
2. Лобанов А.В. Защита информации. – М.: ДМК Пресс, 2018. – 320 с.
3. Федотов А.П. Основы информационной безопасности. – М.: Юрайт, 2017. – 287 с.
4. Довнар А.Г., Семенков О.И., Шестаков А.И. Защита информации в автоматизированных системах. – Мн.: БГУИР, 2018. – 262 с.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2015. – 552 с.
6. Андреев А.А. Защита информации. Практикум. – М.: Гелиос АРВ, 2016. – 160 с.
7. Горелик А.С. Компьютерная безопасность. – СПб.: Питер, 2019. – 432 с.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
2. ГОСТ Р 50.1.056-2005. Информационные технологии. Безопасность автоматизированных систем. Общие положения.
3. СТО БР ИББС-1.0-2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.
4. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
5. Стандарты ISO/IEC 27000.

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 «Проектирование систем защиты информации» 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 «Проектирование систем защиты информации» 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 «Проектирование систем защиты информации» 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.