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

Методы и средства криптографической 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 Методы и средства криптографической 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 «Методы и средства криптографической защиты информации»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Методы и средства криптографической защиты информации" является формирование у студентов теоретических знаний и практических навыков в области защиты информации с использованием криптографических методов. Дисциплина направлена на изучение принципов построения и функционирования криптографических алгоритмов, а также на овладение методами и средствами защиты информации от несанкционированного доступа. В результате изучения дисциплины студенты будут способны разрабатывать и применять криптографические решения для обеспечения безопасности информационных систем.

1.2 Задачи изучения дисциплины Изучение основных понятий и терминологии криптографии. Освоение принципов работы симметричных и асимметричных криптографических алгоритмов. Рассмотрение методов хэширования и цифровой подписи. Изучение протоколов криптографической защиты информации. Формирование навыков анализа и выбора криптографических средств для конкретных задач.

1.3 В результате изучения дисциплины «Методы и средства криптографической защиты информации» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Индикаторы достижения компетенции	Вид оценочного знания
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	"ИУК-1.1 Анализирует задачу, выделяя её базовые составляющие. ИУК-1.2 Демонстрирует знание особенностей системного и критического мышления и готовность к	

		нему. ИУК-1.3 Аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение. ИУК-1.4 Предлагает возможные варианты решения задачи, оценивая их достоинства и недостатки."	
ОПК-2.	Использование современных ИТ	"ИОПК-2.1 Выбирает ИТ и ПО. ИОПК-2.2 Применяет ИТ при решении задач."	
ОПК-9.	Профессиональные коммуникации	"ИОПК-9.1 Использует инструменты коммуникации. ИОПК-9.2 Взаимодействует с заказчиком. ИОПК-9.3 Участвует в презентациях и переговорах."	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Методы и средства криптографической защиты информации»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.О.33).** 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 «Методы и средства криптографической защиты информации» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 108 часа, из которых: лекции – 16 часов, практические занятия – 16 часов, лабораторные работы 16 часов, иная контактная работа – 32 часа, самостоятельная работа – 44. Всего часов аудиторной нагрузки – 64 часа.

По итогам 8 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в криптографию. Основные понятия и определения. История криптографии

Рассмотрение основных терминов и понятий криптографии. Обзор истории развития криптографии.

Лекция 2 Математические основы криптографии. Теория чисел, модульная арифметика.

Изучение математических основ криптографии, включая теорию чисел и модульную арифметику.

Лекция 3 Симметричное шифрование. Классические шифры (замены, перестановки).

Рассмотрение принципов симметричного шифрования и классических шифров.

Лекция 4 Современные симметричные шифры: DES, AES, блочные и поточные шифры.

Изучение современных симметричных шифров, включая DES, AES, блочные и поточные шифры.

Лекция 5 Асимметричное шифрование. RSA, Диффи-Хеллман, ECC.

Рассмотрение принципов асимметричного шифрования и алгоритмов RSA, Диффи-Хеллмана, ECC.

Лекция 6 Функции хэширования. Свойства, SHA-1, SHA-2, MD5.

Изучение функций хэширования, их свойств и популярных алгоритмов, таких как SHA-1, SHA-2, MD5.

Лекция 7 Цифровые подписи. Принципы работы, алгоритмы (RSA, DSA).

Рассмотрение принципов работы цифровых подписей и алгоритмов RSA, DSA.

Лекция 8 Криптографические протоколы: TLS/SSL, SSH, VPN.

Изучение криптографических протоколов, таких как TLS/SSL, SSH, VPN.

Структура и содержание практической части курса

Практическое занятие 1 Анализ классических шифров. Взлом шифра Цезаря. (Практика)

Практическое применение знаний по анализу и взлому классических шифров.

Практическое занятие 2 Реализация шифра простой замены. (Практика)

Разработка и реализация шифра простой замены.

Практическое занятие 3 Реализация блочного шифра (например, DES) (упрощенная версия). (Практика)

Практическая работа по реализации упрощенной версии блочного шифра.

Практическое занятие 4 Практическое использование AES. Шифрование и расшифрование файлов. (Практика)

Практическое использование алгоритма AES для шифрования и расшифрования файлов.

Практическое занятие 5 Реализация алгоритма RSA. Генерация ключей, шифрование и расшифрование. (Практика)

Практическая работа по генерации ключей, шифрованию и расшифрованию с использованием RSA.

Практическое занятие 6 Вычисление хэшей различных данных. Сравнение результатов. (Практика)

Практическое вычисление хэшей для различных данных и сравнение результатов.

Практическое занятие 7 Создание и проверка цифровой подписи. (Практика)

Практическая работа по созданию и проверке цифровой подписи.

Практическое занятие 8 Настройка и использование VPN. (Практика)

Практическое использование VPN для защиты трафика.

Структура и содержание лабораторной части курса

Лабораторная работа 1 Изучение и настройка криптографических библиотек (OpenSSL).

Изучение и настройка криптографических библиотек, таких как OpenSSL.

Лабораторная работа 2 Реализация симметричного шифрования (AES) на языке программирования.

Практическая работа по реализации алгоритма AES на языке программирования.

Лабораторная работа 3 Реализация асимметричного шифрования (RSA) на языке программирования.

Практическая работа по реализации алгоритма RSA на языке программирования.

Лабораторная работа 4 Проведение анализа уязвимостей шифров.

Анализ уязвимостей шифров.

Лабораторная работа 5 Практическое применение хэширования для защиты данных.

Практическая работа по использованию хэширования для защиты данных.

Лабораторная работа 6 Разработка и тестирование протокола аутентификации.

Разработка и тестирование протокола аутентификации.

Лабораторная работа 7 Анализ и применение криптографических протоколов (TLS/SSL).

Анализ и применение криптографических протоколов, таких как TLS/SSL.

Лабораторная работа 8 Разработка безопасного чат-приложения с использованием криптографии.

Разработка безопасного чат-приложения с использованием криптографии.

Структура и содержание КСР

КСР 1 Разработка отчета по анализу выбранного криптографического алгоритма.

Студенты разрабатывают отчет по анализу выбранного криптографического алгоритма.

КСР 2 Разработка и представление презентации по теме «Криптография и облачные вычисления».

Подготовка презентации по теме, связанной с криптографией и облачными вычислениями.

КСР 3 Анализ уязвимостей в конкретном криптографическом протоколе (TLS/SSL).

Анализ уязвимостей в конкретном криптографическом протоколе.

КСР 4 Разработка рекомендаций по повышению безопасности веб-приложения.

Разработка рекомендаций по повышению безопасности веб-приложения с учетом криптографических методов.

КСР 5 Сравнительный анализ симметричных криптоалгоритмов

Студенты выполняют сравнительный анализ различных симметричных криптоалгоритмов

КСР 6 Обзор и анализ современных криптографических атак

Обзор и анализ современных криптографических атак, поиск новых уязвимостей

КСР 7 Разработка сценария применения криптографии в IoT

Разработка сценария применения криптографии в устройствах IoT

КСР 8 Оценка влияния квантовых вычислений на криптографию

Оценка угроз, вызванных развитием квантовых вычислений для классических криптографических систем

Структура и содержание СРС

СРС 1 Изучение дополнительных материалов по симметричному шифрованию.

Самостоятельное изучение дополнительных материалов по симметричному шифрованию.

СРС 2 Изучение дополнительных материалов по асимметричному шифрованию.

Самостоятельное изучение дополнительных материалов по асимметричному шифрованию.

СРС 3 Подготовка к практическим занятиям по реализации криптографических алгоритмов.

Подготовка к практическим занятиям.

СРС 4 Изучение криптографических протоколов и их применение.

Самостоятельное изучение криптографических протоколов.

СРС 5 Подготовка к текущему контролю.

Подготовка к промежуточной аттестации.

СРС 6 Поиск и анализ статей по современным криптографическим атакам.

Самостоятельный поиск и анализ статей.

СРС 7 Подготовка презентации по теме криптографической защиты информации.

Подготовка презентации.

СРС 8 Изучение дополнительной литературы и ресурсов по теме.

Изучение дополнительной литературы и ресурсов по теме.

СРС 9 Исследование перспективных направлений в криптографии

Самостоятельное изучение новых направлений в криптографии

СРС 10 Анализ новых криптографических алгоритмов

Самостоятельный анализ новых криптографических алгоритмов и их свойств

СРС 11 Подготовка к участию в студенческих конференциях по информационной безопасности

Подготовка докладов для участия в студенческих конференциях

СРС 12 Создание криптографических инструментов для защиты данных

Разработка собственных криптографических инструментов

СРС 13 Изучение принципов работы квантовой криптографии

Самостоятельное изучение основ квантовой криптографии

СРС 14 Практическое применение криптографии в проектах IoT

Реализация криптографической защиты в проектах IoT

СРС 15 Разработка и тестирование криптографических модулей

Создание и тестирование криптографических модулей для различных систем

СРС 16 Изучение этических аспектов криптографии

Самостоятельное изучение этических аспектов криптографии

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 криптографию. Основные понятия и определения. История криптографии	2				4		1,5	12,5
	Анализ классических шифров. Взлом шифра Цезаря.		2			4		2,3	
2	Изучение и настройка криптографических библиотек (OpenSSL).				2	4		6,5	12,5
	Разработка отчета по анализу выбранного криптографического алгоритма.			2					
3	Математические основы криптографии. Теория чисел, модульная ариф-метика.	2				4		7,2	12,5
	Реализация шифра простой замены.		2			4		2,3	
4	Реализация симметричного шифрования (AES) на языке программиро-вания.				2	4		2,1	12,5
	Разработка и представление презентации по теме «Криптография и об-лачные вычисления».			2					
5	Симметричное шифрование. Классические шифры (замены, перестановки).	2				4		6,2	12,5
	Реализация блочного шифра (например, DES) (упрощенная версия).		2			4		4,3	
6	Реализация асимметричного шифрования (RSA) на языке программирования.				2			5,1,3,5	12,5
	Анализ уязвимостей в конкретном криптографическом протоколе (TLS/SSL).			2					
7	Современные симметричные шифры: DES, AES, блочные и поточные шифры.	2				4		5,6	12,5

	Практическое использование AES. Шифрование и расшифрование файлов.		2			4		2,3	
8	Проведение анализа уязвимостей шифров.				2	4		6,5	12,5
	Разработка рекомендаций по повышению безопасности веб-приложения.			2					
9	Асимметричное шифрование. RSA, Диффи-Хеллман, ECC.	2				4		7,2	12,5
	Реализация алгоритма RSA. Генерация ключей, шифрование и расшифрование.		2			4		2,3	
10	Практическое применение хэширования для защиты данных.				2	4		2,1	12,5
	Сравнительный анализ симметричных криптоалгоритмов			2					
11	Функции хэширования. Свойства, SHA-1, SHA-2, MD5.	2				4		6,2	12,5
	Вычисление хэшей различных данных. Сравнение результатов.		2			4		2,3	
12	Разработка и тестирование протокола аутентификации.				2			6,5	12,5
	Обзор и анализ современных криптографических атак			2					
13	Цифровые подписи. Принципы работы, алгоритмы (RSA, DSA).	2				4		7,2	12,5
	Создание и проверка цифровой подписи.		2			4		2,3	
14	Анализ и применение криптографических протоколов (TLS/SSL).				2	4		2,1	12,5
	Разработка сценария применения криптографии в IoT			2					
15	Криптографические протоколы: TLS/SSL, SSH, VPN.	2						6,2	12,5
	Настройка и использование VPN.		2			4		4,3	
16	Разработка безопасного чат-приложения с использованием криптографии.				2				12,5
	Оценка влияния квантовых вычислений на криптографию			2				12,5	
Итог		16	16	16	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 **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	Основные понятия и задачи криптографической защиты информации	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	История и классификация криптографических методов	Вопросы 5–8. Презентация методов	Выступление
3	6	Симметричные криптографические алгоритмы	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Асимметричные криптографические алгоритмы	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Хэш-функции и коды аутентичности сообщений	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Электронная цифровая подпись	Выполнение задания 2	Защита работы
7	6	Управление криптографическими ключами	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Криптографические протоколы	Вопросы 16–17. Выполнение задания 4	Защита работы

9	4	Средства криптографической защиты информации	Выполнение задания 5	Защита работы
10	4	Криптография в компьютерных сетях (SSL/TLS, VPN)	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Аппаратные криптографические средства	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы
12	4	Сертификация и стандарты в области криптографии	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы
13	4	Постквантовая криптография	Вопросы 32–37. Презентация	Опрос, выступление
14	4	Криптоанализ и основные атаки	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Реализация криптографических алгоритмов в ПО	Вопросы 41–44. Выполнение задания 9	Защита работы
16	4	Комплексная система криптографической 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. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф, 2018. 816 стр.
2. Васильев А.Н. Криптография: учебник для вузов. Издательство Юрайт, 2020. 368 стр.
3. Молдовян Н.А. Криптография. Конспект лекций. СПбГУ ИТМО, 2019. 120 стр.
4. Аверченков В.И. Защита информации в компьютерных системах. Инфра-М, 2019. 288 стр.
5. Кузнецов А.П. Криптографические методы защиты информации. Учебное пособие. МГТУ им. Н.Э. Баумана, 2020. 156 стр.
6. Калашников О.В. Основы информационной безопасности. Криптографические методы защиты. СПб: Лань, 2019. 196 стр.
7. Горев А.Ю. Криптографическая защита информации. Учебное пособие. СПб: Питер, 2018. 352 стр.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Тимошин А.Н. Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.

2. Данилин А.В., Минаев В.А. Криптография в примерах. М.: СОЛОН-Пресс, 2008. 200 с.
3. Федотов А.М. Методы и средства защиты информации. Учебное пособие. СПб: Питер, 2012. 400 с.
4. Лабораторный практикум по криптографии. Под ред. Салова А.С. М.: МИФИ, 2015.
5. Андреев С.П. Информационная безопасность. Учебное пособие. М.: Юрайт, 2017.
6. Лисицин Д.А. Криптографические алгоритмы и протоколы. Учебное пособие. СПб: БХВ-Петербург, 2016.
7. Богданов В.В. Криптографическая защита информации. Учебник. М.: ДМК Пресс, 2014.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. Сайт компании Microsoft: https://learn.microsoft.com/en-us/security/security-intelligence
2. Сайт OpenSSL: https://www.openssl.org/
3. RFC (Request for Comments): https://www.rfc-editor.org/
4. Портал информационной безопасности: https://www.securitylab.ru/
5. Центр компетенций по информационной безопасности: https://www.cisco.com/c/ru_ru/solutions/security/index.html

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 «Методы и средства криптографической 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 «Методы и средства криптографической 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 «Методы и средства криптографической 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.