

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.03
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы защиты информации
(наименование дисциплины)

по направлению подготовки

09.03.03 Прикладная информатика

направленность (профиль)

Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 53Е

Распределение часов дисциплины по семестрам

Семестр	6	Итого
Форма контроля	Экзамен	
Вид занятий		
Лекции	32	32
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,35	0,35
Контактная работа	64,35	64,35
Самостоятельная работа	80	80
Контроль	35,65	35,65
Итого	180	180

Рабочую программу составил(и):

Доцент ИИиЭБ, к.э.н., доцент, Фрезе Т.Ю.

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2030

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 1 от 01.09.2025).

1. Цель освоения дисциплины

Цель освоения дисциплины – изучить основы криптографии и криптографические методы защиты информации.

Дисциплина «Криптографические методы и средства защиты информации» содержит основные положения криптографии, знакомит с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью. Объясняется математическая теория, лежащая в основе криптографии. Рассматриваются вопросы реализации алгоритмов шифрования и криптоанализа. Изучаются вопросы правовой регуляtorики и применение средств СКЗИ.

Студент получает практические навыки в использовании средств криптографической защиты.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина: Основы дискретной математики и логики.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее: Техническая защита информации

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-11 Способен противодействовать угрозам безопасности информации с использованием средств защиты информации операционных систем и сетей, включая средства криптографической защиты информации	ПК-11.1 Использует знания основ современных криптографических алгоритмов и протоколы для обеспечения информационной безопасности	Знать: - основные понятия криптографии и криптографические методы защиты информации; - основные типы средств криптографической защиты информации и предъявляемые к ним требования; - основные криптографические алгоритмы и механизмы, определяемые национальными стандартами и рекомендациями Российской Федерации, и стандартами международной организации по стандартизации; - основные методы и средства криптографического анализа; - простейшие методы анализа криптографических алгоритмов на примере шифров замены и перестановки;

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		<ul style="list-style-type: none"> - об основных этапах исторического развития криптографии; - типовые поточные и блочные шифры
		Уметь: <ul style="list-style-type: none"> - применять математические модели для оценки стойкости средств криптографической защиты информации
		Владеть: <ul style="list-style-type: none"> - навыками работы с программными и аппаратными средствами защиты информации в компьютерных системах;
	ПК-11.2 Умеет применять криптографические алгоритмы и протоколы для решения задач обеспечения аутентификации и защиты информации в информационных системах	Знать: <ul style="list-style-type: none"> - требования к шифрам и их основные характеристики; - требования к эксплуатационным качествам шифров.
		Уметь: <ul style="list-style-type: none"> - корректно применять необходимые методы криптографической защиты информации в автоматизированных системах
		Владеть: <ul style="list-style-type: none"> - осуществлять обоснованный выбор и использовать средства криптографической защиты информации при решении задач профессиональной деятельности;
	ПК-11.3 Владеет навыками применения программных средств для выполнения криптографических преобразований	Знать: <ul style="list-style-type: none"> - средства криптографической защиты информации
		Уметь: <ul style="list-style-type: none"> - применять и настраивать средства криптографической защиты информации
		Владеть: <ul style="list-style-type: none"> - навыками применения программных средств для выполнения криптографических преобразований;

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
1. Введение. История и основные понятия криптографии.	Лек	Предмет и задачи криптографии. Этапы исторического развития: от античности до Второй мировой войны. Основные понятия: открытый/закрытый текст, ключ, шифр, криптоанализ, стойкость.	6	2	-	-	Банк тестовых заданий
2. Формальные модели шифров. Математические основы.	Лек	Модели Шеннона. Теория информации и энтропия. Совершенная секретность. Криптография и теория сложности вычислений.	6	2	-	-	Банк тестовых заданий
3. Свойства криптографических преобразований. Классификация криптоалгоритмов.	Лек	Детерминированность, стойкость, лавинный эффект, нелинейность. Криптографическая примитивная. Конфузия и диффузия.	6	2	-	-	Банк тестовых заданий
	Лек	Критерии стойкости (вычислительная, доказанная, практическая). Классы атак на криптосистемы. Обзор	6	2	-	-	Банк тестовых заданий

		классических шифров (подстановка, перестановка).					
4. Современные симметричные шифры. Блочные шифры.	Лек	Принципы построения блочных шифров. Сеть Фейстеля. Стандарты DES и 3DES. Анализ их уязвимостей.	6	2	-	-	Банк тестовых заданий
5. Современные симметричные шифры. Стандарт AES и российский стандарт ГОСТ 34.12-2018.	Лек	Структура Rijndael (AES). Особенности, раундовые преобразования. Отечественный блочный шифр "Кузнечик" (ГОСТ 34.12-2018)	6	2	-	-	Банк тестовых заданий
6. Поточные шифры. Гаммирование.	Лек	Принцип поточного шифрования. Синхронные и самосинхронизирующиеся потоки. Генераторы псевдослучайных последовательностей (RC4, отечественный ГОСТ 34.12-2018 "Магма" в режиме гаммирования).	6	2	-	-	Банк тестовых заданий
7. Основы асимметричной криптографии. Модель и теоретические основы.	Лек	7 Проблема распределения ключей. Идея Диффи-Хеллмана. Односторонние функции и функции с потайным ходом.	6	2	-	-	Банк тестовых заданий
8. Алгоритмы асимметричного шифрования. RSA.	Лек	Алгоритм RSA: генерация ключей, шифрование, расшифрование. Математическое обоснование. Примеры. Стойкость и атаки.	6	2	-	-	Банк тестовых заданий

9. Алгоритмы асимметричного шифрования на эллиптических кривых (ЭК). Отечественный стандарт.	Лек	Криптография на ЭК. Преимущества. Алгоритм обмена ключей и шифрования. Отечественный стандарт ГОСТ Р 34.10-2012 (использующий ЭК).	6	2	-	-	Банк тестовых заданий
10. Хэш-функции. Свойства и назначение.	Лек	Понятие хэш-функции. Требования: стойкость к прообразам и коллизиям. Итеративные конструкции (Меркла-Дамгарда). Обзор алгоритмов (SHA-2, SHA-3).	6	2	-	-	Банк тестовых заданий
11. Электронная подпись (ЭП). Принципы работы и стандарты.	Лек	Модель ЭП. Алгоритмы на основе RSA (RSASSA-PSS) и ЭК (ECDSA). Отечественный стандарт ГОСТ Р 34.10-2012 (ЭП на ЭК). Процедуры формирования и проверки. Сертификаты ключей (PKI).	6	2	-	-	Банк тестовых заданий
12. Криптографические протоколы	Лек	Понятие протокола. Протоколы аутентификации (на основе паролей, с нулевым разглашением). Протоколы распределения ключей (Диффи-Хеллман, STS).	6	2	-	-	Банк тестовых заданий
	Лек	Протоколы электронного голосования, слепой подписи, теневое тендера. Атаки на протоколы (атака "человек посередине", повтор передачи).	6	2	-	-	Банк тестовых заданий

13. Средства и методы КЗИ и их применение.	Лек	Аппаратные и программные СКЗИ. Средства защиты каналов связи (VPN, TLS). Средства защиты данных на носителях (шифрование дисков, контейнеры). Криптографические библиотеки.	6	2		-	Банк тестовых заданий
14. Нормативно-правовое регулирование КЗИ в РФ	Лек	Закон "О связи", "Об информации...", Постановления Правительства №№ 313, 1119. Требования ФСБ России (приказы ФСТЭК). Сертификация СКЗИ. Перспективы развития криптографии.	6	2		-	Банк тестовых заданий
	Пр	Практическая работа 1 Анализ классических шифров.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 2. Работа с формальными моделями. Расчет энтропии.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 3. Изучение свойств криптографических преобразований.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 4. Реализация базовых операций симметричного шифрования.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работ 5. Имитационная работа с алгоритмом DES/3DES.	6	2	-	-	Отчет по практическому занятию

	Пр	Практическая работа 6. Имитационная работа с алгоритмами AES и ГОСТ "Кузнечик".	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 7. Реализация поточного шифра на основе линейного регистра сдвига (ЛРС).	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работ 8. Расчеты в асимметричной криптографии. Алгоритм Диффи-Хеллмана.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 9. Практическая работа с алгоритмом RSA.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 10. Основы работы с эллиптическими кривыми в криптографии.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 11. Практикум по хэш-функциям.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 12. Работа с электронной подписью.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 13. Анализ криптографических протоколов.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 14. Проектирование схемы КЗИ для типовой информационной системы.	6	2	-	-	Отчет по практическому занятию

	Пр	Практическая работа 15. Обзор и сравнение современных СКЗИ.	6	2	-	-	Отчет по практическому занятию
	Пр	Практическая работа 16. Зачетное занятие.	6	2	-	-	Отчет по практическому занятию
	Ср	Самостоятельное изучение материала, не вошедшего в лекции	6	80	-	-	Банк тестовых заданий
	К	Контроль	6	35,65	-	-	Банк тестовых заданий
	ПА	Промежуточная аттестация	6	0,35	-	-	Банк тестовых заданий /Вопросы к экзамену
Итого:				180	-	-	

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
Формы и методы обучения		
Дистанционное обучение	Сетевая технология – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. CD-технология – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее.

Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-11	Отчеты по практическим занятиям №№1-16
		Вопросы к экзамену №№1-60
		Б

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Практическое задание

(наименование оценочного средства)

Практическая работа 1 Анализ классических шифров.
 Практическая работа 2. Работа с формальными моделями. Расчет энтропии.
 Практическая работа 3. Изучение свойств криптографических преобразований.
 Практическая работа 4. Реализация базовых операций симметричного шифрования.
 Практическая работ 5. Имитационная работа с алгоритмом DES/3DES.
 Практическая работа 6. Имитационная работа с алгоритмами AES и ГОСТ "Кузнечик".
 Практическая работа 7. Реализация поточного шифра на основе линейного регистра сдвига (LPC).
 Практическая работ 8. Расчеты в асимметричной криптографии. Алгоритм Диффи-Хеллмана.
 Практическая работа 9. Практическая работа с алгоритмом RSA.
 Практическая работа 10. Основы работы с эллиптическими кривыми в криптографии.
 Практическая работа 11. Практикум по хэш-функциям.
 Практическая работа 12. Работа с электронной подписью.
 Практическая работа 13. Анализ криптографических протоколов.
 Практическая работа 14. Проектирование схемы КЗИ для типовой информационной системы.
 Практическая работа 15. Обзор и сравнение современных СКЗИ.
 Практическая работа 16. Зачетное занятие.

Типовой(ые) пример(ы) задания(ий)

Пример фрагмента кода для частотного анализа на Python:

```
python
from collections import Counter

ciphertext = "Ц ФХУНРСО Й РХЛММСФУАЕЛ ЙМШВСФ..." # Ваш текст
# Убираем пробелы и приводим к верхнему регистру
```

```
text_for_analysis = ".join([ch.upper() for ch in ciphertext if ch.isalpha()])
```

```
letter_counts = Counter(text_for_analysis)
```

```
total_letters = len(text_for_analysis)
```

```
print("Частоты букв (в %):")
```

```
for letter, count in letter_counts.most_common():
```

```
    frequency = (count / total_letters) * 100
```

```
    print(f"{letter}: {count} ({frequency:.2f}%)")
```

Темы письменных работ

- 1) От скиталы до «Энигмы»: детальный разбор одного исторического шифра (например, шифр Виженера, «диск Джефферсона») с анализом его криптостойкости и роли в истории.
- 2) Вклад Алана Тьюринга и польских криптографов в криптоанализ «Энигмы»: изучение методов «Бомбы Тьюринга» и «циклометра».
- 3) Криптография в Древней Руси и в Российской Империи: исследование отечественных криптографических традиций (тайнопись, «цифирные азбуки»).

Краткое описание и регламент выполнения

1. Студенту выдается индивидуальный вариант, состоящий из двух зашифрованных текстов и ключевого слова.

Пример варианта:

Вариант № 5

Задача 1. Моноалфавитный шифр (Цезарь/Атбаш/Простая замена).

Шифртекст: "ЮЭЪС ХЦЙЮ БЯЦЙ, ЖЮЪС ХЦЙЮ ВСЭЦ!"

Известно, что использован русский алфавит (А-Я, без Ё).

Задача 2. Шифр Виженера.

Шифртекст: "ЛСРСРФИУ ТЙСФУВЩЗ ДЩЛЙОЩФТЙЙ, УГЙ ИУФВИПЩЗЙЬ НЩВМЙЬ ТЙИ В ФЙУФЧБИ."

Ключевое слово: "ЗАЩИТА".

Задача 3. Криптоанализ (Частотный анализ).

Шифртекст (предположительно, простая замена):

"Ц ФХУНРСО Й РХММСФУАЕЛ ЙМШВСФ Ц БНЯ ПЮАНР ЙНМХЛНМШУ ЖЕАЕИ, Й БСПНЯ ПЮАНР ЙКНМНЛЕММШУ ЖЕАЕИ."

2. Конкретные задачи для студента:

Для Задачи 1: Определить тип шифра (Цезарь или Атбаш) и расшифровать сообщение. Если это шифр Цезаря – найти ключ k.

Для Задачи 2: Используя известное ключевое слово "ЗАЩИТА", расшифровать сообщение, зашифрованное шифром Виженера. Составить таблицу/использовать алгоритм для ручного расчета.

Для Задачи 3: Провести частотный анализ приведенного шифртекста.

- Составить таблицу частот символов (отсортированную по убыванию).
- Сопоставить наиболее частые буквы шифртекста с наиболее частыми буквами русского языка («О», «Е», «А», «И»...).
- Сделать гипотезу о возможных заменах и, используя контекст (короткие слова, повторяющиеся сочетания), попытаться полностью восстановить открытый текст и таблицу замен (ключ).

4. Рекомендации по выполнению и необходимый инструментарий:

Ручной метод (обязательный для понимания):

Иметь под рукой алфавит (русский, 32 буквы).

Для Виженера: составить таблицу (квадрат) Виженера или использовать формулу:
 $P_i = (C_i - K_i + n) \bmod n$, где P – открытый текст, C – шифртекст, K – ключ, $n=32$.

Для частотного анализа: выписать шифртекст в столбик и посчитать каждую букву.

Программный метод (рекомендуется для проверки и ускорения):

Использовать Python с кодировкой cp1251 или utf-8.

Написать или использовать готовые скрипты для:

Перебора всех ключей шифра Цезаря (k от 1 до 31).

Реализации шифрования/дешифрования Атбаша.

Реализации шифрования/дешифрования Виженера.

Автоматического подсчета частот букв в тексте.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическая работа выполнена грамотно или имеет несущественные замечания, выполнен отчет по работе.

- оценка «не зачтено» выставляется студенту, если практическая работа не выполнена, имеет грубые ошибки, не подготовлен отчет.

7.2.2. Тестирование

Типовой пример тестового задания

Какой из перечисленных шифров является полиалфавитным, что делает его, при достаточной длине ключа, устойчивым к простому частотному анализу?

А) Шифр Виженера (Vigenère cipher).

Б) Шифр Цезаря (Caesar cipher).

В) Атбаш (Atbash cipher).

Г) Шифр простой замены (моноалфавитный шифр).

Критерии оценки:

Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 6

Вопросы к экзамену
1. Проследите эволюцию криптографии от моноалфавитных шифров до механических роторных систем («Энигма»). В чем принципиальное отличие в подходе к обеспечению стойкости у шифра Цезаря и у «Энигмы»?
2. Сформулируйте теорему К. Шеннона о совершенной секретности. Почему шифр Вернама (одноразовый блокнот) является единственной идеальной системой с практической точки зрения? Каков его главный недостаток?
3. Объясните, как понятия энтропии и избыточности языка из теории информации связаны с практикой криптоанализа (на примере частотного анализа).
4. Дайте определение стойкости криптографического алгоритма. Раскройте различия между теоретической (доказательной), вычислительной и практической стойкостью. Приведите примеры.

5. Опишите формальную модель шифра как преобразования. Что такое пространство ключей, открытых текстов и шифртекстов? Как атака с известным открытым текстом (Known-plaintext attack) использует эту модель?
6. Раскройте принципы конфузии и диффузии, введенные К. Шенноном. Как эти принципы реализованы в архитектуре современных блочных шифров (например, в AES и ГОСТ «Кузнечик»)?
7. Что такое лавинный эффект? Как он количественно оценивается и почему его наличие является критически важным для блочных шифров и хэш-функций?
8. Объясните, почему нелинейность преобразований (например, S-блоков) является ключевой для противодействия линейному криптоанализу. Как можно оценить нелинейность преобразования?
9. Дайте классификацию криптографических атак по объему доступной атакующему информации (ciphertext-only, known-plaintext и т.д.). Приведите пример реальной атаки для каждого класса.
10. Что такое криптографическая примитивная и криптографический протокол? Приведите примеры и объясните, почему корректность примитива не гарантирует безопасность протокола, его использующего.
11. Сравните архитектуры сети Фейстеля (DES) и SP-сети (AES). Каковы их структурные преимущества и недостатки с точки зрения стойкости, скорости и простоты реализации?
12. Детально опишите алгоритм DES. В чем заключались его исторические ограничения (длина ключа) и как они были преодолены в 3DES? Почему 3DES сегодня считается устаревшим?
13. Опишите структуру одного раунда алгоритма AES (Rijndael). Какие четыре преобразования (SubBytes, ShiftRows, MixColumns, AddRoundKey) выполняются и какую роль каждое из них играет в обеспечении конфузии и диффузии?
14. Дайте сравнительный анализ отечественных блочных шифров «Кузнечик» и «Магма» (ГОСТ Р 34.12-2018) по следующим параметрам: длина блока/ключа, структура (сеть Фейстеля/SP-сеть), производительность, рекомендуемые сферы применения.
15. Объясните различия между блочными и поточными шифрами. В каких практических сценариях предпочтительнее использование поточного шифрования? Приведите пример поточного шифра (например, RC4 или режим гаммирования ГОСТ).
16. Раскройте суть линейного и дифференциального криптоанализа. На каком математическом аппарате они основаны и против каких свойств шифра направлены?
17. Для чего нужны режимы шифрования (ECB, CBC, CFB, OFB, CTR, GCM)? Объясните, почему режим ECB небезопасен для шифрования структурированных данных, и сравните его с режимом CBC.
18. В чем заключается парадокс (проблема) распределения ключей в симметричной криптографии? Как асимметричная криптография решает эту проблему, вводя понятия открытого и закрытого ключа?
19. Объясните концепцию односторонней функции с потайным ходом (trapdoor function). Почему факторизация больших чисел (RSA) и задача дискретного логарифмирования (Диффи-Хеллман, DSA) считаются подходящими кандидатами для таких функций?
20. Детально опишите алгоритм RSA: генерацию ключевой пары, операции шифрования и расшифрования, подписи и проверки. Приведите небольшой числовой пример.
21. Опишите протокол обмена ключами Диффи-Хеллмана. Почему он безопасен при пассивном прослушивании канала? В чем заключается уязвимость к активной атаке «человек посередине» (MitM) и как она парируется?

22. В чем заключаются основные преимущества криптографии на эллиптических кривых (ЕСС) перед «классической» асимметричной криптографией (RSA, Диффи-Хеллман на конечных полях)? Приведите сравнение длин ключей при равной стойкости.
23. Сравните отечественные стандарты ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012. Каков ключевой алгоритмический переход между ними и какие новые возможности и требования он принес?
24. Что такое гибридная криптосистема? Объясните, как в ней сочетаются преимущества симметричного и асимметричного шифрования на примере протокола PGP или S/MIME.
25. Дайте определение криптографической хэш-функции. Перечислите и поясните основные требования к ней: стойкость к нахождению прообраза, второго прообраза и коллизий.
26. Опишите итеративную конструкцию Меркла-Дамгарда. Как она позволяет строить хэш-функции для сообщений произвольной длины на основе сжимающей функции? В чем ее потенциальная уязвимость к атаке расширения длины?
27. Проведите сравнительный анализ семейств хэш-функций SHA-2 и SHA-3 (Кессак). В чем принципиальное различие в их внутренней структуре (конструкция Меркла-Дамгарда vs губчатая конструкция) и почему было необходимо создание SHA-3?
28. Дайте определение электронной подписи (ЭП). Опишите ее жизненный цикл: формирование (подпись), проверка. Чем цифровая подпись принципиально отличается от простого шифрования на приватном ключе?
29. Сравните схемы ЭП на основе RSA (RSASSA-PSS) и эллиптических кривых (ECDSA, ГОСТ Р 34.10-2012). Какая из них эффективнее и почему?
30. Что такое атака «дня рождения» на хэш-функцию? Как вероятность успеха этой атаки влияет на выбор длины выхода хэш-функции для использования в схемах ЭП?
31. Что такое криптографический протокол? Приведите примеры протоколов для решения задач: аутентификации, распределения ключей, электронного голосования.
32. Опишите протокол Needham-Schroeder и его уязвимость, обнаруженную Деннингом и Сакко. Как эта уязвимость была исправлена в протоколе Kerberos?
33. Объясните концепцию доказательства с нулевым разглашением (Zero-Knowledge Proof, ZKP). Приведите классический пример «Пещера Али-Бабы» и объясните, как ZKP может быть использован для аутентификации без передачи пароля.
34. Что такое протокол SSL/TLS? Опишите его основные фазы (рукопожатие, обмен ключами, шифрование трафика). Какую роль в нем играют симметричные и асимметричные алгоритмы, хэш-функции?
35. Раскройте понятия Perfect Forward Secrecy (PFS) и сессионный ключ. Как протокол Диффи-Хеллмана в режиме Ephemeral (DHE, ECDHE) обеспечивает PFS в современных версиях TLS?
36. Что такое атака «человек посередине» (Man-in-the-Middle, MitM)? На каких этапах и в каких протоколах (например, базовый Диффи-Хеллман, SSL) она возможна? Какие механизмы (сертификаты, аутентификация ключей) ее предотвращают?
37. Дайте классификацию средств криптографической защиты информации (СКЗИ) по способу реализации (программные, аппаратные, программно-аппаратные). Приведите примеры и сравните их по быстродействию, защищенности и гибкости.
38. Что такое инфраструктура открытых ключей (PKI)? Опишите ее основные компоненты: удостоверяющий центр (УЦ), регистрационный центр (РА), репозиторий, список отозванных сертификатов (CRL). Как PKI решает проблему доверия к открытым ключам?

39. Объясните принципы работы VPN на основе IPsec. Какие два основных протокола (AH и ESP) входят в его состав и какие функции (аутентификация, шифрование, целостность) они обеспечивают?
40. Что такое криптографическая библиотека (на примере OpenSSL, CryptoAPI, КриптоПро CSP)? Какие задачи она решает и почему использование сертифицированных библиотек критически важно в разработке защищенных приложений?
41. Опишите методы криптографической защиты данных на уровне файловой системы (например, Encrypting File System – EFS в Windows, dm-crypt/LUKS в Linux) и на уровне носителей (полное шифрование диска).
42. Каковы специфические требования и ограничения к криптографии в сфере мобильных устройств и Интернета Вещей (IoT)? Что такое «легковесная криптография» (Lightweight Cryptography)?
43. Перечислите основные федеральные законы РФ, регулирующие вопросы применения криптографических средств. Кратко охарактеризуйте сферу действия каждого (напр., ФЗ-63 «Об ЭП», ФЗ-152 «О персональных данных»).
44. Что такое сертификация СКЗИ по требованиям ФСБ России? Какой документ (регулирующий акт) устанавливает порядок сертификации? Каковы цели и практические последствия получения сертификата для разработчика и пользователя?
45. Какие требования к использованию СКЗИ установлены Приказом ФСТЭК России № 1119 для информационных систем персональных данных (ИСПДн) различных уровней защищенности?
46. В чем заключается разница между квалифицированной и неквалифицированной электронной подписью согласно ФЗ-63? Каковы юридические последствия их использования?
47. Каковы правовые ограничения на ввоз, вывоз и использование криптографических средств на территории РФ? Какой государственный орган уполномочен выдавать соответствующие лицензии и разрешения?
48. Опишите роль ФАПСИ (ныне функции переданы ФСБ и СВР) и ФСБ России в становлении и регулировании отечественной криптографии.
49. Что такое квантовая криптография (например, протокол BB84)? На каких физических принципах она основана и какую проблему (не криптографическую, а физическую) она решает?
50. Объясните угрозу, которую представляют квантовые компьютеры для современных асимметричных алгоритмов (RSA, ECC, Диффи-Хеллман). Какие алгоритмы (постквантовой криптографии) рассматриваются в качестве устойчивой замены?
51. Что такое криптовалюты (например, Bitcoin) с криптографической точки зрения? Как в них используются хэш-функции (SHA-256), цифровые подписи (ECDSA) и доказательство выполненной работы (Proof-of-Work)?
52. Раскройте понятие гомоморфного шифрования. В чем его принципиальная особенность и какие новые возможности оно открывает для облачных вычислений и анализа данных?
53. Что такое криптография с сохранением формата (Format-Preserving Encryption, FPE)? Где она находит практическое применение (например, защита номеров карт в legacy-системах)?
54. Объясните концепцию мультиподписи (multisignature) и пороговой подписи (threshold signature). Как они используются для повышения безопасности управления корпоративными или фондовыми криптокошельками?
55. Что такое стеганография и чем она принципиально отличается от криптографии? Приведите примеры современных стеганографических методов.

56. Сравните отечественный криптографический стек (ГОСТы) и международный (NIST, IETF) по следующим критериям: открытость разработки, алгоритмическая основа, распространенность и поддержка, юридические ограничения.
57. Ситуационная задача: Вам необходимо обеспечить конфиденциальность, целостность и аутентичность документов, передаваемых между филиалами компании по открытым каналам связи. Предложите комплексное криптографическое решение, обосновав выбор конкретных алгоритмов (шифрование, ЭП, хэш) и протоколов.
58. Аналитическая задача: Объясните, почему даже абсолютно стойкий алгоритм шифрования может привести к уязвимой системе. Приведите примеры уязвимостей на уровне реализации (side-channel attacks) и на уровне протокола.
59. Историко-аналитический вопрос: Проанализируйте причины «криптографических войн» (Crypto Wars) между правительствами (желание контролировать) и академическим/техническим сообществом (желание иметь надежную защиту). Актуальны ли эти противоречия сегодня?
60. Итоговый мировоззренческий вопрос: Как развитие криптографии влияет на баланс между правом на приватность гражданина и задачами национальной безопасности государства? Приведите аргументы «за» и «против» наличия в алгоритмах бэкдоров (закладок) для государственных органов.

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
6	Экзамен	«отлично»	85-100 баллов
		«хорошо»	70-84 баллов
		«удовлетворительно»	55-69 баллов
		«неудовлетворительно»	0-54 баллов

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
6	Экзамен (по накопительному рейтингу)	«отлично»	85-100 баллов практические работы выполнены грамотно или имеют несущественные замечания; обучающийся владеет теоретическим материалом, отвечает на дополнительные вопросы
		«хорошо»	70-84 балла практические работы выполнены грамотно или имеют несущественные замечания; обучающийся владеет основным теоретическим материалом, отвечает на дополнительные вопросы, с неточностями
		«удовлетворительно»	55-69 баллов

			практические работы выполнены, имеют замечания; обучающийся владеет теоретическим материалом, не отвечает на дополнительные вопросы
		«неудовлетворительно»	0-54 баллов практические работы не выполнены или имеют существенные замечания; обучающийся не владеет теоретическим материалом, не отвечает на дополнительные вопросы или отвечает с грубыми ошибками

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин	Введение в теоретико-числовые методы криптографии : учебное пособие для вузов / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 3-е изд., стер. — Санкт-Петербург : Лань, 2025. — 396 с. — ISBN 978-5-507-51007-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/499406	учебное пособие	2025	Лань : электронно-библиотечная система
2	Г. В. Басалова	Основы криптографии : учебное пособие / Г. В. Басалова. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 282 с. — ISBN 978-5-4497-2420-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133959.html	учебное пособие	2024	Цифровой образовательный ресурс IPR SMART
3	С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова	Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР :	учебное пособие	2026	ЭБС «ZNANIUM»

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		ИНФРА-М, 2026. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6 . - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2241407			
4	Б. А. Фороузан	Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/146352.html	учебное пособие	2025	Цифровой образовательный ресурс IPR SMART
5	Кунин, Н. Т.	Криптографическая защита информации: Практикум : учебное пособие / Н. Т. Кунин. — Москва : РТУ МИРЭА, 2025. — 66 с. — ISBN 978-5-7339-2447-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/493382	учебное пособие	2025	Лань : электронно-библиотечная система

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
6	Ларионова, Е. И.	Криптографическая защита информации: практикум : учебное пособие / Е. И. Ларионова, Ю. Д. Фот, К. Р. Джукашев. — Оренбург : ОГУ, 2025. — 110 с. — ISBN 978-5-7410-3365-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/502777	учебное пособие	2025	Лань : электронно-библиотечная система

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Зырянова, Т. Ю.	Основы криптографии : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : Уральский государственный университет путей сообщения, 2023. — 83 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/149716.html	учебное пособие	2023	Цифровой образовательный ресурс IPR SMART
2	Александрова, Е. Б.	Криптографические методы защиты	учебное пособие	2023	Цифровой

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		информации. Элементы алгебраической геометрии : учебное пособие / Е. Б. Александрова, А. В. Ярмак. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2023. — 106 с. — ISBN 978-5-7422-8017-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/143094.html			образовательный ресурс IPR SMART

8.3. Перечень профессиональных баз данных и информационных справочных систем

№ пп	Наименование	Ссылка
1	Springer Nature (Полнотекстовая коллекция журналов)	https://www.springernature.com/gp/products
2	Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature)	https://link.springer.com/
3	«Кодекс»	https://kodeks.ru/
4	Техэксперт	https://cntd.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Консультант+	Договор №1522 от 25.12.2015, срок действия - бессрочно
2	Windows: WinPro 10 RUS Upgrd OLP NL Acadmс	договор № 757 от 04.07.2018, срок действия – бессрочно; контракт № 1653 от 14.12.2018, срок действия – бессрочно
3.	Office Standard: ⁴ Office Stdandard 2013 Russian OLP NL AcademicEdition	договор № 690 от 19.05.2015, срок действия – бессрочно
4	Криптографическая библиотека с открытым исходным кодом OpenSSL	https://www.openssl.org/
5	Программа для восстановления паролей Hashcat	https://hashcat.net/hashcat/
6	Свободное программное обеспечение для шифрования информации и создания электронных цифровых подписей GnuPG (GNU Privacy Guard, GPG)	https://www.gnupg.org/
7	встроенные утилиты Linux-систем	https://losst.pro/poleznye-konsolnye-utility-linux-v-2025
8	Интерпретируемый интерактивный объектно-ориентированный язык программирования Python	https://www.python.org/

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Помещение для самостоятельной работы обучающихся Д -409	Стол-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф
2	Помещение для самостоятельной работы обучающихся Г-401	Стол, стулья, компьютеры
3	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий, текущего контроля и промежуточной аттестации. Д-402	Стол учебные двухместные, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая), кафедра напольная
4	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий, текущего контроля и промежуточной аттестации. Д-413	Стол учебные двухместные, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая) , кафедра напольная
5	Лаборатория кибербезопасности. Лаборатория «Автоматизированные системы в защищенном исполнении». Лаборатория «Программно-аппаратные средства защиты информации». Лаборатория «Безопасность вычислительных сетей» Лаборатория «Техническая защита информации». Лаборатория «Сети и системы передачи информации». Учебная аудитория для проведения занятий лекционного типа.	Стол компьютерные, стол преподавательский, стулья, шкаф металлический, телевизор на передвижной тумбе, стойка телекоммуникационная, коммутатор оптический Qtech QSW-6910-26F, коммутатор Qtech QSW-4610-28T-AC, система хранения данных Русский щит Alpha DF5045, сервер Русский щит Gamma SX6302, ноутбук Digma Pro Sprint M DN15P3-8CXW02, осциллограф АКИП-4115/1А, анализатор низкочастотных сигналов

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	<p>Учебная аудитория для проведения занятий семинарского типа.</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций.</p> <p>Учебная аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования.</p> <p>Аудитория для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну</p> <p>Э-101в</p>	<p>СКМ-21, генератор сигналов АКПП-3407/1А, антенна дипольная активная Е-3000А1, антенна рамочная Н-30А1, акустический излучатель АС-1 Лайт Арт.001, рефлектометр ТОПАЗ-7317-ARX, измерительный пробник напряжения ШИП, анализатор спектра АКПП-4211/1, межсетевой экран ССПТ-2</p>