

Документ подписан простой электронной подписью	МИНОБРАЗОВАНИЯ РОССИИ	
Информация о владельце:	Федеральное государственное бюджетное образовательное	
ФИО: Таскаев Сергей Валерьевич	учреждение высшего образования	
Должность: Ректор	«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)	
Дата подписания: 02.10.2025	Рабочая программа дисциплины "Методы и средства криптографической защиты информации" по направлению	стр. 1
Уникальный программный ключ:	подготовки (специальности) 10.05.03 "Информационная безопасность автоматизированных систем"	
04c19ed8b09815b6cb77a486b9a8788b8522525	направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»	

Рабочая программа дисциплины (модуля)*

Методы и средства криптографической защиты информации

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль)

специализация N 4 "Безопасность автоматизированных систем критически важных объектов"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год набора 2025

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2025 г.



Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре ОПОП
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)
4. Объем дисциплины (модуля)
5. Структура и содержание дисциплины (модуля)
6. Фонд оценочных средств
 - 6.1. Перечень видов оценочных средств
 - 6.2. Типовые контрольные задания и иные материалы для текущей аттестации
 - 6.3. Типовые контрольные вопросы и задания для промежуточной аттестации
 - 6.4. Критерии оценивания
7. Учебно-методическое и информационное обеспечение дисциплины (модуля)
 - 7.1. Рекомендуемая литература
 - 7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"
 - 7.3. Перечень информационных технологий
8. Материально-техническое обеспечение дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Специальные условия освоения дисциплины обучающимися с инвалидностью и ограниченными возможностями здоровья



1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины являются:

- приобретение студентами умения самостоятельно изучать новые алгоритмы и методы в криптографии;
- приобретение студентами умения формулировать задачи по криптографическим методам защиты информации;
- приобретение студентами умения самостоятельно оценивать надежность криптографических методов.

Индикаторы достижения компетенций:

ОПК-10.1. Обладает базовыми знаниями в области криптографии.

ОПК-10.2. Демонстрирует умения использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП: Б1.О.21

2.1 Требования к предварительной подготовке обучающегося:

Дискретная математика

Математический анализ

Языки программирования

Алгебра

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Производственная практика (преддипломная практика)

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

Знать:

Для достижения индикатора ОПК-10.1: Знать базовые понятия в области криптографии (основные понятия и классификацию средств криптографической защиты информации, различия между стеганографией и криптографией, основные методы симметричного шифрования, классификацию методов симметричного шифрования, основные свойства симметричных криптосистем, понятие хеш-функции, основные понятия, основные алгоритмы электронной цифровой подписи, основные стандарты на алгоритмы цифровой подписи).

Уметь:

Для достижения индикатора ОПК-10.2: Уметь использовать средства криптографической защиты информации при решении задач профессиональной деятельности (использовать блочные алгоритмы шифрования для формирования хеш-функции, криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем, односторонние функции в целях построения криптосистем, криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем, алгоритмы генерации, хранения и распределения ключей, проектировать и использовать системы электронной цифровой подписи).

Владеть:

Для достижения индикатора ОПК-10.2: Владеть навыками использования средства криптографической защиты информации при решении задач профессиональной деятельности (навыками симметричного шифрования, формирования хеш-функций, по обеспечению безопасной работы в сети Интернет, применения асимметричных криптосистем, управления ключами в системах с открытым ключом, по созданию электронной цифровой подписи).

В результате освоения дисциплины обучающийся должен

3.1 Знать:

3.1.1 основные понятия и классификацию средств криптографической защиты информации;



Рабочая программа дисциплины "Методы и средства криптографической защиты информации" по направлению подготовки (специальности) 10.05.03 "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»		стр. 4
3.1.2	различия между стеганографией и криптографией;	
3.1.3	основные методы симметричного шифрования;	
3.1.4	классификацию методов симметричного шифрования;	
3.1.5	основные свойства симметричных криптосистем;	
3.1.6	понятие хеш-функции;	
3.1.7	основные понятия, основные алгоритмы электронной цифровой подписи;	
3.1.8	основные стандарты на алгоритмы цифровой подписи.	
3.2	Уметь:	
3.2.1	использовать блочные алгоритмы шифрования для формирования хеш-функции;	
3.2.2	использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;	
3.2.3	использовать односторонние функции в целях построения криптосистем;	
3.2.4	использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;	
3.2.5	использовать алгоритмы генерации, хранения и распределения ключей;	
3.2.6	проектировать и использовать системы электронной цифровой подписи.	
3.3	Владеть:	
3.3.1	навыками симметричного шифрования;	
3.3.2	навыками формирования хеш-функций;	
3.3.3	навыками по обеспечению безопасной работы в сети Интернет;	
3.3.4	навыками применения асимметричных криптосистем;	
3.3.5	навыками управления ключами в системах с открытым ключом;	
3.3.6	навыками по созданию электронной цифровой подписи.	

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	6 ЗЕТ
Часов по учебному плану: 216 в том числе: аудиторные занятия: 136 самостоятельная работа: 44,1 часов на контроль: 18 контактная работа: 153,9 ИКР: 17,9	Виды контроля в семестрах: экзамены 8 зачеты 7

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Криптографические методы защиты информации: история криптографии; виды информации, подлежащие закрытию, их модели и свойства. Введение в криптографические методы защиты информации.			
1.1	История вопроса. Математические модели шифров и открытых текстов. Задачи и основные цели криптографии. Основные типы криптоаналитического вскрытия. Безопасность алгоритмов. Стеганография. Протоколы. Характеристики протоколов. Протоколы с посредником. Арбитражные протоколы. Передача информации с использованием симметричной криптографии. Передача информации с использованием криптографии с открытыми ключами. /Лек/	7	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
1.2	Проработка лекционного материала. /Ср/	7	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5



	Раздел 2. Шифры простой замены и перестановки. Поточные и блочные шифры простой замены. Шифры гаммирования.			
2.1	Шифры простой замены и перестановки. Поточные и блочные шифры простой замены. Дисковые многоалфавитные шифры замены. Шифры гаммирования. /Лек/	7	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
2.2	Математические основы криптографии. Решение задач. Шифры простой замены. Программная реализация. Шифры подстановки. Программная реализация. /Пр/	7	18	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
2.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. /Ср/	7	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Криптографическая стойкость шифров: основные требования к шифрам. Совершенные шифры.			
3.1	Криптографическая стойкость шифров. Основные требования к шифрам. Совершенные шифры. /Лек/	7	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
3.2	Проработка лекционного материала. /Ср/	7	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 4. Блочные системы шифрования. Стандарты шифрования ГОСТ 28147-89, DES. Анализ алгоритмов блочного шифрования. Поточные системы шифрования.			
4.1	Блочные системы шифрования. Преобразование Фейстеля. Алгоритм шифрования DES Стандарты шифрования ГОСТ 28147-89, AES. Режимы использования блочных шифров. Поточное шифрование. /Лек/	7	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
4.2	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Криптоанализ блочных шифров. /Ср/	7	9,1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
4.3	Стандарты шифрования DES, ГОСТ 28147 - 89, AES. /Пр/	7	16	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 5. Псевдослучайные последовательности.			
5.1	Генераторы псевдослучайных последовательностей. Криптостойкие генераторы на основе односторонних функций. Тестирование псевдослучайных последовательностей. Универсальный алгоритм тестирования. Тесты на основе приращения энтропии, на основе алгоритма сжатия Лемпеля – Зива и др. /Лек/	7	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
5.2	Проработка лекционного материала. Алгоритмы построения и тестирования псевдослучайных последовательностей. /Ср/	7	8	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 6. Криптоанализ блочных шифров.			
6.1	Криптоанализ блочных шифров. /Лек/	7	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
6.2	Проработка лекционного материала. /Ср/	7	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 7. Асимметричные системы шифрования. Алгоритмы Диффи-Хеллмана. Шифрсистемы RSA, Эль-Гамала, Мак-Элиса, Рабина.			



Рабочая программа дисциплины "Методы и средства криптографической защиты информации" по направлению подготовки (специальности) 10.05.03 "Информационная безопасность автоматизированных систем" направленности (профилю) специализация N 4 "Безопасность автоматизированных систем критически важных объектов" ФГБОУ ВО «ЧелГУ»				стр. 6
7.1	Задачи криптографии. Этапы развития криптографии. Зарождение асимметричной криптографии. Модели симметричных и асимметричных шифров. Задачи асимметричной криптографии. Криптосистема RSA. Описание системы. Взаимосвязь параметров системы. Атаки на RSA. Алгоритмы факторизации. Выбор параметров системы. Асимметричные криптосистемы. Криптосистема Голдвассера- Микали. Рюкзачный метод шифрования. Криптосистема Эль-Гамала. Криптосистема Рабина. Криптосистема Мак-Элиса. Методы дискретного логарифмирования. /Лек/	8	10	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
7.2	Система RSA. Решение задач. Программная реализация. /Пр/	8	8	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
7.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Алгоритмы асимметричной криптографии. /Ср/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 8. Криптографические хеш-функции. Требования. Назначение. Схемы построения. Стандарты. Криптоанализ.			
8.1	Криптографические хеш-функции. Определение. Требования. Назначение. Стандартная схема алгоритма хеш-функции. Семейство алгоритмов SHA. Алгоритмы хеширования MD4, MD5. /Лек/	8	12	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
8.2	Криптографические хеш-функции. Решение задач. Программная реализация. /Пр/	8	14	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
8.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Хеш-функции. /Ср/	8	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 9. Электронная цифровая подпись. Модель ЭЦП. Задачи ЭЦП. Алгоритмы и стандарты ЭЦП.			
9.1	Электронная цифровая подпись. Модель ЭЦП. Задачи ЭЦП. Схема Диффи-Лампорта. Вероятностная схема Рабина. Схема Эль-Гамала. DSA. ГОСТ Р 34.10-94. Схема Онга-Шнорра-Шамира. Схема Шнорра. Схема Фиата-Шамира. Схемы с восстановлением сообщения. /Лек/	8	12	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
9.2	Электронная цифровая подпись. Решение задач. Программная реализация. /Пр/	8	12	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
9.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Электронная цифровая подпись. /Ср/	8	5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
	Раздел 10. Иная контактная работа			
10.1	Индивидуальные консультации, текущий контроль /ИКР/	7	6,9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5
10.2	Индивидуальные консультации, текущий контроль /ИКР/	8	11	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Э1 Э2 Э3 Э4 Э5

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Собеседование и отчеты по практическим работам.
Зачет
Экзамен



6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Собеседование по темам практических работ:

1. Шифры простой замены.
2. Шифры подстановки.
3. Стандарты шифрования DES, ГОСТ 28147 - 89, AES.
4. Система RSA.
5. Криптографические хеш-функции.
6. Электронная цифровая подпись.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к зачету:

1. Задачи и основные цели криптографии.
2. Основные типы криптоаналитического вскрытия.
3. Безопасность алгоритмов.
4. Стеганография.
5. Подстановочные шифры.
6. Шифры перестановки.
7. Гаммирование.
8. Протоколы. Характеристики протоколов.
9. Протоколы с посредником.
10. Арбитражные протоколы.
11. Передача информации с использованием симметричной криптографии.
12. Передача информации с использованием криптографии с открытыми ключами.
13. Шифры гаммирования: Шифр модульного гаммирования Виженера; Шифр Вернама.
14. Надежность шифров.
15. Сеть Фейстеля.
16. Алгоритм шифрования DES.
17. Стандарт шифрования ГОСТ 28147-89.
18. Поточные системы шифрования.
19. Генерация случайных и псевдослучайных последовательностей.
20. Криптоанализ блочных шифров.

Вопросы к экзамену:

1. Алгоритм Диффи-Хеллмана. Задача Диффи-Хеллмана. Задача дискретного логарифмирования.
2. Криптосистема RSA. Задача RSA.
3. Атаки на RSA.
4. Алгоритмы факторизации.
5. Выбор параметров криптосистемы RSA.
6. Схема шифрования RSA-OAEP.
7. Криптосистемы с открытым ключом.
8. Хеш-функции. Требования.
9. Хеш-функции. Предназначение.
10. Стандарты хеш-функций.
11. Общая схема алгоритмов MD4, MD5, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94, SHA.
12. Криптоанализ хеш-функций. Модель случайного оракула (ROM).
13. Электронная цифровая подпись (ЭЦП). Задачи ЭЦП.
14. Схема ЭЦП Диффи-Лампорта. Вероятностная схема ЭЦП Рабина.
15. Схема ЭЦП Эль-Гамала. Уменьшение размера подписи в схеме Эль-Гамала.
16. ЭЦП DSA.
17. ЭЦП ГОСТ Р 34.10-94.
18. ЭЦП Онга-Шнорра-Шамира.
19. ЭЦП Шнорра.
20. Схемы ЭЦП с восстановлением сообщений (на основе RSA, на основе ЭЦП Эль-Гамала, ЭЦП Рабина).
21. Слепая ЭЦП Чаума (на основе RSA).

6.4. Критерии оценивания

Критерии оценивания собеседования и отчета по практическим работам:

В процессе выполнения практической работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование. Практическая работа засчитывается студенту, если он представил правильно оформленный отчет, владеет методикой обработки данных; усвоил теоретический материал по данной теме (последовательно, грамотно и логически стройно его излагает, уверенно отвечает на вопросы). Допускаются несущественные неточности в оформлении и ответах на вопросы.



Практическая работа не засчитывается студенту в случаях: наличия ошибок в расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.

Критерии оценивания зачета:

Студент допускается к зачету по дисциплине в случае выполнения им учебного плана по дисциплине (выполненных и защищенных работ). В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.

Зачет проводится по билетам в устной форме. Студент выбирает билет в случайном порядке. Время подготовки студента для устного ответа на зачете должно составлять не менее 40 минут, время ответа – не более 20 минут. При подготовке и ответе на вопросы билета студент должен вести необходимые записи в листе устного ответа, который по окончании зачета подписывается студентом, сдается преподавателю и сохраняется им до окончания экзаменационной сессии. Проявленные студентом в ходе зачета знания оцениваются словами «зачтено», «не зачтено».

«Зачтено» выставляется:

- 1) содержание материала билета раскрыто полностью;
- 2) материал изложен грамотно, в определенной логической последовательности, точно используется терминология;
- 3) показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации;
- 4) продемонстрировано усвоение ранее изученных сопутствующих вопросов;
- 5) ответ самостоятельный, без наводящих вопросов;
- 6) допущены одна–две неточности при освещении второстепенных вопросов, которые исправляются после замечаний или наводящих вопросов.

«Не зачтено» выставляется:

- 1) не раскрыто основное содержание учебного материала;
- 2) обнаружено незнание или непонимание большей или наиболее важной части учебного материала;
- 3) допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.

Критерии оценивания экзамена:

Студент допускается к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполненных и защищенных работ. В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.

Экзамен проводится по билетам в устной форме. При проведении экзамена экзаменуемый выбирает билет в случайном порядке. Экзаменатору предоставляется право по ходу экзамена задавать экзаменуемому уточняющие и дополнительные вопросы. Время подготовки студента для устного ответа на экзамене должно составлять не менее 40 минут, время ответа экзаменуемого – не более 20 минут. При подготовке и ответе на вопросы билета экзаменуемый должен вести необходимые записи в листе устного ответа, который по окончании экзамена подписывается студентом, сдается экзаменатору и сохраняется им до окончания экзаменационной сессии. Студент, испытывавший затруднения при подготовке к ответу по выбранному билету, вправе выбрать второй билет с продлением времени на подготовку. При этом окончательная оценка студента снижается на один балл. Выбор студентом третьего билета не допускается. Проявленные студентом в ходе экзамена знания оцениваются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знания по предмету демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.

Оценка «хорошо» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.

Оценка «удовлетворительно» выставляется:

Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

Оценка «неудовлетворительно» выставляется:

1) Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.



2) Ответ на вопрос полностью отсутствует.

3) Отказ от ответа.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Фороузан Б. А.	Математика криптографии и теория шифрования: учебное пособие (https://biblioclub.ru/index.php?page=book&id=428998)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.2	Бабаш А.В.	Криптографические методы защиты информации: учебно-методическое пособие: том 3 (https://znanium.com/catalog/document?id=52118)	Москва : Издательский Центр РИОР, 2014	ЭБС
Л1.3	Кирпичников А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации: учебное пособие (https://biblioclub.ru/index.php?page=book&id=560536)	Казань : Казанский национальный исследовательский технологический университет (КНИТУ), 2016	ЭБС
Л1.4	Бабаш А.В.	Криптографические методы защиты информации: учебно-методическое пособие: том 1 (https://znanium.com/catalog/document?id=368272)	Москва : Издательский Центр РИОР, 2021	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Василенко О. Н.	Теоретико-числовые алгоритмы в криптографии: монография (https://biblioclub.ru/index.php?page=book&id=61814)	Москва : МЦНМО, 2006	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Лань [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Лань. - URL: http://e.lanbook.com/
Э2	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. - URL: http://biblioclub.ru/
Э3	Юрайт [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Юрайт. - URL: https://urait.ru/
Э4	Znanium.com [Электронный ресурс] : электронно-библиотечная система (ЭБС) / Научно-издательский центр ИНФРА-М. - URL: http://znanium.com/
Э5	eLIBRARY.RU [Электронный ресурс] : электронная библиотека / Науч. электрон. б-ка. - URL: http://elibrary.ru/defaultx.asp

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

OpenOffice
Adobe Reader
Notepad++
LMS Moodle
Adobe Connect Acrobat
ПО Kaspersky



7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.
2. APS JOURNALS. Physical Review Letters, Physical Review X, Physical Review, and Reviews of Modern Physics : журналы American Physical Society : сайт. – URL: <http://journals.aps.org/about> – Яз. англ. – Режим доступа: только из сети университета. – Текст : электронный.
3. Web of Science : мультидисциплинарная реферативная база данных / компания Thomson Reuters. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.
4. Scopus : реферативная база данных / Elsevier BV. – URL: <http://www.scopus.com/> – Яз. англ. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.
5. Springer Link : [сайт]. – URL: <http://link.springer.com/> – Яз. англ. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, для проведения занятий семинарского типа, для проведения групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации, а также аудитории для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения - мультимедийным оборудованием (экран, ноутбук, проектор, колонки).

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий (мультимедийные презентации), различные формы наглядности (графики, таблицы, схемы и т.д.).

Практические занятия проходят в учебной лаборатории электроники и схемотехники, микропроцессорных систем (аудитория 221 учебный корпус №1). Материально-техническое обеспечение приведено в паспорте лаборатории.

Для самостоятельной работы студента используются аудитория №205 - читальный зал №3 (учебный корпус №1) и аудитория №206 - электронный читальный зал (специализированный медиацентр) (учебный корпус №1), оснащенные персональными компьютерами, мультимедийной аппаратурой. В аудиториях обеспечен доступ к различной справочной литературе, энциклопедиям, библиографическим и полнотекстовым базам данных, информационным ресурсам «Интернет».

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Освоение содержания учебной дисциплины «Методы и средства криптографической защиты информации» осуществляется на лекциях, практических занятиях и в процессе самостоятельной учебной деятельности студентов.

Лекции составляют основу теоретической подготовки студентов с целью понимания ими сущности дисциплины. Лекционные занятия посвящены рассмотрению ключевых, базовых положений дисциплины и разъяснению учебных заданий, выносимых на самостоятельную проработку. В ходе лекционных занятий нужно конспектировать учебный материал, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений. Лекции должны активизировать познавательную деятельность обучающихся, вызывать интерес к поставленным проблемам и направлениям развития в профессиональной области, формировать их профессиональный кругозор, аналитические качества, творческий подход к изучению дисциплины, определять направления дальнейшего самостоятельного изучения и практического освоения в данной области. Изложение материала лекций должно носить проблемный, инновационный характер, способствующий формированию и развитию соответствующих компетенций. Преподавателю необходимо опираться на основную литературу, представленную в рабочей программе данной дисциплины, а также на учебные пособия, монографии, научные статьи и периодические издания известных специалистов в данной области.

Практические занятия предназначены для приобретения опыта практической реализации полученных теоретических знаний. Указания к практическим работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется преподавателем перед проведением практических занятий. На практических занятиях студенты овладевают первоначальными профессиональными умениями и навыками, которые в дальнейшем закрепляются и совершенствуются в процессе прохождения учебной и производственной практик.

Самостоятельная работа студентов включает проработку лекционного курса, подготовку к практическим работам, выполнение всех заявленных в рабочей программе видов самостоятельной работы (выполнение домашних заданий). Самостоятельная работа предусматривает не только проработку материалов лекционного курса, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации из всех возможных источников. В ходе самостоятельной работы необходимо изучить основную литературу, ознакомиться с дополнительной литературой. Очень полезно дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой.



В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, MS Office365, форумы, электронная почта и др.).

При обучении инвалидов и лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ с помощью специальных технических и программных средств к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.

Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и особенностям восприятия информации.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.

При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.



Рабочая программа дисциплины (модуля) одобрена и рекомендована:

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом физического факультета

Протокол заседания № 05 от 06.02.2025

Председатель Ученого совета
физического факультета

согласовано

М.А. Загребин

Заседанием кафедры радиофизики и электроники

Протокол заседания № 07 от 04.02.2025

Заведующий кафедрой

согласовано

А.В. Бутаков

Автор (составитель)

О.О. Павлухина

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1