Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таскаев Сергей Валерьевич
Должность: Ректор
Дата подписания: 02.04.2025 17:03:08
Уникальный программный ключ:
04c19ed8bfb98f3b6cb77a486b9a8788b822f37

Рабочая программа дисциплины (модуля)*

Теоретико-числовые методы в криптографии

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация N 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2023

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

Челябинск 2023 г.

© ФГБОУ ВО «ЧелГУ»

Содержание

© ФГБОУ ВО «ЧелГУ»

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения учебной дисциплины состоит в овладении основами теории чисел, основными теоретико-числовыми методами, которые используются или могут использоваться в криптографии.

Задачами изучения дисциплины являются:

- изучение и освоение вероятностных и детерминистических алгоритмов простоты числа, алгоритмов факторизации числа, алгоритмов дискретного логарифмирования;

- овладение арифметическими операциями с большими целыми числами;

- изучение точных и асимптотических оценок сложности основных теоретико-числовых алгоритмов;

- ознакомление с современным состоянием алгоритмической теорией чисел.

Результаты обучения по дисциплине направлены на достижение индикаторов:

УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует собственные суждения и оценки.

УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации.

ОПК-10.1 Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; базовые понятия теории эллиптических кривых.

ОПК-10.2 Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях; исследовать и решать сравнения в кольцах вычетов; использовать достаточные условия простоты для построения больших простых чисел; оценивать теоретическую сложность применяемых алгоритмов.

ОПК-10.3 Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	К.М.01.03

2.1 Требования к предварительной подготовке обучающегося:

Теория чисел

Языки программирования

Алгебра

Методы программирования

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

Методы и средства криптографической защиты информации

Криптографические протоколы

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

УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Знать:

– основы выполнения эффективного поиска информации.

Уметь:

– определять критерии системного анализа для поставленных задач.

Владеть:

– навыками системного анализа и поиска информации.

© ФГБОУ ВО «ЧелГУ»

ОПК-10: Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

Знать:

– точные и асимптотические оценки сложности основных теоретико-числовых алгоритмов;
– основные теоретико-числовые методы и подходы для решения прикладных задач.

Уметь:

– применять основные теоретико-числовые результаты, изучаемые в курсе, для решения задач в криптографии.

Владеть:

– основными теоретико-числовыми методами, которые используются или могут использоваться в криптографии.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– основные теоретико-числовые свойства делимости, непрерывных дробей, систем и классов вычетов.
3.2	**Уметь:**
3.2.1	– применять методы теории чисел для решения задач.
3.3	**Владеть:**
3.3.1	– решения теоретико-числовых задач.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**3 ЗЕТ**
Часов по учебному плану : 108 в том числе : аудиторные занятия : 50 самостоятельная работа : 52,9 : контактная работа: 55,1 ИКР: 5,1	Виды контроля в семестрах: зачеты 6

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. 1. Оценка сложности арифметических операций			
1.1	Сложность арифметических операций с целыми числами. /Лек/	6	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.2	Сложность арифметических операций с целыми числами. /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.3	Сложность арифметических операций с целыми числами. /Ср/	6	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.4	Сложность арифметических операций в кольцах вычетов. /Лек/	6	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.5	Сложность арифметических операций в кольцах вычетов. /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
1.6	Сложность арифметических операций в кольцах вычетов. /Ср/	6	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
	Раздел 2. 2. Тестирование чисел на простоту и построение больших простых чисел			

© ФГБОУ ВО «ЧелГУ»

2.1	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.2	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.3	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.4	Алгоритм Конягина-Померанса. Алгоритм Миллера. /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.5	Алгоритм Конягина-Померанса. Алгоритм Миллера. /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.6	Алгоритм Конягина-Померанса. Алгоритм Миллера. /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.7	Современные методы проверки простоты числа. Детерминированный полиномиальный алгоритм проверки простоты чисел. /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.8	Современные методы проверки простоты числа. Детерминированный полиномиальный алгоритм проверки простоты чисел. /Пр/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.9	Современные методы проверки простоты числа. Детерминированный полиномиальный алгоритм проверки простоты чисел. /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.10	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.11	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Пр/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
2.12	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Ср/	6	4,9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
	Раздел 3. 3. Факторизация целых чисел			
3.1	Экспоненциальные алгоритмы (метод пробных делений, Ро-метод Полларда, Ферма, (p-1)-метод Полларда, (p+1)-метод Вильямса, Шермана-Лемана, Ленстры). /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.2	Экспоненциальные алгоритмы (метод пробных делений, Ро-метод Полларда, Ферма, (p-1)-метод Полларда, (p+1)-метод Вильямса, Шермана-Лемана, Ленстры). /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.3	Экспоненциальные алгоритмы (метод пробных делений, Ро-метод Полларда, Ферма, (p-1)-метод Полларда, (p+1)-метод Вильямса, Шермана-Лемана, Ленстры). /Ср/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.4	Субэкспоненциальные алгоритмы Диксона, Бриллхарта-Моррисона, метод решета). /Лек/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.5	Субэкспоненциальные алгоритмы Диксона, Бриллхарта-Моррисона, метод решета). /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.6	Субэкспоненциальные алгоритмы Диксона, Бриллхарта-Моррисона, метод решета). /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1

© ФГБОУ ВО «ЧелГУ»

3.7	Применение эллиптических кривых для проверки простоты и факторизации. /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.8	Применение эллиптических кривых для проверки простоты и факторизации. /Пр/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
3.9	Применение эллиптических кривых для проверки простоты и факторизации. /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1
	Раздел 4. Иная контактная работа			
4.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	6	5,1	

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Контрольная работа.
Коллоквиум.
Домашняя самостоятельная работа.
Перечень вопросов к зачету.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Перечень вопросов к коллоквиуму
1. Тест на основе теоремы Ферма.
2. Свойства псевдопростых чисел.
3. Свойства чисел Кармайкла (доказать).
4. Тест Соловея-Штрассена, его обоснование.
5. Тест Рабина –Миллера, его обоснование.
6. Тесты на простоту для чисел специального вида.
7. Алгоритм Конягина-Померанса.
8. Алгоритм Ферма (факторизация).
9. ρ- метод Полларда (факторизация).
10. Алгоритм Ленстры (факторизация).
11. Алгоритм Шермана-Лемана (факторизация).
12. Алгоритм Диксона (факторизация).
13. Алгоритм Миллера (детерминированный).
14. Алгоритм ПоллардаШтрассена (факторизация).
15. $P+1$ метод Вильямса (факторизация).

Домашняя самостоятельная работа
1. Изучить алгоритм факторизации и сделать доклад.
2. Реализовать алгоритм. Написать программу для работы с большими числами.
3. Вычислить сложность алгоритма.
4. Привести числовый пример для маленького числа, иллюстрирующий работу алгоритма.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Перечень вопросов к зачету.
1. Решето Эратосфена.
2. Критерий Вильсона.
3. Тест на основе теоремы Ферма.
4. Свойства псевдопростых чисел (доказать).
5. Свойства чисел Кармайкла (доказать).
6. Тест Соловея-Штрассена, его обоснование.
7. Тест Рабина –Миллера, его обоснование.
8. Тесты на простоту для чисел специального вида.
9. Алгоритм Конягина-Померанса.
10. Алгоритм Ферма (факторизация).
11. ρ- метод Полларда (факторизация).
12. Алгоритм Ленстры (факторизация).
13. Алгоритм Шермана-Лемана (факторизация).

© ФГБОУ ВО «ЧелГУ»

14. Алгоритм Диксона (факторизация).
15. Алгоритм Миллера (детерминированный).
16. Алгоритм Берлекэмпа.
17. Алгоритм ПоллардаШтрассена (факторизация).
18. $P+1$ метод Уильямса (факторизация).
19. Квадратичное решето.

6.4. Критерии оценивания

В ходе изучения дисциплины «Теоретико-числовые методы в криптографии» студент должен выполнить одну контрольную работу, одну домашнюю самостоятельную работу и сдать один коллоквиум. В конце семестра сдаётся зачет.
Каждая из работ, коллоквиум оцениваются в 20 баллов, экзамен оценивается в 40 баллов. Нарушение сроков без уважительной причины ведет за собой снижение баллов за контрольную работу и коллоквиум на 2 балла за каждую неделю задержки.
Билеты для зачета содержат 4 задания (2 практических задачи и 2 теоретических вопроса). За каждое выполненное задание билета студент может получить от 2 до 5 баллов. Если задание выполнено правильно, то оно оценивается 5 баллами. Если задание выполнено с ошибками, то баллы снижаются в зависимости от количества допущенных ошибок. Если допущена одна ошибка, то здание оценивается 4 баллами, допущены две ошибки – 3 баллами, допущены три ошибки – 2 баллами. Если задание выполнено частично, и выполненная часть задания не содержит ошибок, то оно оценивается 2 баллами. Если допущено более трех ошибок в задании или студент выполнил менее половины задания из билета, то за него он получает 0 баллов.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Контрольная работа	20
2	Домашняя самостоятельная работа	20
3	Коллоквиум	20
4	Экзамен	40
Итого		100

Критерии оценивания домашней самостоятельной работы
Максимальный балл за работу — 20 баллов.
Работа включает 4 задания.
Отлично/зачтено/5 баллов - Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета.
Хорошо/зачтено/4 балла - Студентом дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания. Однако допускает неточность в ответе.
Удовлетворительно/зачтено/3 балла - Студентом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, недостаточным умением давать аргументированные ответы и приводить примеры. Допускает несколько ошибок в содержании ответа.
Неудовлетворительно/не зачтено/2 балла - Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории слабым владением монологической речью, отсутствием логичности и последовательности. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Критерии оценивания контрольной работы
Максимальный балл за контрольную работу – 20 баллов.
Контрольная работа включает 4 задания.
Критерии оценивания каждого задания
Отлично/зачтено/5 баллов - Задание решено правильно, дан полный, развернутый ответ на поставленный вопрос.
Хорошо/зачтено/4 балла - Выполнено 3/4 задания, дан полный, развернутый ответ на поставленный вопрос, однако были допущены неточности в определении понятий, терминов и др.
Удовлетворительно/зачтено/3 балла - Выполнено 1/2 задания, дан неполный ответ на поставленный вопрос.
Неудовлетворительно/не зачтено/2 балла - Выполнено менее 1/2 задания, на поставленный вопросы ответ отсутствует или неполный, допущены существенные ошибки в терминах и понятиях.

Критерии оценивания ответа на коллоквиуме
Максимальный балл за коллоквиум – 20 баллов.

© ФГБОУ ВО «ЧелГУ»

Коллоквиум включает 4 вопроса.
Критерии оценивания одного вопроса
Отлично/зачтено/5 баллов - Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета.
Хорошо/зачтено/4 балла - Студентом дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания. Однако допускает неточность в ответе.
Удовлетворительно/зачтено/3 балла - Студентом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, недостаточным умением давать аргументированные ответы и приводить примеры. Допускает несколько ошибок в содержании ответа.
Неудовлетворительно/не зачтено/2 балла - Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории слабым владением монологической речью, отсутствием логичности и последовательности. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Критерии оценивания теоретического вопроса зачета и практической задачи зачета
Максимальный балл за ответ на теоретический вопрос – 10 баллов.
Отлично/зачтено/9-10 баллов - Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса.
Хорошо/зачтено/7-8 баллов - Студентом дан развернутый ответ на поставленный вопрос, в котором студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе.
Удовлетворительно/зачтено/5-6 баллов - Студентом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа.
Неудовлетворительно/не зачтено/0-4 баллов - Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Результаты промежуточной аттестации и уровни сформированности компетенций
При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:
Критерии оценивания экзамена:
менее 50 – «неудовлетворительно»
50 – 69 – «удовлетворительно»
70 – 90 – «хорошо»
91 – 100 – «отлично».

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

© ФГБОУ ВО «ЧелГУ»

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.2	Кнауб Л. В., Новиков Е. А., Шитов Ю. А.	Теоретико-численные методы в криптографии: учебное пособие (https://biblioclub.ru/index.php?page=book&id=229582)	Красноярск : Сибирский федеральный университет (СФУ), 2011	ЭБС
Л1.3		Теоретико-числовые методы в криптографии: практикум (https://biblioclub.ru/index.php?page=book&id=483838)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	Введение в теоретико-числовые методы криптографии: учебное пособие для вузов	Санкт-Петербург [и др.] : Лань, 2011	
Л2.2		Информационный мир XXI века. Криптография- основа информационной безопасности: учебно-методическая литература (https://znanium.com/catalog/document?id=353538)	Москва : Дашков и К, 2020	ЭБС
Л2.3	Мартынов Л. М.	Алгебра и теория чисел для криптографии (https://e.lanbook.com/book/189446)	Санкт- Петербург : Лань, 2022	ЭБС

7.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л3.1	Ниссенбаум О. В.	Теоретико-числовые методы в криптографии. Сборник заданий: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем», направления «Информационная безопасность»: учебно-методическое пособие (https://biblioclub.ru/index.php?page=book&id=567498)	Тюмень : Тюменский государственный университет, 2014	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Visual Studio

Python

Notepad++

WinDjView

Java Development Kit

Adobe Reader

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. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

© ФГБОУ ВО «ЧелГУ»

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

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

При изучении данной дисциплины используются лекционные, практические занятия и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.
На практических занятиях рассматриваются конкретные способы реализации теоретико-числовых алгоритмов.
Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на практических и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

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, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении 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 голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья

© ФГБОУ ВО «ЧелГУ»

ЧелГУ по запросу обучающегося.

1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.
2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.
3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.

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

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся 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 к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).

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

Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.

Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

© ФГБОУ ВО «ЧелГУ»

в) доступная форма предоставления 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 технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. 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.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

© ФГБОУ ВО «ЧелГУ»

Специальность 10.05.01 Компьютерная безопасность
Специализация № 1 «Анализ безопасности компьютерных систем»
Рабочая программа дисциплины «Теоретико-числовые методы в криптографии»
2023 год набора, очная форма обучения

Проректор по учебной работе утверждено 24.04.2023 В.Е. Федоров

Ученым советом математического факультета

Протокол заседания № 8 от 13.04.2023

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 10 от 31.03.2023

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) Кораблева В.В.

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