УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.Е. Федоров
«25» 06 2021 г.

Рабочая программа дисциплины (модуля)*
Теоретико-числовые методы в криптографии

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация № 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)
специалист по защите информации

Форма обучения
очная

Год(ы) набора 2021

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

Челябинск 2021 г.

Рабочая программа дисциплины (модуля) принята:
Ученым советом математического факультета

Протокол заседания № 13 от «24» 06 2021 г.

Председатель Ученого совета
математического факультета _____ Е.А. Сбродова

Секретарь Ученого совета
математического факультета _____ С.А. Никитина

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой компьютерной безопасности и прикладной алгебры.

Протокол заседания № 10 от «04» 06 2021 г.

Заведующий кафедрой _____ А.Н. Ручай

Автор (составитель):
Зав.кафедрой, канд.физ.-мат. наук, доцент _____ А.Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1

Содержание

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:

Освоение дисциплины опирается на знания школьного курса математики.

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

Данная дисциплина является предшествующей для следующих дисциплин:

Криптографические методы 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.

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 : 54 самостоятельная работа : 54 :	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. Простые и составные числа. Делимость чисел.			
1.1	Предмет курса, краткий исторический обзор развития теории чисел, основные направления исследований и основные методы. Влияние теории чисел на развитие других разделов математики. Применение теоретико-числовых результатов в математике и ее приложениях. Роль русских и советских математиков в развитии теории чисел. Свойства делимости целых чисел. Простые числа. Решето Эратосфена. Теорема Евклида о бесконечности множества простых чисел. Основная теорема арифметики о разложении целых чисел на простые сомножители. Наибольший общий делитель и наименьшее общее кратное. Некоторые частные случаи теоремы Дирихле о бесконечности множества простых чисел в арифметической прогрессии. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
1.2	Арифметические функции. Целая и дробная часть числа. Разложение числа n! на простые множители. Суммы, распространенные на делители числа. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
1.3	Мультипликативные функции: функция Эйлера и ее свойства, сумма делителей и число делителей. Оценки Чебышева для функции числа простых чисел, не превосходящих данного x. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
1.4	Простые и составные числа. Делимость чисел. /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
1.5	Простые и составные числа. Делимость чисел. /Ср/	6	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
	Раздел 2. 2. Цепные дроби			
2.1	Конечные цепные дроби, подходящие дроби и их свойства. Нахождение наибольшего общего делителя с помощью цепных дробей. Бесконечные цепные дроби. Разложение действительных чисел в цепные дроби. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
2.2	Приближение действительных чисел рациональными числами, подходящие дроби как наилучшие приближения. Признак иррациональности числа. Иррациональность числа«е». Теорема Лагранжа о разложении квадратичных иррациональностей в цепные дроби. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1

2.3	Цепные дроби /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
2.4	Цепные дроби /Ср/	6	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
	Раздел 3. 3. Числовые сравнения			
3.1	Числовые сравнения и их основные свойства. Вычеты и классы вычетов по модулю m, кольца классов вычетов. Полная система вычетов, приведенная система вычетов. Теорема Эйлера и Ферма. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
3.2	Числовые сравнения /Ср/	6	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
	Раздел 4. 4. Сравнения с одним неизвестным			
4.1	Сравнения первой степени с одним неизвестным. Равносильные сравнения. Определение решения сравнения. Теорема о существовании решений. Простейшие приемы решений, решение сравнений с помощью цепных дробей. Системы сравнений, их решения. Теоремы о решении систем сравнений первой степени. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
4.2	Сравнения n-ой степени по простому модулю. Теоремы о равносильности сравнений. Теорема о числе решений сравнения. Теорема Вильсона. Сравнения n-ой степени по составному модулю, сведение сравнения по составному модулю к системе сравнений по простому модулю. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
4.3	Сравнения с одним неизвестным /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
4.4	Сравнения с одним неизвестным /Ср/	6	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
	Раздел 5. 5. Сравнения второй степени			
5.1	Сравнения второй степени, сведение их к двучленному сравнению. Двучленные сравнения по простому модулю. Квадратичные вычеты и невычеты. Число решений сравнения. Критерий Эйлера для квадратичных вычетов и невычетов. Символ Лежандра и его свойства. Закон взаимности квадратичных вычетов. Сравнения второй степени по составному модулю. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
5.2	Сравнения второй степени /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
5.3	Сравнения второй степени /Ср/	6	8	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
	Раздел 6. 6. Первообразные корни и индексы			
6.1	Первообразные корни и индексы. Показатель числа по модулю m, свойства показателей. Теорема о существовании первообразного корня по простому модулю. Первообразные корни по модулям p и 2p. Теорема об отыскании первообразных корней. Индексы по модулям p и 2p. Таблицы индексов. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
6.2	Двучленные сравнения n-ой степени, существование решений. Степенные вычеты и невычеты n-ой степени. Число степенных вычетов, критерий для отыскания степенных вычетов. Решение двучленных сравнений с помощью вычетов. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
6.3	Решение показательных сравнений. Условие принадлежности числа показателю и, в частности, к классу первообразных корней. Число классов принадлежащих показателю. Число классов первообразных корней. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1

6.4	Арифметические приложения теории сравнений: отыскание остатков от деления некоторого числа на заданное число, установление признаков делимости чисел. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
6.5	Первообразные корни и индексы. /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
6.6	Первообразные корни и индексы /Ср/	6	8	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1
	Раздел 7. 7. Оценка сложности арифметических операций			
7.1	Сложность арифметических операций с целыми числами. Сложность вычисления наибольшего общего делителя чисел. Сложность арифметических операций в кольцах вычетов. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
7.2	Сложность арифметических операций с целыми числами. Сложность арифметических операций в кольцах вычетов. /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
7.3	Сложность арифметических операций с целыми числами. Сложность арифметических операций в кольцах вычетов. /Ср/	6	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
	Раздел 8. 8. Тестирование чисел на простоту и построение больших простых чисел			
8.1	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
8.2	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). /Ср/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
8.3	Алгоритм Конягина-Померанса. Алгоритм Миллера. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
8.4	Вероятностные тесты простоты (на основе малой теоремы Ферма, Рабина-Миллера, Соловея-Штрассена). Алгоритм Конягина-Померанса. Алгоритм Миллера. /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
8.5	Алгоритм Конягина-Померанса. Алгоритм Миллера. /Ср/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
8.6	Современные методы проверки простоты числа. Детерминированный полиномиальный алгоритм проверки простоты чисел. Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
8.7	Современные методы проверки простоты числа. Детерминированный полиномиальный алгоритм проверки простоты чисел. /Ср/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
8.8	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
8.9	Тесты на простоту для чисел специального вида. Построение больших простых чисел. /Ср/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
	Раздел 9. 9. Факторизация целых чисел			
9.1	Ро-метод Полларда/ Метод Ферма. (р-1)-метод Полларда/ Алгоритм Диксона. Метод Шермана-Лемана. Алгоритм Ленстры. /Лек/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
9.2	Факторизация целых чисел /Пр/	6	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1
9.3	Факторизация целых чисел /Ср/	6	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.3Л3.1

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Контрольная работа.
Коллоквиум.
Домашняя самостоятельная работа.
Зачет.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Пример типовых контрольных заданий см. в Приложении.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к зачету (1 часть)
1) Кольцо целых чисел. Делимость. Свойства делимости.
2) Общий делитель. НОД. свойства НОД. Взаимная простота. Алгоритм Евклида.
3) Простые числа. Свойства простых чисел. Основная теорема арифметики.
4) Цепные дроби. Подходящие дроби. Свойства цепных дробей. Теорема о единственности представления рационального числа в виде цепной дроби.
5) Цепные дроби. Подходящие дроби. Свойства цепных дробей. Теорема о единственности представления действительного числа в виде цепной дроби.
6) Наилучшее приближение действительного числа. Теорема о наилучшем приближении.
7) Совершенные числа. Теорема Евклида (достаточное условие для четных чисел).
8) Совершенные числа. Теорема Эйлера (необходимое условие для четных чисел).
9) Простые числа Мерсенна. Простые числа Ферма. Свойства чисел Ферма. Открытые вопросы.
10) Мультипликативные функции. Лемма. Формула суммы распространенной на делители числа.
11) Сумма и число делителей числа.
12) Функция Мёбиуса. Леммы. Формула обращения Мёбиуса.
13) Функция Эйлера. Теорема о представлении числа суммой функций Эйлера. Теорема о вычислении функции Эйлера.
14) Сравнения. Свойства сравнения как бинарного отношения. Классы вычетов. Различные системы вычетов(полная, наименьшая, приведенная).
15) Свойства сравнений (леммы). Кольцо классов вычетов (теорема).
16) Деление в кольце классов вычетов. Две теоремы о делении.
17) Группа классов вычетов. Условие того, что кольцо классов вычетов образует поле.
18) Малая теорема Ферма. Теорема Эйлера.
19) Системы сравнений первой степени. Китайская теорема об остатках.
20) Линейные системы сравнений. Метод решения.
21) Сравнения по простому модулю. Две теоремы о сравнениях по простому модулю. Критерий Вильсона.
22) Сравнения по составному модулю. Теорема о равносильности сравнения по составному модулю системе сравнений по взаимно простым модулям. Теорема о сравнении по модулю p^k.
23) Вычеты и невычеты степени n. Леммы и теорема о квадратичном вычете по простому модулю.
24) Символ Лежандра. Теорема о свойствах символа Лежандра. Квадратичный закон взаимности.
25) Символ Якоби. Теорема о свойствах символа Якоби.
26) Сравнения по составному модулю. Теоремы о решении сравнений второй степени по модулям p^k и 2^k.
27) Показатель. Три теоремы о показателе. Первообразные корни.
28) Первообразные корни по простому модулю. Леммы. Теорема о существовании.
29) Первообразные корни по модулям p^k и 2p^k. Теоремы о существовании. Теорема об отыскании первообразных корней.
30) Индексы по модулям p^k и 2p^k. Теорема о степенях первообразного корня. Теорема(свойство индексов).
31) Критерий существования первообразных корней. Теорема (следствия).
32) Индексы по модулю 2^k.

Вопросы к зачету (2 часть)
1. Тест на основе теоремы Ферма.
2. Свойства псевдопростых чисел (доказать).
3. Свойства чисел Кармайкла (доказать).
4. Тест Соловея-Штрассена, его обоснование.
5. Тест Рабина –Миллера, его обоснование.
6. Ро-метод Полларда.
7. Вычисление квадратных корней по простому модулю.
8. Алгоритм Ленстры.
9. Алгоритм Конягина-Померанса.
10. Метод Шермана-Лемана.
11. Метод Ферма.
12. Алгоритм Полларда-Штрассена.

13. Алгоритм согласования (дискретное логарифмирование).
14. Индекс метод (дискретное логарифмирование).
15. Детерминированный полиномиальный алгоритм проверки простоты чисел (AKS).
16. Алгоритм Карацубы.
17. Эллиптические кривые над конечным полем. Группа точек.
18. Экспоненциальные алгоритмы.
19. Субэкспоненциальные алгоритмы.

6.4. Критерии оценивания

Написать

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 (2-е издание, дополненное): монография (https://biblioclub.ru/index.php?page=book&id=61814)	Москва : МЦНМО, 2006	ЭБС
Л1.2		Теоретико-числовые методы в криптографии: практикум (https://biblioclub.ru/index.php?page=book&id=483838)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017	ЭБС
Л1.3	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
Л1.4	Виноградов И. М.	Основы теории чисел (https://e.lanbook.com/book/139285)	Санкт- Петербург : Лань, 2020	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Глухов М. М., Круглов И. А.	Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии (http://e.lanbook.com/books/element.php?pl1_id=65044)	Санкт- Петербург : Лань, 2015	ЭБС
Л2.2	Манин Ю. И., Панчишкин А. А.	Введение в современную теорию чисел: монография (https://biblioclub.ru/index.php?page=book&id=62989)	Москва : МЦНМО, 2009	ЭБС
Л2.3	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
Л2.4	Александров В. А., Горшенин С. М.	Задачник-практикум по теории чисел (https://biblioclub.ru/index.php?page=book&id=454825)	Москва : Просвещение, 1972	ЭБС

7.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л3.1	Гречников Е. А., Михайлов С. В., Нестеренко Ю. В., Поповян И. А.	Вычислительно сложные задачи теории чисел: учебное пособие (https://biblioclub.ru/index.php?page=book&id=595699)	Москва : Московский Государственный Университет, 2012	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

MS Office365

Adobe Reader

Mathcad Prime (Лицензия Математический факультет)

Maxima

Notepad++

Octave

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.

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 разбираются задачи. Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволит лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных 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, видеохостинг YouYube, 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 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);

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.