УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «_17_» ___05_____ 2022_г., протокол №_4/22_
Председатель _____
(подпись, расшифровка подписи)
«_17_» ____05_____ 2022___г.

РАБОЧАЯ ПРОГРАММА

Дисциплина	Теоретико-числовые методы в криптографии
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	3

Специальность: 10.05.01 «Компьютерная безопасность»
код направления (специальности), полное наименование

Специализация: «Математические методы защиты информации»
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «_01_» _____09_____ 2022___ г.

Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04.2024 г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Рацеев Сергей Михайлович	ИБиТУ	профессор, д.ф-м.н, доцент

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления» /_____/ Андреев А.С. / *(подпись)* *(Ф.И.О.)* «__11__»_____05_____2022___г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- обеспечение подготовки в одной из важных областей, находящихся на границе теории чисел, информатики и криптографии;
- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография.

Задачи освоения дисциплины:

- овладение основными вычислительными методами классической и современной теории чисел;
- овладение методами теоретико-числового характера;
- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография;
- выявление различных приложений теории чисел.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части цикла Б1 образовательной программы и читается в 6-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов «Вычислительные методы в алгебре и теории чисел», «Информатика», а также некоторых разделов дисциплин «Алгебра и геометрия», «Дискретная математика», «Математическая логика и теория алгоритмов» и «Математический анализ». Кроме того, необходимо наличие практических навыков программирования на одном из языков программирования высокого уровня.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: вычислительные методы в алгебре и теории чисел, элементы высшей алгебры.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин, как «Методы и средства криптографической защиты информации», «Криптографические протоколы», «Методы алгебраической геометрии в криптографии», а также для прохождения учебной, производственной и преддипломной практик, государственной итоговой аттестации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ДИСЦИПЛИНЕ, СООТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-8 – Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Знать: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; Уметь: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с исполь-

	зованием компьютерных программ; Владеть: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.
ОПК-10 – Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	Знать: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; Уметь: 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; проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; Владеть: методами построения быстрых вычислительных алгоритмов алгебры и теории чисел; навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 4.

4.2. Объем дисциплины по видам учебной работы (в часах):

Вид учебной работы	Количество часов (форма обучения: *очная*)	
	Всего по плану	**В т.ч. по семестрам**
		6
1	2	3
Контактная работа обучающихся с преподавателем	54/54*	54/54*
Аудиторные занятия		
• Лекции	36/36*	36/36*
• Практические и семинарские занятия		
• Лабораторные работы (лабораторный практикум)	18/18*	18/18*
Самостоятельная работа	54	54
Экзамен	36	36
Форма текущего контроля знаний и контроля самостоятельной		Лабораторные работы, проверка решения задач

работы		
Курсовая работа		
Виды промежуточной аттестации		Экзамен
Всего часов по дисциплине	144	144
Общая трудоемкость в зач. ед.	4	4

**В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения*

4.3. Содержание дисциплины. распределение часов по темам и видам учебной работы:

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	
Раздел 1. Сравнения							
1. Системы линейных диофантовых уравнений	12	6				6	
2. Степенные вычеты	16	6		2	2	8	Лабораторная работа. Домашние задания
3. Сравнения второй степени	20	6		4	4	10	Лабораторная работа. Домашние задания
Раздел 2. Тесты на простоту. Факторизация. Дискретное логарифмирование							
4. Тесты на простоту	20	6		4	4	10	Лабораторная работа. Домашние задания
5. Задача факторизации	20	6		4	4	10	Лабораторная работа. Домашние задания
6. Методы дискретного логарифмирования	20	6		4	4	10	Лабораторная работа. Домашние задания
Экзамен	36						
Итого:	144	36	0	18	18	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Сравнения

Тема 1. Системы линейных диофантовых уравнений.

Системы линейных диофантовых уравнений. Допустимые преобразования расширенной матрицы. Алгоритм решения систем диофантовых уравнений. Критерий существования решения. Формула общего решения.

Тема 2. Степенные вычеты.

Показатель числа. Свойства показателя. Первообразные корни по простому модулю. Первообразные корни по составному модулю. Критерий, описывающий все случаи существования первообразных корней. Индексы (дискретные логарифмы). Свойства индексов.

Тема 3. Сравнения второй степени.

Квадратичные вычеты и невычеты. Критерий Эйлера. Символ Лежандра. Свойства символа Лежандра. Критерий Гаусса. Квадратичный закон взаимности Гаусса. Символ Якоби. Свойства символа Якоби. Алгоритм эффективного вычисления символа Лежандра на основе символа Якоби. Вычисление квадратного корня. Алгоритм Тонелли-Шенкса.

Раздел 2. Тесты на простоту. Факторизация. Дискретное логарифмирование

Тема 4. Тесты на простоту.

Тест на простоту на основе малой теоремы Ферма. Псевдопростые числа по заданному основанию. Числа Кармайкла и их свойства. Критерий Корсельта. Критерий Эйлера простоты числа. Эйлеровы псевдопростые числа по заданному основанию. Тест на простоту Соловея-Штрассена. Теорема Миллера. Теорема Рабина. Тест на простоту Миллера-Рабина. Генерация простых чисел. N-1 методы доказательства простоты. Метод Поклингтона проверки на простоту. Теорема Лемера. Алгоритм построения простых чисел p с известным простым делителем q числа p-1.

Тема 5. Задача факторизации.

Задача факторизации. ρ-метод Полларда. (p-1)-метод Полларда.

Тема 6. Методы дискретного логарифмирования.

Метод Гельфонла-Шенкса. ρ-метод Полларда. Метод исчисления порядка. Решение систем сравнений, возникающих в методе исчисления порядка.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторные работы проводятся в интерактивной форме, а именно, используются: диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, группами студентов; элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

Полные задания для лабораторных работ приводятся в учебно-методическом пособии:

Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с.

Раздел 1. Сравнения

Тема 2. Степенные вычеты.

Цель работы: освоение методов нахождения первообразных корней.

Задание. Требуется составить программу, которая для любого простого числа $p > 2$ и любого натурального n находит все первообразные корни по модулю p; первообразный корень по модулю p^n; первообразный корень по модулю $2p^n$.

Входные данные: p и n.

Выходные данные: первообразные корни по соответствующим модулям.
Методические указания. Использовать следующий критерий первообразного корня.
Пусть $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a,m)=1$, $\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ – каноническое разложение числа $\varphi(m)$.
Число a является первообразным корнем по модулю m тогда и только тогда, когда
$a^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \pmod{p}, \quad i = 1,\dots,n.$

Тема 3. Сравнения второй степени.
Цель работы: освоение методов вычисления символа Якоби.
Задание. Требуется составить программу, которая для любого целого числа a и любого нечетного целого $m > 2$ вычисляет значение символа Якоби $\left(\frac{a}{m}\right)$.

Входные данные: a и m.

Выходные данные: значение символа Якоби $\left(\frac{a}{m}\right)$.

Методические указания. Использовать эффективный алгоритм вычисления символа Лежандра на основе символа Якоби.

Тема 3. Сравнения второй степени.
Цель работы: освоение методов вычисления квадратного корня по простому модулю.
Задание. Требуется составить программу, которая для любого целого числа a, любого нечетного простого числа p, $\left(\frac{a}{p}\right)=1$, находит такое x, что $x^2 \equiv a \pmod{p}$.

Входные данные: a и p.

Выходные данные: квадратный корень числа a по модулю p.

Методические указания. Использовать алгоритм Тонелли-Шенкса.

Раздел 2. Тесты на простоту. Факторизация. Дискретное логарифмирование
Тема 4. Тесты на простоту.
Цель работы: освоение методов проверки числа на простоту.
Задание. Требуется составить программу, которая для любого целого числа n проверяет, является ли оно простым.
Входные данные: n
Выходные данные: Заключение о том, что число составное, либо заключение о том, что число не является составным с некоторой вероятностью.
Варианты заданий.
1. Метод Соловея-Штрассена. 2. Метод Миллера-Рабина.
Методические указания. Использовать тест Соловея-Штрассена или тест Миллера-Рабина.

Тема 4. Тесты на простоту.
Цель работы: освоение методов генерации простых чисел.
Задание. Требуется составить программу, которая генерирует простые числа.
Входные данные: k – разрядность простого числа.
Выходные данные: k-битное простое число.
Методические указания. Использовать алгоритм на основе теста Миллера-Рабина.

Тема 5. Задача факторизации.
Цель работы: освоение методов факторизации целых чисел.
Задание. Требуется составить программу, которая раскладывает целые числа на множители.
Входные данные: n – натуральное число.
Выходные данные: разложение числа n на множители.
Методические указания. Использовать алгоритм ρ-метода Полларда.

Тема 6. Методы дискретного логарифмирования.
Цель работы: освоение методов дискретного логарифмирования.
Задание. Требуется составить программу, которая вычисляет дискретный логарифм $\log_a b$.

Входные данные: a, b – натуральные числа, p – простое.

Выходные данные: дискретный логарифм $\log_a b$.

Варианты заданий:
1. Метод Гельфонда-Шенкса.
2. ρ-метод Полларда.
3. Метод исчисления порядка.

Методические указания: основное внимание должно быть уделено освоению методов факторизации на примере метода Гельфонда-Шенкса, ρ-метода Полларда, метода исчисления порядка.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Сравнения произвольной степени по простому модулю.
2. Сравнения по составному модулю.
3. Степенные вычеты. Показатель числа. Свойства показателя.
4. Первообразные корни по простому модулю p.
5. Первообразные корни по модулю p^n.
6. Первообразные корни по модулю $2p^n$.
7. Индексы (дискретные логарифмы), их свойства.
8. Сравнения второй степени. Квадратичный вычет. Критерий Эйлера квадратичного вычета по простому модулю.
9. Квадратичный невычет. Критерий квадратичного невычета по простому модулю.
10. Символ Лежандра и его свойства.
11. Критерий Гаусса и его следствие.
12. Квадратичный закон взаимности Гаусса.
13. Алгоритм вычисления символа Лежандра, использующий факторизацию.
14. Символ Якоби и его свойства.
15. Эффективный алгоритм вычисления символа Лежандра на основе символа Якоби.
16. Алгоритм Тонелли-Шенкса вычисления квадратного корня по простому модулю.
17. Тест на простоту на основе малой теоремы Ферма.
18. Псевдопростые числа по заданному основанию.
19. Числа Кармайкла и их свойства. Критерий Корсельта.
20. Метод Поклингтона проверки на простоту.
21. Критерий Эйлера простоты числа.
22. Эйлеровы псевдопростые числа по заданному основанию.
23. Тест на простоту Соловея-Штрассена.
24. Теорема Миллера. Теорема Рабина. Тест на простоту Миллера-Рабина.
25. Генерация простых чисел.
26. Задача факторизации. ρ-метод Полларда.
27. Задача факторизации. (p-1)-метод Полларда.
28. Методы дискретного логарифмирования. Метод Гельфонла-Шенкса.
29. Методы дискретного логарифмирования. Метод исчисления порядка.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Системы линейных диофантовых уравнений	Проработка учебного материала, подготовка к сдаче зачета, решение задач	6	Экзамен, проверка решения задач
2. Степенные вычеты	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	8	Экзамен, проверка лабораторных работ, проверка решения задач
3. Сравнения второй степени	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	10	Экзамен, проверка лабораторных работ, проверка решения задач
4. Тесты на простоту	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета	10	Экзамен, проверка лабораторных работ
5. Задача факторизации	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета	10	Экзамен, проверка лабораторных работ, проверка решения задач
6. Методы дискретного логарифмирования	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	10	Экзамен, проверка лабораторных работ, проверка решения задач

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Рацеев, С. М. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2022. — 544 с. — ISBN 978-5-8114-8589-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/193323
2. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : Учебник для вузов / Фомичёв Владимир Михайлович, Мельников Дмитрий Анатольевич; Фомичёв В. М., Мельников Д. А. ; под ред. Фомичёва В.М. - Москва : Юрайт, 2022. - 209 с. - (Высшее образование). - URL: https://urait.ru/bcode/489745

дополнительная

1. Бабаш А. В. Моделирование системы защиты информации: Практикум : Учебное пособие / Бабаш А. В., Баранова Е. К.; Национальный исследовательский университет "Высшая школа экономики". - 3 ; перераб. и доп. - Москва : Издательский Центр РИОР, 2021. - 320 с. - ВО - Бакалавриат. - Режим доступа: ЭБС Znanium; по подписке. - ISBN 978-5-369-01848-4. - ISBN 978-5-16-108538-7. - ISBN 978-5-16-016214-0. Ссылка на ресурс http://znanium.com/catalog/document?id=371348
2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-34.10-2012
3. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-34.11-2012

учебно-методическая

1. Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/270
2. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Теоретико-числовые методы в криптографии» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев. - Ульяновск : УлГУ, 2022. - 6 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13330

Согласовано:

ДИРЕКТОР НБ	/ БУРХАНОВА М.М. /		04.05.2022
Должность сотрудника научной библиотеки	ФИО	подпись	дата

б) Программное обеспечение

Реализация программы дисциплины требует наличия учебной лаборатории. Оборудование учебной лаборатории: посадочные места по количеству студентов. Технические средства обучения: компьютеры с лицензионным программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования на языках Си/С++ (Code::Blocks).

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2022]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2022]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2022]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2022]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2022]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2022]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2022]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : научно-информационная база данных EBSCO // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. База данных «Русский как иностранный» : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2022]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2022].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий EastView : электронные журналы / ООО ИВИС. - Москва, [2022]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2022]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase : научно-информационная база данных EBSCO // EBSCOhost : [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал . – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Заместитель начальника УИТиТ /Клочкова А.В. _____/ 04.05.2022

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитория -3/316. Аудитория для проведения лекционных, семинарских и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Комплект переносного мультимедийного оборудования: ноутбук с выходом в Интернет, экран, проектор, Wi-Fi с доступом в Интернет, ЭИОС,ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106-3 корпус

Помещение 503. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 10). Компьютеры, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106 (1 корпус).

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров.

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

Реализация программы дисциплины требует наличия учебной лаборатории. Оборудование учебной лаборатории: посадочные места по количеству студентов. Технические средства обучения: компьютеры с лицензионным программным обеспечением:

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- системы программирования на языках Си/С++ (Code::Blocks, Visual Studio).

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:

- для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик _____ / Ганеев С.М. /
подпись ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/вы-пускающей кафедрой	Подпись	Дата
1.	Внесение изменений в п.п. в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 1	Андреев А.С.		12.04.2023
	Внесение изменений в п.п. в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 2	Андреев А.С.		15.04.2024

б) Программное обеспечение: МойОфис Стандартный, Альт Рабочая станция 8.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступадля пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Инженер ведущий	/ Щуренко Ю.В.	/	/ 04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

б) Программное обеспечение: МойОфис Стандартный, Альт Рабочая станция 8.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. Базы данных периодических изданий: eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Начальник ОА	/ Пышкова Н.А.	/	/ 04.09.2024
должность	ФИО	подпись	дата