

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |



УТВЕРЖДЕНО

решением Ученого совета ФМИАТ
от «17» мая 2022 г., протокол № 4/22
Председатель Волков М.А.
(подпись, расшифровка подписи)
«17» мая 2022 г.

РАБОЧАЯ ПРОГРАММА

| | |
|------------|---|
| Дисциплина | Теория псевдослучайных генераторов |
| Факультет | Математики, информационных и авиационных технологий |
| Кафедра | Информационной безопасности и теории управления |
| Курс | 5 |

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»
код направления (специальности), полное наименование

Специализация: «Безопасность открытых информационных систем»
полное наименование

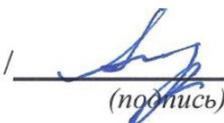
Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

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.

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» | |
|  (подпись) | / Андреев А.С. / (Ф.И.О.) |
| « 11 » 05 2022 г. | |

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- ознакомление студентов с основными понятиями теории генераторов псевдослучайных чисел;
- развитие навыка построения генераторов псевдослучайных чисел.

Задачи освоения дисциплины:

- овладение основными идеями и методами построения генераторов псевдослучайных чисел;
- формирование навыков грамотного применения основ теории генераторов псевдослучайных чисел в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части цикла Б1.В образовательной программы и читается в 9-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра», «Дискретная математика», «Информатика», «Методы и средства криптографической защиты информации».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Дисциплина «Теория псевдослучайных генераторов» является предшествующей для прохождения преддипломной практики и итоговой государственной аттестации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Теория псевдослучайных генераторов» направлен на формирование следующих компетенций.

| Код и наименование реализуемой компетенции | Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций |
|---|---|
| ПК-3 – Способен разрабатывать проектные решения по защите информации в автоматизированных системах | Знать: методы построения криптографических генераторов псевдослучайных чисел; Уметь: решать задачи на построение криптографического генератора псевдослучайных чисел; разрабатывать быстрые вычислительные алгоритмы построения генераторов псевдослучайных чисел для криптографических приложений; Владеть: терминологией теории генераторов псевдослучайных чисел |
| ПК-5 – Способен участвовать в научных и исследовательских работах в сфере разработки средств защиты информации от НСД | Знать: методы построения криптографических генераторов псевдослучайных чисел; Уметь: |

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

| | |
|--|---|
| | <p>решать задачи на построение криптографического генератора псевдослучайных чисел; разрабатывать быстрые вычислительные алгоритмы построения генераторов псевдослучайных чисел для криптографических приложений; Владеть: терминологией теории генераторов псевдослучайных чисел</p> |
|--|---|

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

4.2. Объем дисциплины по видам учебной работы:

| Вид учебной работы | Количество часов (форма обучения - дневная) | |
|--|---|---|
| | Всего по плану | В т.ч. по семестрам |
| | | 9 |
| Контактная работа обучающихся с преподавателем | 72/72* | 72/72* |
| Аудиторные занятия: | | |
| • Лекции | 36/36* | 36/36* |
| • Практические и семинарские занятия | | |
| • Лабораторные работы (лабораторный практикум) | 36/36* | 36/36* |
| Самостоятельная работа | 36 | 36 |
| Экзамен | 36 | 36 |
| Курсовая работа | | |
| Всего часов по дисциплине | 144 | 144 |
| Форма текущего контроля знаний и контроля самостоятельной работы | | Лабораторные работы, проверка решения задач |
| Виды промежуточной аттестации (экзамен, зачет) | | экзамен |
| Общая трудоемкость в зач. ед. | 4 | 4 |

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

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. Генераторы на основе регистра сдвига с линейной обратной связью | | | | | | | |
| 1. Генераторы на основе регистра сдвига с линейной обратной связью | 48 | 12 | | 20 | 6 | 16 | Лабораторная работа. Домашние задания |
| 2. Алгоритм Берлекэмп-Месси | 12 | 8 | | | | 4 | Домашние задания |
| Раздел 2. Генераторы на основе шифров | | | | | | | |
| 3. Генераторы на основе симметричных блочных шифров. | 24 | 8 | | 8 | 3 | 8 | Лабораторная работа. Домашние задания |
| 4. Генераторы на основе хеш-функций и асимметричных блочных шифров. | 24 | 8 | | 8 | 3 | 8 | Лабораторная работа. Домашние задания |
| Экзамен | 36 | | | | | | |
| ВСЕГО | 144 | 36 | | 36 | 12 | 36 | |

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Генераторы на основе регистра сдвига с линейной обратной связью

Тема 1. Генераторы на основе регистра сдвига с линейной обратной связью.

Генераторы случайных чисел. Два класса методов генерации случайных чисел. Требования к генератору псевдослучайных чисел. Среднеквадратичный ГПСЧ. Формула линейного конгруэнтного метода. Теорема о периоде последовательности, формируемой линейным конгруэнтным генератором. Мультипликативные генераторы. Теорема о максимальном периоде последовательности, генерируемой мультипликативным генератором. Обобщение линейного конгруэнтного генератора. Потенциал линейной конгруэнтной последовательности с максимальным периодом. Инверсный конгруэнтный генератор. Теорема о

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

максимальном периоде инверсного конгруэнтного генератора. Недостатки линейных конгруэнтных генераторов. Квадратичный, кубический и полиномиальный конгруэнтные генераторы. Регистр сдвига. Регистр сдвига с линейной обратной связью. Отводная последовательность битов. Примитивные многочлены. Условие максимальности периода последовательности на основе РСЛОС. Частные случаи РСЛОС. Схема работы РСЛОСП. Максимальный период последовательности генератора РСЛОСП. Аддитивные генераторы ПСЧ. Генератор Фибоначчи. Разновидность генератора, предложенная G. Mitchell и D. Moore в 1958 году. Теорема о максимальном периоде последовательности, формируемой аддитивным ГСПЧ Фибоначчи с запаздыванием. Обобщение аддитивного ГСПЧ. Теорема о периоде обобщенного аддитивного ГСПЧ. Выбор коэффициентов.

Тема 2. Алгоритм Берлекэмпа-Мессе.

Алгоритм Берлекэмпа-Мессе над любым полем. Алгоритм Берлекэмпа-Мессе над двоичным полем. Алгоритм Берлекэмпа-Мессе с минимальным числом вычислений обратных элементов. Обобщенный алгоритм Евклида. Взаимосвязь алгоритма Берлекэмпа-Мессе и обобщенного алгоритма Евклида. Криптоанализ последовательности, выработанной с помощью регистра сдвига с линейной обратной связью, на основе алгоритма Берлекэмпа-Мессе.

Раздел 2. Генераторы на основе шифров

Тема 3. Генераторы на основе симметричных блочных шифров.

Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспечивающие обратимость шифра Фейстеля. Режимы использования блочных шифров. Режим электронной кодовой книги. Режим сцепления блоков. Режим гаммирования с обратной связью по шифртексту. Режим гаммирования. Режим выработки имитовставки. Свойства данных режимов. Примеры итеративных блочных шифров. Шифры “Магма” и “Кузнечик” из ГОСТ Р 34.12-2015. Шифр AES. Генераторы на основе симметричных блочных шифров.

Тема 4. Генераторы на основе хеш-функций и асимметричных блочных шифров.

Система Диффи-Хеллмана. Криптосистема без передачи ключа (шифр Шамира). Описание системы. Надежность системы. Шифр Эль-Гамала. Ограничения на параметры системы. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Ограничения на параметры системы. Рюкзачные системы. Описание «проблемы рюкзака». Система Меркла-Хеллмана на основе супервозрастающей последовательности. Криптосистема Шора-Ривеста на основе конечных полей. Построение хеш-функций. Генераторы на основе асимметричных блочных шифров. Генераторы на основе хеш-функций. Алгоритм Блюма-Блюма-Шуба.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом дисциплины.

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.

Подробное задание к лабораторным работам дано в учебно-методическом пособии: Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математиче-

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

ское обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. - URL: ftp://10.2.96.134/Text/Amiranov_2016.pdf

Раздел 1. Генераторы на основе регистра сдвига с линейной обратной связью

Тема 1. Генераторы на основе регистра сдвига с линейной обратной связью.

Цель работы: ознакомиться с методом построения конгруэнтного генератора.

Задание. Написать программу, реализующую алгоритм генерации последовательности псевдослучайных чисел используя конгруэнтный генератор.

Варианты задания.

1. Разработать программу генерации псевдослучайных чисел по формуле линейного конгруэнтного генератора смешанного типа.
2. Разработать программу генерации псевдослучайных чисел по формуле линейного мультипликативного конгруэнтного генератора.
3. Разработать программу генерации псевдослучайных чисел по формуле инверсного конгруэнтного генератора.

Методические указания: параметры генератора подобрать из условия максимальности периода последовательности, используя соответствующую теорему.

Тема 1. Генераторы на основе регистра сдвига с линейной обратной связью.

Цель работы: ознакомиться с методом построения генератора Фибоначчи.

Задание. Написать программу, реализующую алгоритм генерации последовательности псевдослучайных чисел используя конгруэнтный генератор Фибоначчи.

Варианты задания.

1. Разработать программу генерации псевдослучайных чисел по формуле аддитивного генератора Фибоначчи с запаздыванием.
2. Разработать программу генерации псевдослучайных чисел по формуле аддитивного генератора Фибоначчи обобщенного типа.

Тема 1. Генераторы на основе регистра сдвига с линейной обратной связью.

Цель работы: ознакомиться с методом построения заданного генератора.

Задание. Написать программу, реализующую алгоритм генерации последовательности псевдослучайных чисел используя заданный генератор.

Варианты задания.

1. Разработать программу генерации псевдослучайных чисел по формуле: Генератор Геффа.
2. Разработать программу генерации псевдослучайных чисел по формуле: Генератор «Стоп-пошел».
3. Разработать программу генерации псевдослучайных чисел по формуле: Чередующийся генератор «Стоп-пошел».
4. Разработать программу генерации псевдослучайных чисел по формуле: Двухсторонний генератор «Стоп-пошел».
5. Разработать программу генерации псевдослучайных чисел по формуле: Каскад Голлмана из трех РСЛОС.
6. Разработать программу генерации псевдослучайных чисел по формуле: Сжимающий генератор.

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

7. Разработать программу генерации псевдослучайных чисел по формуле: Пороговый генератор из трех РСЛОС.

Методические указания: основное внимание должно быть уделено освоению методам построения генераторов РСЛОС.

Раздел 2. Генераторы на основе шифров

Тема 3. Генераторы на основе симметричных блочных шифров.

Цель работы: Освоение методов построения криптостойких ГПСП на основе блочного шифрования.

Задание: реализация криптографических ГПСП с использованием функций блочных шифров.

Методические указания: основное внимание должно быть уделено освоению методам построения криптостойких ГПСП на основе блочного шифрования.

Тема 4. Генераторы на основе хеш-функций и асимметричных блочных шифров.

Цель работы: Освоение методов построения криптостойких ГПСП на основе односторонних функций.

Задание: реализация криптографических ГПСП с использованием односторонних функций.

Методические указания: основное внимание должно быть уделено освоению методам построения криптостойких ГПСП на основе односторонних функций.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые, контрольные работы и рефераты не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Генераторы случайных чисел. Два класса методов генерации случайных чисел. Требования к генератору псевдослучайных чисел. Среднеквадратичный ГПСЧ.
2. Формула линейного конгруэнтного метода. Теорема о периоде последовательности, формируемой линейным конгруэнтным генератором.
3. Мультипликативные генераторы. Теорема о максимальном периоде последовательности, генерируемой мультипликативным генератором.
4. Обобщение линейного конгруэнтного генератора. Потенциал линейной конгруэнтной последовательности с максимальным периодом.
5. Инверсный конгруэнтный генератор. Теорема о максимальном периоде инверсного конгруэнтного генератора. Недостатки линейных конгруэнтных генераторов.
6. Квадратичный, кубический и полиномиальный конгруэнтные генераторы.
7. Регистр сдвига. Регистр сдвига с линейной обратной связью. Отводная последовательность битов. Примитивные многочлены. Условие максимальности периода последовательности на основе РСЛОС.
8. Частные случаи РСЛОС.
9. Схема работы РСЛОСП. Максимальный период последовательности генератора РСЛОСП
10. Аддитивные генераторы ПСЧ. Генератор Фибоначчи. Разновидность генератора, предложенная G. Mitchell и D. Moore в 1958 году. Теорема о максимальном периоде последовательности, формируемой аддитивным ГСПЧ Фибоначчи с запаздыванием.

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

11. Обобщение аддитивного ГСПЧ. Теорема о периоде обобщенного аддитивного ГСПЧ. Выбор коэффициентов.
12. Генератор Галуа.
13. Генератор Геффе.
14. Пороговый генератор.
15. Генератор «Стоп-пошел».
16. Чередующийся генератор «Стоп-пошел». Двухсторонний генератор «Стоп-пошел».
17. Каскад Голлмана.
18. Самопрореживающие генераторы.
19. Сжимающие генераторы.
20. Безопасный блочный шифр.
21. Генераторы на основе алгоритмов потокового шифра.
22. Генераторы на основе вычислительно сложных математических задач..
23. Генераторы на основе односторонней функции.
24. Графические тесты качества ПСЧП.
25. Статистические тесты качества ПСЧП.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

| Название разделов и тем | Вид самостоятельной работы | Объем в часах | Форма контроля |
|---|---|---------------|---|
| 1. Генераторы на основе регистра сдвига с линейной обратной связью | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач | 16 | Зачет, проверка лабораторных работ, проверка решения домашних задач |
| 2. Алгоритм Берлекэмпа-Месси | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач | 4 | Зачет, проверка решения домашних задач |
| 3. Генераторы на основе симметричных блочных шифров. | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач | 8 | Зачет, проверка лабораторных работ, проверка решения домашних задач |
| 4. Генераторы на основе хеш-функций и асимметричных блочных шифров. | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач | 8 | Зачет, проверка лабораторных работ, проверка решения домашних задач |

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Рябко Б.Я., Криптографические методы защиты информации : Учебное пособие для вузов / Рябко Б.Я., Фионов А.Н. - 2-е издание, стереотип. - М. : Горячая линия - Телеком, 2012. - 229 с. - ISBN 978-5-9912-0286-2 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <http://www.studentlibrary.ru/book/ISBN9785991202862.html>

2. 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>

дополнительная

1. Поднебесова Г.Б. Абстрактная и компьютерная алгебра: практикум/ Поднебесова Г.Б.— Электрон. текстовые данные.— Челябинск: Южно-Уральский государственный гуманитарно-педагогический университет, 2016.— 125 с.— Режим доступа: <http://www.iprbookshop.ru/83852.html>

2. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/87998.html>

учебно-методическая

1. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Теория псевдослучайных генераторов» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2019. - 7 с. - Неопубликованный ресурс. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/10711>.

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. /  / 04.05.2022 /
 должность сотрудника научной библиотеки ФИО подпись дата

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

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.

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: <https://нэб.пф>. – 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](http://window.edu.ru/) : федеральный портал . – URL: <http://window.edu.ru/> . – Текст : электронный.

6.2. [Российское образование](http://www.edu.ru) : 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:

Зам.нач. УИТиТ
должность сотрудника УИТиТ

/ Клочкова А.В.
ФИО


подпись

/ _____
дата

| | | |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа по дисциплине | | |

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 3/317. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций с набором демонстрационного оборудования для обеспечения тематических иллюстраций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 24). Генератор шума для акустического зашумления помещения. Сканирующий радиоприемник AP 3000 А. Широкополосная антенна. Осциллограф АСК 2102. Прибор В6-9 (селективный вольтметр). Генератор НЧ ГЗ-118. Поисковый прибор ST 032 «Пиранья». Имитатор закладных устройств ИМФ-2. Универсальный акустический излучатель к генератору акустического шума OMS-2000. Универсальный электромагнитный излучатель к генератору акустического шума. Генератор электромагнитного зашумления Гром-ЗИ4. Детектор поля D 006. Экран настенный, мультимедийный проектор. Информационные плакаты. Компьютер, Wi-Fi с доступом к сети «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).

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/C++ (Code::Blocks).

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

подпись

ФИО

ЛИСТ ИЗМЕНЕНИЙ

| № п/п | Содержание изменения или ссылка на прилагаемый текст изменения | ФИО заведующего кафедрой, реализующей дисциплину/в ы- 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 доступа для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Инженер ведущий /

Должность сотрудника УИГТ

Щуренко Ю.В. /

ФИО

 /

подпись

04.05.2023 /

дата

