


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



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	Криптографические протоколы
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	5

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 № 13 от 11.05.2022 г.


Программа актуализирована на заседании кафедры: протокол № ___ от ___ 20 ___ 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.

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

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цель изучения дисциплины:

- изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации.

Задачи изучения дисциплины:

- обучить студентов принципам работы основных протоколов;
- привить студентам навыки реализации криптографических протоколов с использованием ЭВМ;
- дать студентам представление об анализе стойкости протоколов к атакам.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части цикла Б1 образовательной программы и читается в 10-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

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


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 «Криптографические протоколы» является предшествующей для прохождения практики и итоговой государственной аттестации.

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

Процесс изучения дисциплины «Криптографические протоколы» 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 использованием 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	Знать: основные типы криптопротоколов и принципов их построения с использованием шифрсистем Уметь:

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

при решении задач профессиональной деятельности	проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств Владеть: подходами к разработке и анализу безопасности криптографических протоколов
---	--


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		
		10		
Контактная работа обучающихся с преподавателем	40/40*	40/40*		
Аудиторные занятия:				
• Лекции	20/20*	20/20*		
• Практические и семинарские занятия				
• Лабораторные работы (лабораторный практикум)	20/20*	20/20*		
Самостоятельная работа	68	68		
Экзамен				
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, проверка решения задач		
Всего часов по дисциплине	108	108		
Виды промежуточного контроля (экзамен, зачет)		зачет		
Общая трудоемкость в зач. ед.	3	3		

**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*

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

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. Протоколы аутентификации								
1. Протоколы аутентификации, использующие технику «запрос–ответ»	16	4					12	
2. Протоколы аутентификации с нулевым разглашением	50	8		10	6	32	Лабораторная работа. Домашние задания	
Раздел 2. Протоколы передачи ключей								
3. Протоколы с нулевым разглашением	26	4		10	6	12	Лабораторная работа. Домашние задания	
4. Протоколы передачи ключей	16	4				12		
Экзамен								
Итого:	108	20		20	12	68		

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)


Раздел 1. Протоколы аутентификации

Тема 1. Протоколы аутентификации, использующие технику «запрос–ответ»

Протоколы аутентификации, использующие пароли (слабая аутентификация). Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием симметричных алгоритмов шифрования. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием асимметричных алгоритмов шифрования.

Тема 2. Протоколы аутентификации с нулевым разглашением

Протокол аутентификации Фиата-Шамира. Протокол Фейга-Фиата-Шамира. Итеративный протокол аутентификации Фиата-Шамира без доверенного центра. Трехпроходный протокол аутентификации Фиата-Шамира без доверенного центра. Протокол аутентификации Шнорра. Итеративный и трехпроходный модифицированный протокол Шнорра. Модификация протокола Шнорра на эллиптических кривых. Итеративный и трехпроходный модифицированный протокол Шнорра на эллиптических кривых. Протокол аутентификации Окамото. Модификация протокола Окамото на эллиптических кривых. Протокол аутентификации Гиллоу-Куискатр (GQ). Протокол аутентификации с нулевым разглашением на основе доказательства изоморфизма графов. Пятипроходный протокол аутенти-

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

фикации на основе изоморфизма графов с использованием эллиптических кривых. Протокол аутентификации с нулевым разглашением на основе асимметричных шифров. Протокола аутентификации с нулевым разглашением на основе шифра RSA. Протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала с использованием эллиптических кривых. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.

Раздел 2. Протоколы передачи ключей

Тема 3. Протоколы с нулевым разглашением

Протокол подбрасывания монеты по телефону. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых. Протоколы привязки к биту. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых.

Тема 4. Протоколы передачи ключей

Передача ключей с использованием симметричного шифрования: двусторонние протоколы. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Протоколы МТІ. Модификация семейства протоколов МТІ на эллиптических кривых. Предварительное распределение ключей. Схема Блома.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические (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: Рацеев С.М. Лабораторный практикум по криптографическим протоколам [Электронный ресурс] / С. М. Рацеев; УлГУ, ФМИАТ, Каф. информ. безопасности и теории управления. - Ульяновск : УлГУ, 2019.

Раздел 1. Протоколы аутентификации

Тема 2. Протоколы аутентификации с нулевым разглашением

Цель работы: освоить методику работы протоколов аутентификации.

Задание. Требуется реализовать протокол аутентификации Фиата-Шамира.

Методические указания: основное внимание должно быть уделено освоению протоколов аутентификации.


Раздел 2. Протоколы передачи ключей

Тема 3. Протоколы с нулевым разглашением

Цель работы: изучение протоколов привязки к биту.

Задание. Реализовать протокол привязки к биту на основе протокола Шнорра.

Методические указания: основное внимание должно быть уделено освоению протоколов привязки к биту.

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

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

Протоколы аутентификации

1. Протоколы аутентификации, использующие пароли (слабая аутентификация).
2. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием симметричных алгоритмов шифрования.
3. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием асимметричных алгоритмов шифрования.

Протоколы аутентификации с нулевым разглашением знания


4. Протокол аутентификации Фиата-Шамира.
5. Протокол Фейга-Фиата-Шамира.
6. Итеративный протокол аутентификации Фиата-Шамира без доверенного центра.
7. Трехпроходный протокол аутентификации Фиата-Шамира без доверенного центра.
8. Протокол аутентификации Шнорра.
9. Итеративный и трехпроходный модифицированный протокол Шнорра.
10. Модификация протокола Шнорра на эллиптических кривых.
11. Итеративный и трехпроходный модифицированный протокол Шнорра на эллиптических кривых.
12. Протокол аутентификации Окамото.
13. Модификация протокола Окамото на эллиптических кривых.
14. Протокол аутентификации Гиллоу-Куискатр (GQ).
15. Протокол аутентификации с нулевым разглашением на основе доказательства изоморфизма графов.
16. Пятипроходный протокол аутентификации на основе изоморфизма графов с использованием эллиптических кривых.
17. Протокол аутентификации с нулевым разглашением на основе асимметричных шифров.
18. Протокола аутентификации с нулевым разглашением на основе шифра RSA.
19. Протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала.
20. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала с использованием эллиптических кривых.
21. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.

Протоколы с нулевым разглашением

22. Протокол подбрасывания монеты по телефону.
23. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых.
24. Протоколы привязки к биту.
25. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых.

Протоколы передачи ключей


26. Передача ключей с использованием симметричного шифрования: двусторонние протоколы.
27. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos.

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

28. Передача ключей с использованием асимметричного шифрования.
29. Открытое распределение ключей. Протоколы МТИ.
30. Модификация семейства протоколов МТИ на эллиптических кривых.
31. Предварительное распределение ключей. Схема Блома.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Протоколы аутентификации, использующие технику «запрос–ответ»	Проработка учебного материала, подготовка к зачету	12	Зачет
2. Протоколы аутентификации с нулевым разглашением	Проработка учебного материала, лабораторные работы, подготовка к зачету, решение задач	32	Проверка лабораторных работ, зачет, проверка решения задач
3. Протоколы с нулевым разглашением	Проработка учебного материала, лабораторные работы, подготовка к зачету	12	Проверка лабораторных работ, зачет
4. Протоколы передачи ключей	Проработка учебного материала, подготовка к зачету	12	Зачет

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. Запечников, С. В. Криптографические методы защиты информации : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblionline.ru/bcode/433133>
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. 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. Лабораторный практикум по криптографическим протоколам / С. М. Рацеев; УлГУ, ФМИАТ, Каф. информ. безопасности и теории управления. - Ульяновск : УлГУ, 2019. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/1344>
3. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Криптографические протоколы» 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/13335>.

Согласовано:

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

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

б) Программное обеспечение

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования на языках Си/C++ (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:

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

<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.

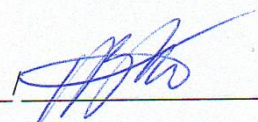
6.2. **Российское образование** : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: <http://www.edu.ru>. – Текст : электронный.

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

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 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. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус

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/C++ (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



подпись



ФИО