УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Безопасность открытых информационных систем**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	5 - очная форма обучения

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем Форма обучения: очная _____
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 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
Сутыркина Екатерина Алексеевна	Кафедра информационной безопасности и теории управления	Доцент,Кандидат физико-математических наук

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- изучение основных уязвимостей открытых информационных систем;

- освоение методов и средств защиты ОИС;

Задачи освоения дисциплины:

- формирование у студентов навыков экспертизы качества и надёжности реализации открытых информационных систем;

- знакомство студентов с программно-аппаратными средствами обеспечения безопасности открытых информационных систем;

- развитие навыков обеспечения высокой степени защиты открытых информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность открытых информационных систем» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-5.2., ОПК-5.3..

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: .

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах;	**знать**: современные методы и технологии аудита защищённых приложений ОИС, основные угрозы, уязвимости и методы защиты информации в ОИС **уметь**: проводить контроль обеспечения ИБ и верификации данных в ОИС **владеть**: навыками проведения контроля обеспечения ИБ и верификации данных в ОИС
ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных	**знать**: классификацию типовых удалённых атак на ОИС и

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
систем;	основные методы защиты от них, основные способы и правила применения основных программных и аппаратных средств защиты информации в ОИС, модели атак, направленных на преодоление защиты ОИС **уметь**: разрабатывать защищённые приложения ОИС **владеть**: навыками комплексного проектирования, обслуживания и анализа ОИС с точки зрения обеспечения ИБ

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 5 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 180 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		9
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	90	90
Аудиторные занятия:	90	90
Лекции	36	36
Семинары и практические занятия	18	18
Лабораторные работы, практикумы	36	36
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Экзамен (18)	Экзамен
Всего часов по дисциплине	180	180

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	8
Раздел 1. Угрозы безопасности открытых информационных систем и средства защиты от НСД							
Тема 1.1. Структура ОИС	4	2	0	0	0	2	Тестирование
Тема 1.2. Модели угроз кибербезопасности	10	4	0	2	0	4	Тестирование
Тема 1.3. Эволюция угроз	10	2	0	4	0	4	Тестирование
Тема 1.4. Средства анонимизации в сети	14	4	0	4	0	6	Тестирование
Тема 1.5. Защита сети	14	2	4	4	0	4	Тестирование
Раздел 2. Безопасность на стороне клиента							
Тема 2.1. Google dorks	8	2	0	2	0	4	Тестирование
Тема 2.2. Межсайтовый скриптинг	12	4	0	4	0	4	Тестирование
Тема 2.3. Куки и сессии	8	2	0	2	0	4	Тестирование
Тема 2.4. Прогрессивные атаки	12	2	4	2	0	4	Тестирование
Раздел 3. Безопасность на стороне сервера							
Тема 3.1. Подмена запросов	12	4	0	4	0	4	Тестирование

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	8
Тема 3.2. Инъекции в БД	18	2	8	4	0	4	Тестирование
Раздел 4. Способы выявления атак и тестирование ПО.							
Тема 4.1. Анализ и защита от анализа кода.	10	2	0	4	0	4	Тестирование
Тема 4.2. Современные инструменты анализа на проникновение ОИС	12	4	2	0	0	6	Тестирование
Итого подлежит изучению	144	36	18	36	0	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Угрозы безопасности открытых информационных систем и средства защиты от НСД

Тема 1.1. Структура ОИС

7 уровней OSI, модель TCP\IP. Оборудование и протоколы на каждом из уровней. Вектора атак на нижних и верхних уровнях.

Тема 1.2. Модели угроз кибербезопасности

Модель нарушителя, построение модели угроз для заданной ИС. Классификация пентестеров. Известные примеры реализации атак.

Тема 1.3. Эволюция угроз

Вирусология. История появления зловредов, их классификация. Разновидности вирусов, современные зловреды. Основные причины заражения и способы защиты от НСД.

Тема 1.4. Средства анонимизации в сети

Анонимные сети. Приватный режим. VPN, прокси, TOR.

Тема 1.5. Защита сети

Виды и настройка межсетевых экранов.

Раздел 2. Безопасность на стороне клиента

Тема 2.1. Google dorks

Поиск конфиденциальной информации в сети и способы защиты от утечек.

Тема 2.2. Межсайтовый скриптинг

Понятие эксплойта. Отраженные, внедрённые и DOM атаки XSS . Обход фильтра XSS. Экспоненциальные атаки XSS.

Тема 2.3. Куки и сессии

Угон куки, подмена токена, Фальсификация межсайтовых запросов.

Тема 2.4. Прогрессивные атаки

Человек посередине (Man-In-The-Middle). SideJacking. Атака Man-In-The-Browser.

Раздел 3. Безопасность на стороне сервера

Тема 3.1. Подмена запросов

XXE, request smuggling, command injection, SSTI. ARP-spoofing. Использование фальсификации заголовков запросов.

Тема 3.2. Инъекции в БД

SQL Injection (SQLi). Черные ходы в медиа-файлах. Атаки "Drive-by Download".

Раздел 4. Способы выявления атак и тестирование ПО.

Тема 4.1. Анализ и защита от анализа кода.

Черный, белый, серый ящики. Обфускация, трассировка и деобфускация кода.

Тема 4.2. Современные инструменты анализа на проникновение ОИС

Знакомство с Kali Linux. Длинный путь в Penetration Testing: с чего начать и куда смотреть.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Угрозы безопасности открытых информационных систем и средства защиты от НСД

Тема 1.5. Защита сети

Раздел 2. Безопасность на стороне клиента

Тема 2.4. Прогрессивные атаки

Раздел 3. Безопасность на стороне сервера

Тема 3.2. Инъекции в БД

Раздел 4. Способы выявления атак и тестирование ПО.

Тема 4.2. Современные инструменты анализа на проникновение ОИС

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Разработка модели угроз
Цели: ознакомление с моделями угроз, понятием вектора атак и модели нарушителя.
Содержание: анализ предложенной информационной системы, анализ актуальных угроз согласно классификации ФСТЭК, расчет уровня опасности той или иной угрозы.
Результаты: таблица модели угроз для рассматриваемой информационной системы.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
Вирусы: создание и обнаружение
Цели: : знакомство со способами написания простейших зловредов, их безопасной инициализации и обнаружения.
Содержание: написание программы, блокирующей действия пользователя, знакомство с «песочницей», распознавание антивирусным ПО созданной программы.
Результаты: программа, реализующая решение поставленной задачи.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
Анонимность в Internet
Цели: знакомство с основными средствами повышения анонимности в сети.
Содержание: основные моменты настройки прокси, виртуальной частной сети и установки TOR, установление уровня распознавания пользователя по отпечатку браузера.
Результаты: модификация браузера с помощью плагинов, серфинг с помощью браузера TOR
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
Межсетевые экраны
Цели: знакомство со средствами фильтрации трафика на стороне сервера и клиента.
Содержание: установка и настройка пакетного межсетевого экрана.
Результаты: настроенный межсетевой экран, удовлетворяющий требованиям фильтрации
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085

Поиск и защита конфиденциальной информации
Цели: знакомство с техникой, используемая СМИ, следственными органами, инженерами по безопасности и любыми пользователями для создания запросов в различных поисковых системах для обнаружения скрытой информации и уязвимостях, которые можно обнаружить на общедоступных серверах.
Содержание: Поиск уязвимых служб и паролей в открытых логах в Гугле при помощи дорков.
Результаты: информация в виде списка адресов, электронной почты, картинок или перечня веб-камер в открытом доступе.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
XSS и способы предотвращения
Цели: знакомство с атаками на веб-системы.
Содержание: тестирование на возможность внедрения вредоносного кода на определённую страницу.
Результаты: полезная нагрузка для реализации эксплойта и перечень мер по предотвращению атаки.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
Куки и сессии
Цели: знакомство со способами безопасной передачи данных в браузере.
Содержание: получение куков и токена пользователя на определённой странице без использования специального ПО.
Результаты: авторизация с административными правами на тестовой странице.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
MITM и MITB
Цели: знакомство с атакой компрометации канала связи, при которой взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию..
Содержание: перехват трафика между клиентом и веб-сервером.
Результаты: предоставление данных, отправленных клиентом.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
Подмена запросов
Цели: знакомство с инъекционными атаками на стороне сервера.
Содержание: удаленное исполнение кода.
Результаты: использование Postman для отчета.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
SQLi и sqlmap
Цели: построение защиты от реализации инъекций в БД.
Содержание: анализ на уязвимость к инъекции SQL тестовых страниц веб-приложений.
Результаты: получение данных из базы данных
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085
Обфускаторы и анализ кода
Цели: знакомство с инструментами, обеспечивающими защиту от реверс-инжиниринга и способами тестирования приложений.
Содержание: обфускация и деобфускация скрипта
Результаты: деобфусцированная программа, функционал которой изменен под нужды программиста.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7085

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. 7 уровней OSI, особенности функционирования уровней.
2. Модель TCP\IP, особенности формирования пакетов.
3. Сравнительная характеристика эталонной модели и TCP\IP.
4. Протоколы передачи данных на нижних уровнях TCP\IP.
5. Протоколы передачи данных на прикладном уровне TCP\IP.
6. Вектора атак на нижних уровнях TCP\IP.
7. Уязвимости пользовательских приложений.
8. Модель нарушителя. Алгоритм построение модели нарушителя для ИС.
9. Примеры фишинговых атак.
10. Основные причины заражения и способы защиты ИС от НСД.
11. Разновидности вирусов и современные зловреды.
12. История появления и становления вирусописания.
13. Способы анонимизации в сети Internet.
14. Прокси и VPN.
15. Виды межсетевых экранов
16. Сканеры уязвимостей.
17. Формирование поисковых запросов с помощью специальных выражений.
18. Поиск открытых умных устройств в сети и правила настройки для обеспечения безопасности.
19. Понятие эксплойта. Виды кроссайтовых скриптов, способы защиты.
20. Использование белых и черных списков для формирования атаки xss
21. Понятие cookies. Способы угона кук.
22. Обход защиты с токеном для кражи куков админа
23. Атаки «Человек посередине».
24. Пути к эффективному процессу управления безопасностью открытой информационной системы.
25. Безопасность серверов. Основные вектора атак.
26. Возможные векторы атаки на объект защиты: лобовое, интерактивное и физическое воздействие злоумышленника.
27. Инъекции в БД. Разновидности SQLi, ПО для тестирония на проникновение.
28. Математическая модель потенциального нарушителя. Определение вероятности (коэффициента готовности) реализовать угрозу атаки потенциальным нарушителем.
29. Тестирование на основе черного, белого и серого ящиков.
30. Обфускация и деобфускация кода. Инструментарий кодокопателей.
31. Современные инструменты специалиста по информационной безопасности.
32. Этическая сторона вопроса пентеста.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Угрозы безопасности открытых информационных систем и средства защиты от НСД			
Тема 1.1. Структура ОИС	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Вопросы к экзамену, Тестирование
Тема 1.2. Модели угроз кибербезопасности	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 1.3. Эволюция угроз	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 1.4. Средства анонимизации в сети	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Вопросы к экзамену, Тестирование
Тема 1.5. Защита сети	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Раздел 2. Безопасность на стороне клиента			
Тема 2.1. Google dorks	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 2.2. Межсайтовый скриптинг	Проработка учебного материала с использованием ресурсов учебно-	4	Вопросы к экзамену, Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
	методического и информационного обеспечения дисциплины.		
Тема 2.3. Куки и сессии	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 2.4. Прогрессивные атаки	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Раздел 3. Безопасность на стороне сервера			
Тема 3.1. Подмена запросов	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 3.2. Инъекции в БД	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Раздел 4. Способы выявления атак и тестирование ПО.			
Тема 4.1. Анализ и защита от анализа кода.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 4.2. Современные инструменты анализа на проникновение ОИС	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Вопросы к экзамену, Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы
основная

1. Мартемьянов Ю.Ф. Операционные системы. Концепции построения и обеспечения безопасности :

учебное пособие / Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев ; Мартемьянов Ю.Ф.; Яковлев Ал.В.; Яковлев Ан.В. - Москва : Горячая линия - Телеком, 2010. - 332 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991201285.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0128-5. / .— ISBN 0_242489

2. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский ; В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. - Брянск : Брянский государственный технический университет, 2012. - 224 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Весь срок охраны авторского права. - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/7007.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-89838-488-3. / .— ISBN 0_119401

дополнительная

1. Ракитин, Р. Ю. Компьютерные сети : учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко ; Р. Ю. Ракитин, Е. В. Москаленко. - Барнаул : Алтайский государственный педагогический университет, 2019. - 338 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Гарантированный срок размещения в ЭБС до 07.01.2026 (автопролонгация). - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/102731.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-88210-942-3. / .— ISBN 0_157538

2. Климентьев К.Е. Компьютерные вирусы и антивирусы: взгляд программиста : монография / К.Е. Климентьев ; Климентьев К.Е. - Москва : ДМК-пресс, 2013. - 656 с. - URL: https://www.studentlibrary.ru/book/ISBN9785940748854.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-94074-885-4. / .— ISBN 0_243268

учебно-методическая

1. Сутыркина Е. А. Методические указания для самостоятельной работы студентов по дисциплине «Безопасность открытых информационных систем» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / Е. А. Сутыркина ; УлГУ, Фак. математики, информ. и авиац. технологий. - 2019. - Загл. с экрана. - Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 2,81 МБ). - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_40621.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Альт рабочая станция

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. 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.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

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	Кандидат физико-математических наук	Сутыркина Екатерина Алексеевна
	Должность, ученая степень, звание	ФИО