УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от « 18 » мая 2021 г., протокол № 4/21
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
« 18 » мая 2021г

РАБОЧАЯ ПРОГРАММА

Дисциплина	Анализ уязвимостей программного обеспечения
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 2021г.

Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ 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	ИБиТУ	доцент, к.ф-м.н

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
/ _____ / Андреев А.С. / *(подпись) (Ф.И.О.)* « 12 » 05 2021 г.	/ _____ / Андреев А.С. / *(подпись) (Ф.И.О.)* « 12 » 05 2021 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Анализ уязвимостей программного обеспечения» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию системного и аналитического мышления.

Цели освоения дисциплины:

- изучение студентом основных видов уязвимостей программного обеспечения;
- освоение основных методов и средств анализа и устранения уязвимостей программных реализаций;

Задачи освоения дисциплины:

– развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций;

– формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;

– формирование навыков анализа программных реализаций на предмет наличия уязвимостей;

– развитие навыков организации антивирусной защиты

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части дисциплин по выбору Б1.В.ДВ в рамках образовательной программы и читается в 10-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов «Системный анализ», «Дополнительные главы криптографии», «Вредоносные программы в компьютерных сетях».

Основные положения дисциплины используются в дальнейшем при прохождении практик, сдаче ВКР и сдаче государственного экзамена.

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

Процесс изучения дисциплины «Анализ уязвимости программ» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-1 Способен формировать комплекс мер для защиты информации ограниченного доступа, управлять процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	Знать: специальные средства защиты в современных средах программирования Уметь: строить соответствующие математические модели Владеть: способами оценки и прогнозирования работы моделей безопасности
ПК-2 Способен осуществлять тестирование систем защиты информации компьютерных систем	Знать: основные средства и методы анализа программных реализаций на предмет уязвимостей Уметь: разрабатывать программы с защитой от

	уязвимостей Владеть: навыками выявления и устранения уязвимостей
ПК-3 Способен разрабатывать проектные решения по защите информации в компьютерных системах	Знать: статические и динамические методы анализы программных реализаций Уметь: выбирать адекватный инструмент для оценки эффективности безопасности ПО Владеть: способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 2.

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		
Аудиторные занятия:				
• Лекции	20	20		
• Практические и семинарские занятия				
• Лабораторные работы (лабораторный практикум)	20	20		
Самостоятельная работа	32	32		
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, тестирование		
Курсовая работа				
Экзамен				
Всего часов по дисциплине	72	72		

Виды промежуточной аттестации (экзамен, зачет)		зачет		
Общая трудоемкость в зач. ед.	2	2		

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. Безопасность и уязвимости КС							
1. Модели угроз кибербезопасности	2	1			1	1	тестирование
2. Средства анонимизации в сети	5	2			1	3	тестирование
3. GOOGLE дорки	6	1		2	2	3	лабораторная работа 1, тестирование
Раздел 2. Уязвимости Frontend							
4. Внедрение межсайтовых запросов	8	2		2	2	4	лабораторная работа 2, тестирование
5. Токены и куки	7	2		2	2	3	лабораторная работа 3, тестирование
Раздел 3. Уязвимости Backend							
6. Фальсификация и подмена заголовков запросов и политика безопасности в браузере	6	2		2	2	2	лабораторная работа 4, тестирование
7. Загрузка файлов	7	2		2	2	3	лабораторная работа 5, тестирование
8. Инъекции в БД	8	2		2	2	4	лабораторная работа 6, тестирование
Раздел 4. Уязвимости ОС							
9. Повышение прав в Windows, MAC OS	8	2		2	2	4	лабораторная работа 7, тестирование
10. Безопасность мобильных телефонов.	8	2		2	2	4	лабораторная работа 8, тестирование

Раздел 5. Этичный хакинг							
11. Взлом сайта	9	1		4	1	4	лабораторная работа 9, тестирование
12. Пентестинг этика	2	1			1	1	тестирование
Зачеты							
Итого	72	20		20	(20*)	32	

*-занятия проводятся в интерактивной форме

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Безопасность и уязвимости КС

Тема 1. Модели угроз кибербезопасности. Модель нарушителя, построение модели угроз для заданной ИС. Классификация пентестеров. Известные примеры реализации атак.

Тема 2. Средства анонимизации в сети. Анонимные сети. Приватный режим. VPN, прокси, TOR.

Тема 3. GOOGLE дорки. Поиск конфиденциальной информации в сети без спец.средств и способы защиты от утечек.

Раздел 2. Уязвимости Frontend

Тема 4. Внедрение межсайтовых запросов. Понятие эксплойта. Отраженные, внедрённые и DOM атаки XSS . Обход фильтра XSS. Экспоненциальные атаки XSS.

Тема 5. Токены и куки. Угон куки, подмена токена,

Раздел 3. Уязвимости Backend

Тема 6. Фальсификация и подмена заголовков запросов. Фальсификация межсайтовых запросов. CORS, Samesite coockie, request smuggling, command injection, SSTI. ARP-spoofing.

Тема 7. Загрузка файлов. XXE, Черные ходы в медиа-файлах. Атаки "Drive-by Download".

Тема 8. Инъекции в БД. SQLi: вручную и с использованием инструментов автоматизации.

Раздел 4. Уязвимости ОС

Тема 9. Повышение прав в Windows, MAC OS. Способы несанкционированного повышения привилегий пользователя и способы защиты.

Тема 10. Безопасность мобильных телефонов. Как защитить свой телефон от хакеров и кибератак. Антивирусы. Разрешения приложений. Антикриминалистика. Как защитить смартфон от извлечения данных.

Раздел 5. Этичный хакинг

Тема 11. Взлом сайта. Анализ на проникновение на примере тестового веб-ресурса с использование инструментов Kali.

Тема 12. Пентестинг этика. Длинный путь в Penetration Testing: с чего начать и куда смотреть.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторная работа 1. Поиск и защита конфиденциальной информации
Цель: 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.
Результат: информация в виде списка адресов, электронной почты, картинок или перечня веб-камер в открытом доступе.

Лабораторная работа 2. XSS и способы предотвращения
Цель: знакомство с атаками на веб-системы.
Содержание: тестирование на возможность внедрения вредоносного кода на определённую страницу.
Результат: полезная нагрузка для реализации эксплойта и перечень мер по предотвращению атаки.

Лабораторная работа 3. Анализ уязвимостей уникальных идентификаторов
Цель: знакомство со способами безопасной передачи данных в браузере.
Содержание: получение куков и токена пользователя на определённой странице без использования специального ПО.
Результат: авторизация с административными правами на тестовой странице.
Лабораторная работа 4. Подмена запросов
Цель: знакомство с инъекционными атаками на стороне сервера.
Содержание: удаленное исполнение кода.
Результат: использование BurpSuite для отчета.

Лабораторная работа 5. Загрузка зараженных файлов
Цель: Изучение способов внедрения файлов на сервер и способы взаимодействия с ними.
Содержание: создание заведомо вредоносного файла и изучение возможности загрузки его на тестовый веб-ресурс
Результат: удаленное исполнение кода

Лабораторная работа 6. SQLi и sqlmap
Цель: построение защиты от реализации инъекций в БД.
Содержание: анализ на уязвимость к инъекции SQL тестовых страниц веб-приложений.
Результат: получение данных из базы данных.

Лабораторная работа 7. Повышение прав в операционных системах
Цель: изучение способов обхода защиты несанкционированного повышения привилегий пользователя до администратора и супер-администратора
Содержание: исследовать систему на возможность повышения прав

Результат: действия в системе, характерные для пользователя с повышенными привилегиями.

Лабораторная работа 8. Защита данных от извлечения на iOS и Android.

Цель: ознакомиться со способами защиты персональной информации на мобильном устройстве.

Содержание работы: изменение настроек мобильного телефона для максимальной защиты от антикриминалистической экспертизы.

Результат: мобильное устройство, максимально защищенное от угрозы извлечения данных третьими лицами.

Лабораторная работа 9. Анализ уязвимостей тестового веб-ресурса
Цель: знакомство с особенностями работы этичного хакера
Содержание: исследование веб-ресурса на наличие уязвимостей и возможности их эксплуатации
Результат: райтап по проделанной работе и список выявленных уязвимостей

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

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

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (ЗАЧЕТУ)

1. Модель нарушителя. Алгоритм построение модели нарушителя для ИС?
2. Основные причины заражения и способы защиты ИС от НСД.
3. Способы анонимизации в сети Internet.
4. Прокси и VPN.
5. Виды межсетевых экранов.
6. Формирование поисковых запросов с помощью специальных выражений.
7. Как организована атака MAC-flooding?
8. Как происходит подмена субдомена DNS? Сокращения названий субдоменов DNS.
9. Что такое Potentially Unwanted Program (PUP - потенциально нежелательная программа)?
10. Как атакуют WEB-серверы? Какие существуют способы встраивания вредоносного кода на страницу?
11. Что такое «Атаки нулевого дня». Что делают разработчики, узнав о таких атаках? Как узнать, что обнаружена уязвимость и как её закрыть?
12. Что такое Adware (Madware) и Grayware?
13. Как реализуются Hijackers –атаки?
14. Что такое Ransomware, Scareware и Rouge Security (rogueware)?
15. Какие виды Cross-Site Scripting (XSS) вам известны? Как они реализуются и как от них защититься?
16. Как происходит взлом WEB-приложений с помощью "отравленных" Cookie?
17. Понятие cookies. Способы угона кук.
18. Атаки «Человек посередине».
19. Безопасность серверов. Основные вектора атак.
20. Кликеры Clickjacking и likejecking, что это?
21. Угрозы на стороне сервера. SQL Injection (SQLi).
22. Что такое ARP-spoofing и фальсификация межсайтовых запросов CSRF.

23. Как использовать черные ходы в медиа-файлах?
24. Разновидности атаки «Человек посередине (Man-In-The-Middle).»
25. Какие имеются скрытые угрозы безопасности?
26. Современные инструменты специалиста по информационной безопасности.
27. Этическая сторона вопроса пентеста.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

В рамках самостоятельной работы студентам выделяется время на:

– теоретическую подготовку по дисциплине посредством изучения тематической литературы (базовой, дополнительной) и конспектов лекций по дисциплине;

– практическую подготовку по дисциплине посредством выполнения лабораторных работ;

– подготовку к сдаче итогового зачета по дисциплине.

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Модели угроз кибербезопасности	Проработка учебного материала, подготовка к сдаче зачета,	1	Тестирование, зачет,
2. Средства анонимизации в сети	Проработка учебного материала, подготовка к сдаче зачета,	3	Тестирование, зачет,
3. GOOGLE дорки	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	3	Тестирование, зачет, лабораторная работа
4. Внедрение межсайтовых запросов	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	Тестирование, зачет, лабораторная работа
5. Токены и куки	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	3	Тестирование, зачет, лабораторная работа
6. Фальсификация и подмена заголовков запросов и политика безопасности в браузере	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	2	Тестирование, зачет, лабораторная работа
7. Загрузка файлов	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	3	Тестирование, зачет, лабораторная работа
8. Инъекции в БД	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	Тестирование, зачет, лабораторная работа
9. Повышение прав в Windows, MAC OS	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	Тестирование, зачет, лабораторная работа
10. Безопасность мобильных телефонов.	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	Тестирование, зачет, лабораторная работа
11. Взлом сайта	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	Тестирование, зачет, лабораторная работа
12. Пентестинг этика	Проработка учебного материала, подготовка к сдаче зачета,	1	Тестирование, зачет,

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Платонов Владимир Владимирович. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для вузов по спец. 090102 "Компьютерная безопасность", 090105 "Комплекс. обеспечение информ. безопасности автоматизир. систем" / Платонов Владимир Владимирович. - Москва : Академия, 2006
2. Щербаков А.Ю., А.Ю. Щербаков. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с. - ISBN 978-5-8041-0378-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785804103782.html
3. *Внуков, А. А.* Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/444046

дополнительная

1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/437163

Учебно-методическая

1. Сутыркина Е. А. Методические указания к лабораторным работам по дисциплине «Анализ уязвимостей программного обеспечения» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / Е. А. Сутыркина; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 1,10 МБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/5603

Согласовано:

Гл. библ-рь НБ УлГУ	Попова И.Ю.	
должность сотрудника научной библиотеки	ФИО	подпись

б) Программное обеспечение

МойОфис Стандартный, Альт Рабочая станция 8.

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

- Wireshark,
- python,
- Oracle VM VirtualBox
- Kali

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва , [2019]. - Режим доступа: https://www.biblio-online.ru.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.

1.5. Znanium.com [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

Согласовано:

зам нач УИТ / Ключкова ВВ / _____

должность сотрудника УИТиТ | ФИО | подпись

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.

Аудитория 24б для проведения лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 11 персональных компьютеров, проектор, экран, системы защиты информации: Соболь, Аккорд, Dallas Lock, Secret Net Studio. Сервер Vimark, АПКШ "Континент", Маршрутизаторы Cisco, Система защиты информации ViPNet. 432017, Ульяновская обл, г Ульяновск, ул Набережная реки Свияги, д 106-2 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:

- Wireshark,
- python,
- Oracle VM VirtualBox
- Kali

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 некоторые 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: _____ доцент _____ Сутыркина Екатерина Алексеевна
подпись должность ФИО