УТВЕРЖДЕНО
решением Ученого совета ФМИАТ
от «16» мая 2023 г., протокол № 4/23
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
«16 мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	3

Специальность: 10.05.03 "Информационная безопасность автоматизированных систем"
(код специальности (направления), 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 2023 г.

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

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
/ _____ / Андреев А.С. / *(подпись)* *(Ф.И.О.)* « 12 » 05 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Дисциплина «Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа» является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Дисциплина реализует требования профессионального стандарта «Специалист по технической защите информации" и направлена на получение студентами знаний, умений и навыков по вопросам технической защиты конфиденциальной информации (ТЗКИ) от несанкционированного доступа (НСД).

Задачи освоения дисциплины:

изучить основные методы и средства ТЗКИ от НСД;

обеспечить освоение студентами умений и навыков по вопросам ТЗКИ от НСД.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа» изучается в 6 семестре и относится к дисциплинам блока Б1.В. Дисциплина основывается на знаниях, полученных при изучении дисциплин «Основы информационной безопасности», «Профессиональный электив. Организационно-правовые основы технической защиты конфиденциальной информации», «Организационное и правовое обеспечение информационной безопасности».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

- знание базовых профессиональных понятий и определений в области информационной безопасности;
- способность использовать нормативные правовые документы;
- способность использовать основные положения и методы социальных и гуманитарных наук;
- способность анализировать социально-значимые проблемы и процессы.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Безопасность операционных систем», «Безопасность вычислительных сетей», «Защита информации от утечки по техническим каналам», «Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации», а также в ходе всех видов практик и в повседневной деятельности.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ПК-7 - Способен проводить работы по техническому обслуживанию защищён-ных технических средств обработки информации	**Знает:** Технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации

	Порядок устранения неисправностей технических средств обработки информации в защищенном исполнении и организации их ремонта **Умеет:** Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией Проводить устранение выявленных неисправностей защищенных технических средств обработки информации **Владеет:** Навыками проведения технического обслуживания защищенных технических средств обработки информации
ПК-8 - Способен проводить работы по установке, настройке и испытаниям технических средств обработки информации	**Знает:** Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и эксплуатации защищенных технических средств обработки информации. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электро-питания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах. Способы защиты информации от утечки по техническим каналам **Умеет:** Проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами. Производить установку и монтаж защищенных технических средств обработки информации **Владеет:** Навыками установки и монтажа защищенных технических средств обработки информации. Навыками настройки защищенных технических средств обработки информации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3.

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

Вид учебной работы	Количество часов (форма обучения очная)			
	Всего по плану	В т.ч. по семестрам		
		6		
Контактная работа обучающихся с преподавателем	54	54/54*		
Аудиторные занятия:	54	54/54*		
Лекции	18	18/18*		
Практические и семинарские занятия	18	18/18*		
Лабораторные работы (лабораторный практикум)	18	18/18*		
Самостоятельная работа	54	54		
Форма текущего контроля знаний и контроля самостоятельной работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на семинарах; - вопросы при защите лабора-торных работ		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	зачет	зачет		
Всего часов по дисциплине	108	108		

* 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 (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название и разделов и тем	Все-го	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практические занятия, семинары	Лабораторные работы			
Раздел 1. Угрозы безопасности информации, связанные с НСД							
1. Понятие и общая классификация угроз безопасности информации, связанных с НСД		2	2			4	Тесты Т1
2. Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах		2				2	Тесты Т2
3. Банк данных угроз безопасности информации, включающих базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах		2	6			6	Тесты Т3
Раздел 2. Меры и средства защиты информации от НСД							
4. Общая характеристика и классификация мер и средств защиты информации от НСД		2	2			4	Тесты Т4
5. Средства защиты информации от НСД		4	2	12		20	Тесты Т5
6. Общий порядок сертификации средств защиты информации от НСД		2	2			4	Тесты Т6
7. Определение факта доступа к файлам. доступ к данным со стороны процесса		2	2	6		10	Тесты Т7
8. Мероприятия по фи-		2	2			4	Тесты

зической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности							Т8
Итого:	108	18	18	18		54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Угрозы безопасности информации, связанные с НСД

Тема 1. Понятие и общая классификация угроз безопасности информации, связанных с НСД

Основные термины и определения в области НСД. Источники угроз безопасности информации. Модели угроз безопасности информации, связанных с НСД.

Тема 2. Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах

Методы выявления уязвимостей информационных систем. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем, в том числе средств защиты информации информационных систем.

Тема 3. Банк данных угроз безопасности информации, включающих базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах

Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE. Общая система оценки уязвимостей (стандарт CVSS).

Раздел 2. Меры и средства защиты информации от НСД

Тема 4. Общая характеристика и классификация мер и средств защиты информации от НСД

Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД.

Тема 5. Средства защиты информации от НСД

Межсетевые экраны, требования к ним и способы применения. Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации. Криптографические средства защиты информации. DLP-системы, их возможности и перспективы применения.

Тема 6. Общий порядок сертификации средств защиты информации от НСД

Стандарты по сертификации средств защиты информации от НСД. Порядок проведения сертификационных испытаний на соответствие классам защищённости СВТ. Отчетность по результатам испытаний.

Тема 7. Определение факта доступа к файлам. доступ к данным со стороны процесса

Основные способы определения факта доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа. Понятие электронного замка. Механизмы контроля аппаратной конфигурации ПЭВМ.

Тема 8. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности

Общая характеристика объекта информатизации. Система физической защиты объекта информатизации и отдельных технических средств. Основные мероприятия по физической защите объекта информатизации и отдельных технических средств.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Угрозы безопасности информации, связанные с НСД

Тема 1. Понятие и общая классификация угроз безопасности информации, связанных с НСД (семинар).

1. Основные термины и определения в области НСД.
2. Источники угроз безопасности информации.
3. Модели угроз безопасности информации, связанных с НСД.

Тема 3. Банк данных угроз безопасности информации, включающих базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах (семинар).

1. Общая характеристика Банка данных угроз безопасности информации

2. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

3. Методы выявления уязвимостей информационных систем. Порядок и содержание работ по анализу уязвимостей программного обеспечения информационных систем, в том числе средств защиты информации информационных систем

4. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE.

5. Общая система оценки уязвимостей (стандарт CVSS).

Раздел 2. Меры и средства защиты информации от НСД

Тема 4. Общая характеристика и классификация мер и средств защиты информации от НСД (семинар)**.**

1. Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе.

2. Классификация мер и средств защиты информации от НСД (управление доступом; регистрация и учет; обеспечение целостности; антивирусная защита; межсетевое экранирование и сегментирование сетей; анализ защищенности и обнаружение вторжений и т.д.)

Тема 5. Средства защиты информации от НСД (семинар)

1. Межсетевые экраны, требования к ним и способы применения.

2. Системы обнаружения вторжений, требования к ним и способы применения.

3. Средства антивирусной защиты, требования к ним и способы применения.

4. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа.

5. Средства регистрации и учета.

6. Средства (механизмы) обеспечения целостности информации.

7. Криптографические средства защиты информации.

8. DLP-системы, их возможности и перспективы применения.

Тема 6. Общий порядок сертификации средств защиты информации от НСД (семинар)

1. Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации

2. Порядок проведения сертификационных испытаний на соответствие классам защищенности СВТ.

3. Отчетность по результатам испытаний. **Тема 7.** Установка, настройка, эксплуатация и техническое обслуживание средств защиты информации от НСД (семинар)

Тема 7. Определение факта доступа к файлам. доступ к данным со стороны процесса (семинар)

1. Способы определения факта доступа

2. Журналы доступа. Критерии информативности журналов доступа

3. Механизмы контроля аппаратной конфигурации ПЭВМ

Тема 8. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности (семинар)**.**

1. Общая характеристика объекта информатизации.

2. Система физической защиты объекта информатизации и отдельных технических средств.

3. Основные мероприятия по физической защите объекта информатизации и отдельных технических средств.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 2. Меры и средства защиты информации от НСД

Тема 5. Средства защиты информации от НСД

Лабораторная работа № 1. (2 часа). Назначение и возможности встроенных межсетевых экранов (МЭ).

Цель: изучить возможности и научиться работать с встроенными МЭ. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей встроенных МЭ.

Лабораторная работа № 2. (4 часа). Системы обнаружения вторжений на примере Системы защиты от НСД «Dallas Lock».

Цель: изучить возможности Системы обнаружения вторжений «Dallas Lock» и научиться работать с ней. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей Системы обнаружения вторжений «**Dallas Lock**».

Лабораторная работа № 3. (2 часа). Средства антивирусной защиты.

Цель: изучить возможности выбранной системы антивирусной защиты и научиться работать с ней. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей выбранной системы антивирусной защиты.

Лабораторная работа № 4. (4 часа). Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа на примере Программно-аппаратного комплекса средств защиты информации от НСД “Аккорд–АМДЗ”.

Цель: изучить возможности и научиться работать с комплексом средств защиты от НСД. Результат: отчет. Методические указания: основное внимание должно быть уделено настройке, установке и практическому освоению возможностей Программно-аппаратного комплекса средств защиты информации от НСД.

Тема 7. Определение факта доступа к файлам. доступ к данным со стороны процесса

Лабораторная работа № 5. (6 часов). Назначение, возможности и порядок работы с системой SecretNet Studio.

Цель: изучить возможности и научиться работать с системой SecretNet Studio. Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей системы SecretNet Studio.

Все 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.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

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

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

1. Угрозы безопасности информации, связанные с НСД.
2. Методы анализа угроз безопасности информации.
3. Требования по защите информации от НСД.
4. Меры защиты информации от НСД.
5. Основные средства защиты информации от НСД.
6. Общая характеристика межсетевых экранов
6. Методы контроля защищенности информации от НСД.
7. Системы обнаружения вторжений, требования к ним и способы применения.
8. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа.
9. Средства регистрации и учета.
10. Средства (механизмы) обеспечения целостности информации.
11. Криптографические средства защиты информации.
12. DLP-системы, их возможности и перспективы применения.
13. Сканеры безопасности и их характеристика.
14. Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.
15. Классификация автоматизированных систем по требованиям защиты информации.
16. Способы контроля целостности программного обеспечения и аппаратных средств.
17. Способы и средства контроля доступа к автоматизированным системам и рабочему месту пользователя.

7. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Угрозы безопасности информации, связанные с НСД. Тема 1. Понятие и общая классификация угроз безопасности информации, связанных с НСД	Подготовка к лекции, семинару, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 1. Тема 2 Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах	Подготовка к лекции, подготовка к сдаче зачёта	2	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 1. Тема 3. Банк данных угроз безопасности информации, включающих базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах	Подготовка к лекции, семинару, подготовка к сдаче зачёта	6	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 2. Меры и средства защиты информации от НСД. Тема 4. Общая характеристика и классификация мер и средств защиты информации от НСД	Подготовка к лекции, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 2. Тема 5. Средства защиты информации от НСД	Подготовка к лекции, семинару, лабораторным работам, подготовка к сдаче зачёта	20	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 2. Тема 6. Общий порядок сертификации средств защиты информации от НСД	Подготовка к лекции, семинару, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты на семинаре, зачёт
Раздел 2. Тема 7. Установка, настройка, эксплуатация и техническое обслуживание средств защиты информации от НСД	Подготовка к лекции, семинару, лабораторным работам, подготовка к сдаче зачёта	10	Тесты перед лекцией, тесты на семинаре, зачёт

Раздел 2. Тема 8. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности	Подготовка к лекции, семинару, подготовка к сдаче зачёта	4	Тесты перед лекцией, тесты на семинаре, зачёт

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084

2. Гродзенский, Я. С. Информационная безопасность : учебное пособие / Гродзенский Я. С. - Москва : РГ-Пресс, 2020. - 144 с. - ISBN 978-5-9988-0845-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785998808456.html

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации". - URL: http://www.consultant.ru/document/cons_doc_LAW_61798

1.2 Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных". - URL: http://www.consultant.ru/document/cons_doc_LAW_61801

2.1 Иванцов А. М. Основы информационной безопасности : курс лекций : учебное пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем». Часть 2 / А. М. Иванцов, В. Г. Козловский; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2020. - Загл. с экрана. - Электрон. текстовые дан. (1 файл : 1,41 МБ). – URL: http://lib.ulsu.ru/MegaPro/Download/MObject/8697

2.2 Иванцов, А. М. Основы информационной безопасности : курс лекций : учебное пособие. Ч. 1 / А. М. Иванцов, В. Г. Козловский ; УлГУ, ФМИАТ. - Электрон. текстовые дан. (1 файл : 776 КБ). - Ульяновск : УлГУ, 2019. - Загл. с экрана. – URL: http://lib.ulsu.ru/MegaPro/Download/MObject/1396

3. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204248.html

учебно-методическая

1. Методические указания для самостоятельной работы студентов по дисциплине «Профессиональный электив. Методы и средства технической защиты конфиденциальной информации от несанкционированного доступа» для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов. - Ульяновск: УлГУ, 2022. - 15 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13989.

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. / _____ / 04.05.2023 /
должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

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

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.

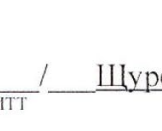
3.3. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

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

3.5. 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 / Щуренко Ю.В. /  / 04.05.2023

Должность сотрудника УИТТ | ФИО | подпись | дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;

Аудитории для проведения занятий — 2/24б, 3/317, 2/26.

Аудитории укомплектованы специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

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: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1.	Утверждение РПД и ФОС для набора 2023 года (10.05.01 и 10.05.03). Актуализация РПД и ФОС для наборов 2022 года 10.05.01 и 10.05.03 (без изменений)	Андреев А.С.		12.04.2023 Протокол заседания кафедры № 12
2.	Утверждение РПД и ФОС для набора 2024 года (10.05.03). Актуализация РПД и ФОС для наборов 2023 года 10.05.01 и 10.05.03 (без изменений)	Андреев А.С.		15.04.2024 Протокол заседания кафедры № 10