УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «15» мая 2023 г., протокол № 4/23
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
«15» мая 2023 г.

РАБОЧАЯ ПРОГРАММА

Дисциплина	Основы построения защищенных компьютерных сетей
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» сентября 2023 г.

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
Клочков Андрей Евгеньевич	ИБиТУ	Старший преподаватель

СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину
(подпись) Андреев А.С. / *(Ф.И.О.)*
«11» мая 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Целью изучения дисциплины «Основы построения защищенных компьютерных сетей» является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Задачи освоения дисциплины:

- изучение типовых угроз безопасности в компьютерных сетях;
- изучение криптографических и программно-аппаратных методов обеспечения
- информационной безопасности в компьютерных сетях;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
- овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Основы построения защищенных компьютерных сетей» относится к обязательной части Блока 1 «Дисциплины (модули)» Основной Профессиональной Образовательной Программы специалитета по специальности 10.05.01 – «Компьютерная безопасность», специализация «Математические методы защиты информации» (Б1.О.1.1.36).

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:
«Информатика» - знание основных понятий информатики;
«Языки программирования» - знание языков программирования высокого уровня и языка ассемблера персонального компьютера, владение навыками разработки, документирования, тестирования и отладки программ;
«Основы информационной безопасности» - знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации, владение профессиональной терминологией в области информационной безопасности;
«Операционные системы» - знание принципов построения современных операционных систем и особенностей их применения, владение навыками конфигурирования и администрирования операционных систем;
«Защита программ и данных» - знание основных средств и методов анализа программных реализаций, владение навыками анализа программных реализаций;
«Криптографические методы защиты информации» - знание основных видов симметричных и асимметричных криптографических алгоритмов, средств и методов хранения аутентификационной информации, владение криптографической терминологией.
Знания и практические навыки, полученные из дисциплины «Основы построения защищенных компьютерных сетей», используются студентами при разработке курсовых и дипломных работ.

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

Процесс изучения дисциплины «Основы построения защищенных компьютерных сетей»

направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	Знать: Основные виды угроз информационной безопасности компьютерных сетей; Механизмы практической реализации защиты информации; Особенности современных программно-аппаратных комплексов защиты информации. Уметь: Осуществлять поиск информации по работе компьютерных сетей; Правильно настраивать системы защиты информации для операционных систем; Настраивать работу компьютерной сети с применением средств защиты информации. Владеть: Навыками работы с современными реализациями механизмов защиты информации.
ОПК-13 – Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.	Знать: Основные системы защиты информации в компьютерных сетях; Существующие средства защиты информации в компьютерных сетях; Различные подходы к решению задач по защите компьютерных сетей; Методы реализации системы восстановления после сбоев. Уметь: Выявлять и ранжировать угрозы информационной безопасности; Комплексно применять механизмы защиты информации для компьютерных сетей; Настраивать работу компьютерной сети с применением средств защиты информации. Владеть: Терминологией по защите информации компьютерных сетей; Возможностями современного прикладного программного обеспечения для защиты компьютерных сетей.
ОПК-15 – Способен администрировать компьютерные сети и контролировать корректность их функционирования.	Знать: Руководящие документы по описанию системы защиты объекта информатизации; Механизмы проведения аудита информационной безопасности. Методы сбора журналов событий; Руководящие документы по организации защиты

	компьютерных сетей различного класса. Уметь: Формировать техническую документацию на защиту компьютерных сетей; Настраивать и анализировать журналы информационной безопасности.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

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**
		9
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	**72/72***	**72/72***
Аудиторные занятия	**72/72***	**72/72***
Лекции	**36/36***	**36/36***
Практические и семинарские занятия		
Лабораторные работы (лабораторный практикум)	**36/36***	**36/36***
Самостоятельная Работа	**36**	**36**
Форма текущего контроля знаний и контроля самостоятельной работы.	Лабораторные работы	Лабораторные работы
Курсовая работа	**0**	**0**
Контроль	**36**	**36**
Виды промежуточной аттестации	–	экзамен
Всего часов по дисциплине	**144**	**144**

**В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.*

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			

1	2	3	4	5	6	7	
Раздел 1. Типовые угрозы сетевой безопасности							
1. Сетевые атаки	12	4		4		4	Защита лабораторной работы
2. Механизмы реализации атак в сетях TCP/IP	12	4		4		4	Защита лабораторной работы
3. Методы перехвата сетевых соединений в сетях TCP/IP	12	4		4		4	Защита лабораторной работы
4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	12	4		4		4	Защита лабораторной работы
Раздел 2. Криптографические методы защиты информации в компьютерных сетях							
5. Криптографические протоколы обеспечения безопасности	12	4		4		4	Защита лабораторной работы
6. Защита виртуальных частных сетей (VPN)	12	4		4		4	Защита лабораторной работы
7. Разработка защищенных сетевых приложений.	12	4		4		4	Защита лабораторной работы
Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях							
8. Средства защиты локальных сетей при подключении к Интернет	12	4		4		4	Защита лабораторной работы
9. Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений	12	4		4		4	Защита лабораторной работы
Итого	108	36		36		36	
Контроль	36					36	
Всего	**144**						

5. СОДЕРЖАНИЕ КУРСА

Раздел 1. Типовые угрозы сетевой безопасности

Тема № 1. Сетевые атаки

Стадии проведения сетевой атаки. Классификация сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.

Тема № 2. Механизмы реализации атак в сетях TCP/IP

Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ.

Тема № 3. Методы перехвата сетевых соединений в сетях TCP/IP

Имперсонация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру.

Тема № 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак

Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак.

Раздел 2. Криптографические методы защиты информации в компьютерных сетях

Тема № 5. Криптографические протоколы обеспечения безопасности

Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

Тема № 6. Защита виртуальных частных сетей (VPN)

Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.

Тема № 7. Разработка защищенных сетевых приложений

Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.

Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях

Тема № 8. Средства защиты локальных сетей при подключении к Интернет

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.

Тема № 9. Защита серверов и рабочих станций.

Средства и методы предотвращения и обнаружения вторжений. Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы
противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell).

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Не предусмотрены учебным планом дисциплины.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторная работа №1. Строение сетей.

Цель. Изучение базовых механизмов получения информации о конфигурации сети. Получение навыков работы с различными программами, позволяющими определить конфигурацию сети или конфигурацию отдельного устройства в сети. Требуется для выполнения всех последующих лабораторных работ.

Лабораторная работа №2. Удалённый доступ по протоколу SSH.

Цель. Изучение возможностей протокола SSH для получения удалённого доступа к серверу. Применение функцию шифрования каналов связи при использовании протокола SSH.

Лабораторная работа №3. Использование VPN

Цель. Изучение возможностей программного обеспечения VPN для создания защищенных компьютерных сетей. Получение навыков работы со стандартным программным обеспечением для создания защищенных каналов связи.

Лабораторная работа №4. Работа с сертификатами SSL.

Цель. Изучение возможностей центров сертификации (Certificate Authorities). Получение навыков работы с криптографическими ключами. Применение встроенных систем шифрования информации в стандартных приложениях операционных систем.

Лабораторная работа №5. Моделирование виртуальной сети.

Цель. Ознакомление с методами моделирования сетей. Знакомство с телекоммуникационным оборудованием компании CISCO. Решение практических задач.

Лабораторная работа №6. Обнаружение вторжений

Цель. Изучение возможностей современного программного обеспечения для обнаружения вторжений. Управление правилами безопасности, анализ журналов событий.

Лабораторная работа №7. АПКШ «Континент» Обнаружение вторжений

Цель. Изучение возможностей комплекса АПКШ «Континент» для регистрации вторжений в локальную сеть.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (ЗАЧЕТУ)

1. Стадии проведения сетевой атаки.
2. Классификация сетевых угроз, уязвимостей и атак.
3. Атаки на реализации сетевых протоколов, отдельные узлы и службы.
4. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
5. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.
6. Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP.
7. Методы сканирования портов.
8. Методы обнаружения пакетных сниферов. Методы обхода МЭ.
9. Имперсонация вслепую. Десинхронизация TCP-соединений.
10. Атаки, направленные на сетевую инфраструктуру.
11. Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании.
12. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации.
13. Технические меры защиты от сетевых атак.
14. Протоколы аутентификации на прикладном уровне.
15. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS.
16. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.
17. Назначение, основные возможности, принципы функционирования и варианты реализации VPN.
18. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN.
19. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и
транспортном режимах.
20. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.
21. Аутентификация, шифрование, обеспечение целостности с использованием программного
интерфейса SSPI. Программный интерфейс OpenSSL.
22. Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности.
23. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ.
24. Достоинства и недостатки МЭ. Построение правил фильтрации.

25.Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений.
26.Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.
27.Системы обнаружения вторжений (СОВ).
28.Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы.
29.Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности.
30.Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий.
31.Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб.
32.Способы противодействия вторжениям.
33.Системы виртуальных ловушек (Honey Pot и Padded Cell).

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Типовые угрозы сетевой безопасности	Проработка учебного материала, выполнение лабораторных работ	16	Защита лабораторных работ
Раздел 2. Криптографические методы защиты информации в компьютерных сетях	Проработка учебного материала, выполнение лабораторных работ	12	Защита лабораторных работ
Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях	Проработка учебного материала, выполнение лабораторных работ	8	Защита лабораторных работ
	подготовка к сдаче экзамена	36	Экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102069.html. — Режим доступа: для авторизир. пользователей
2. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98200.html — Режим доступа: для авторизир. пользователей
3. Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. — Минск : Республиканский институт профессионального образования (РИПО), 2019. — 179 с.

3. Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. — Минск : Республиканский институт профессионального образования (РИПО), 2019. — 179 с — ISBN 978-985-503-947-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL:https://www.iprbookshop.ru/93384.html —

дополнительная

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/473348.
2. 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, 2021. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/471159.

учебно-методическая

1. Практикум по выполнению лабораторных работ по дисциплине Системы обнаружения вторжений в компьютерные сети / составители Д. В. Костин. —Москва: Московский технический университет связи и информатики, 2016. — 42 с.— Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. —URL: https://www.iprbookshop.ru/61546.html — Режим доступа: для авторизир. пользователей
2. Учебно-методическое пособие по выполнению курсового проекта по дисциплине «Методы и средства защиты информации в компьютерных сетях» / составители О. И. Шелухин. — Москва : Московский технический университет связи и информатики, 2015. — 35 с.— Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL:https://www.iprbookshop.ru/61741.html —Режим доступа: для авторизир. пользователей
3. Клочков А. Е. Методические указания для самостоятельной работы студентов по дисциплине «Основы построения защищенных компьютерных сетей» для студентов специалитета по специальности 10.05.01 очной формы обучения / А. Е. Клочков; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2019. -
Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан.
(1 файл : 260 КБ). - Текст : электронный http://lib.ulsu.ru/MegaPro/Download/MObject/8740
4. Клочков А.Е. Методические указания для выполнения лабораторных работ и самостоятельной работы студентов по дисциплине «Основы построения защищенных компьютерных сетей» для студентов специалитета по специальности 10.05.01 компьютерная безопасность, УлГУ,Ульяновск, 2021

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. /___/_04.05.2023_/
должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

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

- операционная среда ОС Windows 10, Microsoft Windows Server, BaseAlt (Альт Рабочая станция, Альт сервер), Kali.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. 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].

Согласовано:

Инженер ведущий	/ Щуренко Ю.В.	/	/ 04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитории для проведения лекций, практических занятий, выполнения лабораторных работ, для проведения текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций.

Аудитории для проведения лекций и практических занятий укомплектованы специализированной мебелью, учебной доской. Помещения для самостоятельной работы обеспечены Wi-Fi с доступом к сети «Интернет», электронной информационно-образовательной среде, электронно-библиотечной системе.

Помещение 2/24б. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций с набором демонстрационного оборудования для обеспечения тематических иллюстраций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 12). Экран настенный, мультимедийный проектор. Информационные плакаты. Компьютер, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106 (3 корпус).

Для выполнения лабораторных работ студенты используют несколько виртуальных машин с различными версиями операционных систем. Возможно самостоятельное выполнение лабораторных работ вне лаборатории. Компьютер с жестким диском – 100 Gb, ОЗУ: 8 Gb, Windows 10 Pro, BaseAlt (Альт Рабочая станция, Альт сервер), Kali Linux, Oracle Virtual Box, Putty, PGP, Apache, nginx, Statistica, Origin. По желанию студента все виртуальные машины могут быть развернуты на выделенном сервере виртуальных машин в лаборатории. Для моделирования работы сетей используется CISCO Packet Tracer. Сеть лаборатории представляет собой гетерогенную сеть, включающую в себя индивидуальный набор следующего оборудования:

1. Коммутатор L2, L3.
2. Маршрутизатор L3 с функциями VPN.
3. Маршрутизатор Континет КШ 25.
4. Маршрутизатор VipNet Координатор.

Для поддержания работы сетей используется выделенный Коммутатор L3, L3 сконфигурированный для работы независимых сегментов сети.

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: _____ ст. преподаватель кафедры Клочков Андрей Евгеньевич
подпись должность ФИО