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	**Виртуальные частные сети**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4

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
Иванцов Андрей Михайлович	Кафедра информационной безопасности и теории управления	Доцент, Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Дисциплина «Виртуальные частные сети» является одной из составляющих общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Дисциплина реализует требования федерального государственного образовательного стандарта высшего профессионального образования по специальности "Информационная безопасность автоматизированных систем". Цель курса – ознакомление студентов с основными техническими средствами построения виртуальных частных сетей.

Задачи освоения дисциплины:

изучить основы построения виртуальных частных сетей (VPN);

рассмотреть различные варианты и схемы создания VPN;

ознакомиться со стандартными протоколами VPN и управлением криптографическими ключами в VPN.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Виртуальные частные сети» относится к числу дисциплин блока Б1.В.1.ДВ.03, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ПК-1, ПК-2, ПК-3.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Математические модели информационных систем, Теория вычислительной сложности, Виртуальные частные сети, Сертификация средств защиты информации, Преддипломная практика, Технические средства обнаружения каналов утечки информации, Инструментальные средства контроля защищенности информации, Эксплуатационная практика, Подготовка к сдаче и сдача государственного экзамена, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Вейвлет-анализ, Системный анализ, Анализ уязвимостей программного обеспечения, Теория управления в информационных системах, Методы принятия оптимальных решений, Защита программ и данных, Функциональный анализ, Теоретико-числовые методы и алгоритмы, информационные технологии в автоматизированных системах, Модели безопасности компьютерных систем, Нелинейные динамические системы, Профессиональная этика, Аттестация объектов информатизации.

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**
ПК-2 Способен осуществлять тестирование систем защиты информации автоматизированных систем	**знать**: Принципы построения и функционирования систем и сетей передачи информации Эталонную модель взаимодействия открытых систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах **уметь**: Применять действующую нормативную базу в области обеспечения безопасности информации Контролировать безотказное функционирование технических средств защиты информации **владеть**: Навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем
ПК-3 Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**знать**: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем Принципы формирования политики информационной безопасности в автоматизированных системах **уметь**: Применять действующую нормативную базу в области обеспечения защиты информации Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе **владеть**: регламентирующих работу по защите информации Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-1 Способен организовать работы по выполнению в информационной системе требований защиты информации ограниченного доступа	**знать**: Источники и классификацию угроз информационной безопасности Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Нормативные правовые акты в области защиты информации **уметь**: Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	Организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях **владеть**: Навыками организации применения защищенных протоколов, межсетевых экранов и средств обнаружения вторжений для защиты информации в сетях Навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

4.2. Объем дисциплины по видам учебной работы (в часах): 72 часа

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		8
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54
Лекции	18	18
Семинары и практические занятия	-	-
Лабораторные работы, практикумы	36	36
Самостоятельная работа	18	18
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Оценивание реферата, Тестирование	Оценивание реферата, Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет (-18)	Зачет
Всего часов по дисциплине	72	72

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. Виртуальная частная сеть как средство защиты информации							
Тема 1.1. Введение в технологию виртуальных частных сетей (VPN)	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 1.2. Схема и политики безопасности VPN	16	2	0	12	4	2	Тестирование, Оценивание реферата
Тема 1.3. Стандартные протоколы создания VPN	20	4	0	12	6	4	Тестирование, Оценивание реферата
Раздел 2. Управление криптографическими ключами в виртуальных частных сетях							
Тема 2.1. Особенности управления ключевой системой асимметричных крипто систем. Инфрастуктура открытых ключей	4	2	0	0	0	2	Тестирование, Оценивание реферата
Тема 2.2. Сертификация открытых ключей	4	2	0	0	2	2	Тестирование, Оценивание реферата
Раздел 3. Построение виртуальной частной сети							
Тема 3.1. Требования к	4	2	0	0	0	2	Тестирование, Оценивани

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
продуктам построения виртуальных частных сетей. Варианты реализации							е реферата
Тема 3.2. Решения для построения виртуальных частных сетей	16	2	0	12	6	2	Тестирование, Оценивание реферата
Тема 3.3. Характеристика российских продуктов для создания виртуальных частных сетей.	4	2	0	0	0	2	Тестирование, Оценивание реферата
Итого подлежит изучению	72	18	0	36	18	18	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Виртуальная частная сеть как средство защиты информации

Тема 1.1. Введение в технологию виртуальных частных сетей (VPN)

Виртуальная частная сеть: основные понятия, цели создания, определения, подходы. Основные задачи технологии VPN. Специфика построения VPN. VPN в публичных сетях. Туннелирование в VPN. Протоколы механизма туннелирования.

Тема 1.2. Схема и политики безопасности VPN

Схема VPN. Алгоритм работы VPN-агентов. Функции VPN-агентов. Политики безопасности в VPN. Критерии безопасности VPN. Варианты создания VPN (защищённые каналы, частные каналы,

промежуточные каналы). Примеры политик безопасности VPN

Тема 1.3. Стандартные протоколы создания VPN

Уровни защищённых каналов. Семиуровневая модель взаимодействия открытых систем (OSI). Протоколы защиты данных канального уровня (PPTP, L2F и L2TP). Сравнительный анализ протоколов защиты на канальном уровне. Защита данных на сетевом уровне (Протокол IPSec). Протоколы туннельного и транспортного режимов. Защита на сеансовом уровне (Протоколы SSL, TLS, SOCKS).

Раздел 2. Управление криптографическими ключами в виртуальных частных сетях

Тема 2.1. Особенности управления ключевой системой асимметричных криптосистем. Инфрастуктура открытых ключей

Проблемы управления криптографическими ключами. Жизненный цикл ключей. Компрометация ключей. Управление секретными и открытыми ключами. Инфраструктура открытых ключей (ИОК). Модели APKI и PKIX.

Тема 2.2. Сертификация открытых ключей

Основные подходы к обеспечению безопасности открытых ключей. Содержание метода сертификации открытых ключей. Удостоверяющий центр. Сертификат открытого ключа. Формат сертификации открытого ключа. Аннулирование сертификатов. Модель инфраструктуры открытых ключей. Основные протоколы ИОК согласно модели PKIX. Закон РФ «Об электронной подписи».

Раздел 3. Построение виртуальной частной сети

Тема 3.1. Требования к продуктам построения виртуальных частных сетей. Варианты реализации

Характеристика основных средств построения VPN. Производительность. Управляемость. Совместимость. Поддержка справочной службы. Надёжность защиты и функциональная полнота. Реализация алгоритмов скоростной криптозащиты. Варианты реализации VPN. Шлюзы и клиенты VPN.

Тема 3.2. Решения для построения виртуальных частных сетей

VPN на базе сетевых операционных систем. VPN на базе маршрутизаторов. VPN на базе межсетевых экранов. VPN на базе специализированного программного обеспечения. VPN на базе аппаратных средств. Виды виртуальных частных сетей.

Тема 3.3. Характеристика российских продуктов для создания виртуальных частных сетей.

Аппаратно-программный комплекс «Континент». Программные продукты семейства «Застава». Продукты комплекса «VipNet». Семейство продуктов «Net-PRO». Продукты «Шип» и «Игла-2».

Сравнительный анализ российских продуктов.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Строение сетей
Цели: Изучение базовых механизмов получения информации о конфигурации сети
Содержание: Получение навыков работы с различными программами, позволяющими определить конфигурацию сети или конфигурацию отдельного устройства в сети. Требуется для выполнения всех последующих лабораторных работ. Задача. Все задачи необходимо выполнить на ОС MS Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер). • Для каждой из операционных систем установить следующее программное обеспечение: • Сканер безопасности Nmap (ZenMap - с графическим режимом) • Wireshark • Putty • whois • tranceroute • nslookup • Произвести анализ сайта 80.250.180.133. Обнаружить все открытые порты и протоколы. Составить схему расположения данного ресурса. Установить DNS имена расположенных на указанном IP адресе серверов. ь • Произвести подключение к серверу 62.76.32.162 по протоколу ssh (стандартный порт). • Произвести перехват пакетов ssh протокола направляемых к данному серверу при помощи Wireshark. Внимание! Необходимо показать перехват пакетов при получение первого ключа шифрования SSH. • Для обоих серверов указать номер автономной системы и её владельца. • Подключиться к WiFi сети университета. • Вычислить IP адрес шлюза выхода в Интернет. • Определить протокол шифрования трафика.
Результаты: Продемонстрированы навыки работы с базовыми механизмами получения информации о конфигурации сети
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7920
Удалённый доступ по протоколу SSH
Цели: Изучение возможностей протокола SSH для получения удалённого доступа к серверу. возможностей протокола SSH для получения удалённого доступа к серверу
Содержание: Задача №1. Все задачи необходимо выполнить на BaseAlt (Альт Рабочая станция, Альт сервер), с использованием ОС MS Windows в качестве клиентской операционной системы. • Установить систему openSSH сервер на ОС BaseAlt (Альт Рабочая станция, Альт сервер) и putty на ОС MS Windows. • Создать ключ серверного шифрования информации. • Установить соединение с данным сервером с другого клиента, на котором запущен WireShark. Перехватить ключ серверного шифрования. • Запретить передачу ключа по отрытому каналу. • Создать ключ клиента. • Записать ключ клиента на отчуждаемый носитель информации. • Установить соединение с другой ОС используя ключ клиента. Перехватить трафик и проанализировать полученные пакеты. Объяснить увиденный результат. • Создать ключи шифрования на клиенте используя puttyGen. Переписать их на отчуждаемый носитель. • Установить клиентские ключи шифрования для openSSH. • Произвести соединение с сервером. Задача №2. Все задачи необходимо выполнить на BaseAlt (Альт Рабочая станция, Альт сервер), с использованием ОС MS Windows в качестве клиентской операционной системы. • Отключить клиентский компьютер на ОС MS Windows от сети Интернет. • Настроить работы протокола SSH в режиме PORT FORWARDING. • Создать «проброс» порта из внутренней защищенной сети через сервер до сайта www.ulsu.ru и протоколов HTTP и HTTPS. Перехватить

отправленные пакеты с информацией и продемонстрировать использование шифрования информации
Результаты: Продемонстрированы возможности протокола SSH для получения удалённого доступа к серверу. возможностей протокола SSH для получения удалённого доступа к серверу
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7920
Использование VPN
Цели: Изучение возможностей программного обеспечения VPN для создания защищенных компьютерных сетей. Получение навыков работы со стандартным программным обеспечением для создания защищенных каналов связи.
Содержание: Задача №1. Создание защищенного межсетевого взаимодействия сетей. Изменить конфигурацию сети. 1. Скачать на локальный жесткий диск три образа операционных систем: MS Windows 10, MS Windows Server, BaseAlt (Альт Рабочая станция, Альт сервер). 2. Отключиться от общей сети лаборатории и включиться в один из маршрутизаторов MicroTik. 3. Назначить порты марштуризатора следующим образом: Порты №1,2 – VLAN1; Порты 3,4 – VLAN2; 4. Подключить виртуальные машины клиентских ОС к VLAN1. 5. Подключить виртуальную машину с сервером к VLAN2. 6. Создать ключи доступа и файлы конфигураций для клиентских компьютеров. 7. Установить VPN клиент и применить файлы конфигурации. 8. Передать файл по протоколу SMB в защищенной сети. Задача №2. Использование АПКШ «Континент» для создания защищенной сети. Изменить конфигурацию сети. 1. Подключить порт 3 к VLAN9. 2. Получить ключи шифрования для АПКШ «Континент» Сервер Доступа. 3. Подключить АПКШ «Континент» к VLAN1. 4. Настроить АПКШ «Континент» Сервер доступа в соответствии с руководством администратора. 5. Передать файл по протоколу SMB в защищенной сети.
Результаты: Изучены возможности программного обеспечения VPN для создания защищенных компьютерных сетей. Получены навыки работы со стандартным программным обеспечением для создания защищенных каналов связи.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/7920

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Темы рефератов

Тема 1. Туннелирование в виртуальных частных сетях
Тема 2. Общая характеристика VPN-технологии
Тема 3. Варианты построения виртуальных защищенных каналов
Тема 4. Политики безопасности в виртуальных частных сетях
Тема 5. Протоколы построения защищенных виртуальных сетей
Тема 6. Семиуровневая модель взаимодействия открытых систем (OSI)
Тема 7. Средства обеспечения безопасности виртуальных частных сетей
Тема 8. Назначение и использование сертификатов открытых ключей
Тема 9. Сертификация открытых ключей
Тема 10. Примеры отечественного и зарубежного построения VPN
Тема 11. Решения для построения виртуальных частных сетей
Тема 12. Характеристика и состав системы «Континент»
Тема 13. Характеристика и состав системы комплекса «ViPNet»
Тема 14. Аппаратно-программный комплекс «Континент»
Тема 15. Программные продукты семейства «Застава»

Тема 16. Семейство продуктов «Net-PRO»
Тема 17. Продукты «Шип» и «Игла-2»

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Виртуальная частная сеть: основные понятия, цели создания, определения, подходы

2. Основные задачи технологии VPN. Специфика построения VPN

3. VPN в публичных сетях

4. Туннелирование в VPN. Протоколы механизма туннелирования

5. Схема VPN. Алгоритм работы VPN-агентов. Функции VPN-агентов

6. Политики безопасности в VPN. Критерии безопасности VPN

7. Варианты создания VPN (защищённые каналы, частные каналы, промежуточные каналы). Примеры политик безопасности VPN

8. Уровни защищённых каналов. Семиуровневая модель взаимодействия открытых систем (OSI)

9. Протоколы защиты данных канального уровня (PPTP, L2F и L2TP). Сравнительный анализ протоколов защиты на канальном уровне

10. Протоколы туннельного и транспортного режимов. Защита на сеансовом уровне (Протоколы SSL, TLS, SOCKS)

11. Проблемы управления криптографическими ключами. Жизненный цикл ключей. Компрометация ключей

12. Модели APKI и PKIX

13. Основные подходы к обеспечению безопасности открытых ключей. Содержание метода сертификации открытых ключей

14. Модель инфраструктуры открытых ключей. Основные протоколы ИОК согласно модели PKIX

15. Модель инфраструктуры открытых ключей. Основные протоколы ИОК согласно модели PKIX

16. Требования к продуктам построения виртуальных частных сетей

17. Варианты реализации VPN

18. Шлюзы и клиенты VPN

19. VPN на базе сетевых операционных систем

20. VPN на базе маршрутизаторов

21. VPN на базе межсетевых экранов

22. VPN на базе специализированного программного обеспечения

23. VPN на базе аппаратных средств

24. Виды виртуальных частных сетей

25. Аппаратно-программный комплекс «Континент»

26. Программные продукты семейства «Застава»

27. Продукты комплекса «VipNet»

28. Продукты «Шип» и «Игла-2»

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. Виртуальная частная сеть как средство защиты информации			
Тема 1.1. Введение в технологию виртуальных частных сетей (VPN)	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 1.2. Схема и политики безопасности VPN	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 1.3. Стандартные протоколы создания VPN	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание реферата
Раздел 2. Управление криптографическими ключами в виртуальных частных сетях			
Тема 2.1. Особенности управления ключевой системой асимметричных криптосистем. Инфрастуктура открытых ключей	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 2.2. Сертификация открытых ключей	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Раздел 3. Построение виртуальной частной сети			
Тема 3.1. Требования к продуктам построения виртуальных частных сетей. Варианты реализации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата
Тема 3.2. Решения для построения виртуальных частных сетей	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата

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.)***
Тема 3.3. Характеристика российских продуктов для создания виртуальных частных сетей.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование, Оценивание реферата

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Запечников С.В. Основы построения виртуальных частных сетей : учебное пособие / С.В. Запечников, Н.Г. Милославская, А.И. Толстой ; Запечников С.В.; Милославская Н.Г.; Толстой А.И. - Москва : Горячая линия - Телеком, 2011. - 248 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991202152.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0215-2. / .— ISBN 0_242559

2. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов ; Душкин А.В.; Барсуков О.М.; Кравцов Е.В.; Славнов К.В. - Москва : Горячая линия - Телеком, 2016. - 248 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204705.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0470-5. / .— ISBN 0_250838

дополнительная

1. Внуков Андрей Анатольевич. Защита информации : Учебное пособие для вузов / А.А. Внуков ; Внуков А. А. - 3-е изд. ; пер. и доп. - Москва : Юрайт, 2020. - 161 с. - (Высшее образование). - URL: https://urait.ru/bcode/422772 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-07248-8 : 459.00. / .— ISBN 0_291692

2. Бизин Д. И. Виртуальные частные сети (VPN) : учебно-методическое пособие к выполнению лабораторных работ / Д. И. Бизин, О. Н. Коваленко ; Бизин Д. И., Коваленко О. Н. - Омск : ОмГУПС, 2019. - 37 с. - Утверждено методическим советом университета. - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции ОмГУПС - Информатика. - https://e.lanbook.com/book/165629. - https://e.lanbook.com/img/cover/book/165629.jpg. - Режим доступа: ЭБС "Лань"; для авторизир. пользователей. / .— ISBN 0_390415

3. Суворова Галина Михайловна. Информационная безопасность : Учебное пособие для вузов / Г.М. Суворова ; Суворова Г. М. - Москва : Юрайт, 2022. - 253 с. - (Высшее образование). - URL: https://urait.ru/bcode/496741 . - Режим доступа: Электронно-библиотечная система Юрайт, для

авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-13960-0 : 819.00. / .— ISBN 0_317760

учебно-методическая

1. Иванцов А. М. Методические указания для самостоятельной работы студентов по дисциплине «Виртуальные частные сети» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. М. Иванцов ; УлГУ, Фак. математики, информ. и авиац. технологий. - 2019. - Загл. с экрана. - Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 292 КБ). - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_41397.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Альт рабочая станция
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

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	Доцент, Кандидат технических наук, Доцент	Иванцов Андрей Михайлович
	Должность, ученая степень, звание	ФИО