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	Виртуальные частные сети
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

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.)* «11» 05 2023 г.

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 ВО

Дисциплина «Виртуальные частные сети» изучается в 8 семестре и относится к вариативной части дисциплин блока Б1 специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Дисциплина основывается на знаниях, полученных при изучении дисциплин «Информатика», «Основы информационной безопасности», «Организация ЭВМ и вычислительных систем», «Открытые информационные системы», «Сети и системы передачи информации», «Криптографические методы защиты информации».

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

- знание базовых профессиональных понятий и определений в области в области физики, вычислительной техники, электроники и схемотехники и информационной безопасности;
- способность использовать нормативные правовые документы;
- способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования;
- способность анализировать проблемы и процессы.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Безопасность вычислительных сетей», «Разработка и эксплуатация автоматизированных систем в защищённом исполнении», «Безопасность открытых информационных систем», «Инструментальные средства контроля защищенности 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-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 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
ПК-2 - Способен осуществлять тестирование систем защиты информации автоматизированных систем	**Знает:** 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 **Умеет:** Применять действующую нормативную базу в области обеспечения безопасности информации Контролировать безотказное функционирование технических средств защиты информации **Владеет:** Навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем
ПК-3 - Способен разрабатывать проектные решения по защите	**Знать:** Руководящие и методические документы уполномоченных федеральных органов исполнительной власти

информации в автоматизированных системах	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:** Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

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
		8 семестр
Контактная работа обучающихся с преподавателем	54/54*	54/54*
Аудиторные занятия:	54/54*	54/54*
Лекции	18/18*	18/18*
Практические и семинарские занятия	-	-
Лабораторные работы (лабораторный практикум)	36/36*	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)		- вопросы при защите лабораторных работ - рефераты на заданные темы
Курсовая работа		

Вид учебной работы	Количество часов (форма обучения ___*очная*_____)	
	Всего по плану	В т.ч. по семестрам
		8 семестр
Виды промежуточной аттестации (экзамен, зачет)	зачет	зачет
Всего часов по дисциплине:	72	72

* 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	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практические занятия, семинары	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Виртуальная частная сеть как средство защиты информации							
1. Введение в технологию виртуальных частных сетей (VPN)	4	2				2	Тесты Т1, реф. (1,4,10)
2. Схема и политики безопасности VPN	16	2		12	4	2	Тесты Т2, реф. (№ 2,3)
3. Стандартные протоколы создания VPN	20	4		12	6	4	Тесты Т3, реф. (№ 5,11)
Раздел 2. Управление криптографическими ключами в виртуальных частных сетях							
4. Особенности управления ключевой системой асимметричных криптосистем. Инфрастуктура открытых ключей	4	2				2	Тесты Т4, реф. (№ 9)
5. Сертификация открытых ключей	4	2			4	2	Тесты Т5, реф. (№ 17)
Раздел 3. Построение виртуальной частной сети							
6. Требования к продуктам построения виртуальных частных	4	2				2	Тесты Т6, реферат

сетей. Варианты реализации							(№ 12-15)
7. Решения для построения виртуальных частных сетей	16	2		12	4	2	Тесты Т7, реф. (№ 16)
8. Характеристика российских продуктов для создания виртуальных частных сетей	4	2				2	Тесты Т8, реф. (№ 6,7,8, 12-15)
Итого:	72	18		36	18	18	Зачёт

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Виртуальная частная сеть как средство защиты информации

Тема 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 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 3. Стандартные протоколы создания VPN (семинар).

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 4. Особенности управления ключевой системой асимметричных криптосистем. Инфраструктура 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 5. 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 6. 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 7. 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 8. 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.

ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические и семинарские занятия не предусмотрены учебным планом дисциплины.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 1. Виртуальная частная сеть как средство защиты информации

Тема 2. Схема и политики безопасности

Лабораторная работа № 1 (12 часов). **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.

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.

Тема 3. Стандартные протоколы создания VPN

Лабораторная работа №2 (12 часов). **Удалённый доступ по протоколу SSH.**

Цель. Изучение возможностей протокола SSH для получения удалённого доступа к серверу. возможностей протокола SSH для получения удалённого доступа к серверу

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

Раздел 3. Построение виртуальной частной сети

Тема 6. Требования к продуктам построения виртуальных частных сетей. Варианты реализации.

Лабораторная работа № 3 (12 часов). **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.

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.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

8.2 **Примерная тематика рефератов:**

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

8.2.1 Правила оформления рефератов

1. Объём реферата 7-10 листов печатного текста. К оформлению рефератов предъявляются такие же требования, как и к курсовым работам для студентов 3 курса, описанные в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

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. Управление секретными и открытыми ключами. Инфрастуктура открытых ключей
13. Модели APKI и PKIX
14. Основные подходы к обеспечению безопасности открытых ключей. Содержание метода сертификации открытых ключей
15. Удостоверяющий центр. Сертификат открытого ключа. Формат сертификации открытого ключа
16. Модель инфраструктуры открытых ключей. Основные протоколы ИОК согласно модели PKIX
17. Требования к продуктам построения виртуальных частных сетей
18. Варианты реализации VPN
19. Шлюзы и клиенты VPN
20. VPN на базе сетевых операционных систем
21. VPN на базе маршрутизаторов
22. VPN на базе межсетевых экранов
23. VPN на базе специализированного программного обеспечения
24. VPN на базе аппаратных средств
25. Виды виртуальных частных сетей
26. Аппаратно-программный комплекс «Континент»
27. Программные продукты семейства «Застава»
28. Продукты комплекса «VipNet»
29. Семейство продуктов «Net-PRO»
30. Продукты «Шип» и «Игла-2»

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Виртуальная частная сеть как средство защиты информации. Тема 1. Введение в технологию виртуальных частных сетей (VPN)	Подготовка к лекции, лабораторным работам, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты на лекции, реферат, отчёты на лабораторных работах, зачёт
Раздел 1. Тема 2. Схема и политики безопасности VPN	Подготовка к лекции, лабораторным работам, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты на лекции, реферат, отчёты на лабораторных работах, зачёт
Раздел 1. Тема 3. Стандартные протоколы создания VPN	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачёта	4	Тесты на лекциях, реферат, зачёт
Раздел 2. Управление криптографическими ключами в виртуальных частных сетях. Тема 4. Особенности управления	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты на лекциях, реферат, зачёт

ключевой системой асимметричных криптосистем. Инфраструктура открытых ключей			
Раздел 2. Тема 5. Сертификация открытых ключей	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты на лекциях, реферат, зачёт
Раздел 3. Построение виртуальной частной сети. Тема 6. Требования к продуктам построения виртуальных частных сетей. Варианты реализации	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты на лекциях, реферат, зачёт
Раздел 3. Тема 7. Решения для построения виртуальных частных сетей	Подготовка к лекции, лабораторным работам, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты на лекции, реферат, отчёты на лабораторных работах, зачёт
Раздел 3. Тема 8. Характеристика российских продуктов для создания виртуальных частных сетей	Подготовка к лекции, подготовка рефератов, подготовка к сдаче зачёта	2	Тесты на лекциях, реферат, зачёт

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Запечников С.В., Основы построения виртуальных частных сетей: Учебное пособие для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И. - 2-е изд., стереотип. - М.: Горячая линия - Телеком, 2011. - 248 с. - ISBN 978-5-9912-0215-2 – URL: http://www.studentlibrary.ru/book/ISBN9785991202152.html

2. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 – URL: http://www.studentlibrary.ru/book/ISBN9785991204705.html

Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации") – URL: http://www.consultant.ru/document/cons_doc_LAW_208191/

1.3 Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» – URL: http://www.consultant.ru/document/cons_doc_LAW_112701/

1.4. 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/

2. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности. – URL: http://gostexpert.ru/gost/gost-27002-2012

3. Бизин, Д. И. Виртуальные частные сети (VPN) : учебно-методическое пособие / Д. И. Бизин, О. Н. Коваленко. — Омск : ОмГУПС, 2019. — 37 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165629

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

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. - Ульяновск: УлГУ, 2020. - Загл. с экрана;

Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл: 292 КБ). – URL: http://lib.ulsu.ru/MegaPro/Download/MObject/7920

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.

в) Профессиональные базы данных, информационно-справочные 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.

4. 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.

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.

Согласовано:

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

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций: 3/317, 2/24б.

Аудитория 2/24б укомплектована 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