

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ОРГАНИЗАЦИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

**«Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)»**,

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

ОРГАНИЗАЦИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Рабочая программа дисциплины

Составитель(и):

Кандидат технических наук, доцент, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор

Кандидат технических наук, доцент, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры
комплексной защиты информации

№ 8 от 14.03.2024 г. _____

ОГЛАВЛЕНИЕ

1. Пояснительная записка	4
1.1. Цель и задачи дисциплины	4
1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:	4
1.3. Место дисциплины в структуре образовательной программы	5
2. Структура дисциплины	6
3. Содержание дисциплины	6
4. Образовательные технологии	7
5. Оценка планируемых результатов обучения	8
5.1. Система оценивания	8
5.2. Критерии выставления оценки по дисциплине	8
5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине	9
6. Учебно-методическое и информационное обеспечение дисциплины	13
6.1. Список источников и литературы	13
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».	13
7. Материально-техническое обеспечение дисциплины.....	14
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов	14
9. Методические материалы	15
9.1. Планы практических занятий – проверка сформированности компетенций – ПК-13	15
АННОТАЦИЯ ДИСЦИПЛИНЫ	17

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем; навыков организации работы по применению виртуальных частных сетей, оптимального выбора и интеграции сетевых протоколов виртуальных частных сетей (ВЧС).

Задачи дисциплины:

- рассмотрение существа проблемы безопасной передачи информации в информационных системах, основных способов обеспечения конфиденциальности и целостности информации при её передаче, основных протоколов, применяемых для организации защищённых ВЧС, критериев выбора оптимальных схемных решений для организации защищённых ВЧС на канальном, сетевом и прикладном уровнях.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-8 Способен осуществлять мониторинг и аудит защищённости информации в автоматизированных системах	ПК-8.1 Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации	Знать: <ul style="list-style-type: none"> • основные виды угроз безопасности информации при её передаче по компьютерным сетям; способы построения виртуальных каналов; протоколы организации ВЧС
	ПК-8.2 Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем	Уметь: <ul style="list-style-type: none"> • проводить анализ проблем безопасности передачи информации с точки зрения конфиденциальности и целостности; проводить анализ и выбор сетевых протоколов ВЧС
	ПК-8.3 Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы	Владеть: <ul style="list-style-type: none"> • приёмами настройки и применения современных сетевых протоколов ВЧС

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Организация виртуальных частных сетей» относится к дисциплинам по выбору вариативной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Сети и системы передачи информации», «Технические средства защиты информации от утечки по техническим каналам», «Математические основы защиты информации».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: дисциплина является одной из завершающих обучение.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 2 з.е., 72 академических часов,

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
8	Лекции	22
8	Практические занятия	28
Всего:		50

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 22 академических часа.

3. Содержание дисциплины

Тема 1. Основные угрозы информационной безопасности

Анализ угроз сетевой безопасности. Проблемы безопасности IP-сетей. Угрозы и уязвимости корпоративных проводных сетей. Угрозы и уязвимости беспроводных сетей. Способы обеспечения информационной безопасности.

Тема 2 Определение, цели и задачи виртуальных частных сетей

Основные понятия и функции виртуальных частных сетей (VPN). Варианты построения виртуальных защищённых каналов. Средства обеспечения безопасности VPN. классификация сетей VPN. Основные варианты архитектуры VPN. Достоинства использования технологии VPN.

Тема 3. Защита виртуальных каналов на канальном и сеансовом уровнях модели OSI

Канальный уровень модели OSI. Протокол PPTP. Протокол L2F. Протокол L2TP. Протокол SSL/TLS. Протокол SOCKS.

Тема 4. Защита виртуальных каналов на сетевом уровне модели OSI

Сетевой уровень модели OSI. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол управления криптоключами. Особенности реализации средств IPSec.

Тема 5. Инфраструктура защиты на прикладном уровне модели OSI

Управление идентификацией и доступом. Особенности управления доступом. функционирование системы управления доступом. Организация защищённого удалённого доступа. Протоколы аутентификации удалённых пользователей. Централизованный контроль удалённого доступа. Управление доступом по схеме SSO. Протокол Kerberos. Инфраструктура управления открытыми ключами PKI. Принципы функционирования, логическая структура и компоненты PKI.

Тема 6. Средства защиты информации, дополняющие виртуальные частные сети

Межсетевое экранирование. Системы антивирусной защиты. Системы обнаружения вторжений. Комплексная защита информации.

Тема 7. Программно-аппаратные комплексы для создания виртуальных частных сетей

Построение сетей VPN на базе маршрутизаторов. Создание защищённых туннелей с помощью межсетевых экранов. Построение сетей VPN с помощью специализированного ПО. Туннелирование на основе специальных аппаратных средств. VPN-решения компании «Инфотекс». VPN-решения в семействе продуктов «Net-PRO» компании «Сигнал-КОМ».

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Основные угрозы информационной безопасности	Лекция 1. Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
2	Определение, цели и задачи виртуальных частных сетей	Лекция 2. Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
3	Защита виртуальных каналов на канальном и сеансовом уровнях модели OSI	Лекция 3 Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
4	Защита виртуальных каналов на сетевом уровне модели OSI	Лекция 4. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций
5	Инфраструктура защиты на прикладном уровне модели OSI	Лекция 5.1 Лекция 5.2 Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
6	Средства защиты информации, дополняющие виртуальные частные сети	Лекция 6 Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
7	Программно-аппаратные комплексы для создания виртуальных частных сетей	Лекция 6 Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
8	Практическая работа № 1. Создание простого VPN канала	Практическая работа	Выполнение задания
9	Практическая работа № 2. Разработка и создание сети сложной структуры территориально-распределённой компании. Создание VPN каналов	Практическая работа	Выполнение задания

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну ра- боту	Всего
Текущий контроль: – опрос (темы 1-8) – практическое занятие 1...2	4 балла 20 баллов	20 баллов 40 баллов
Промежуточная аттестация <i>зачёт</i> В традиционной форме по билетам		40 баллов
Итого за семестр <i>зачёт</i>		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шка- ла	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шка- ла ECTS	Оценка по дисци- плине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ С	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Дайте различные определения виртуальной частной сети и поясните их.	ПК-8

2.	Какие задачи решает построение VPN, а какие – установка МЭ?	ПК-8
3.	Каковы значения термина "частный" применительно к VPN?	ПК-8
4.	В чем различие использования провайдеров связи и провайдеров Internet для создания VPN?	ПК-8
5.	Возможно ли использование только каналов связи предприятия для создания его VPN?	ПК-8
6.	Каковы преимущества и недостатки использования Internet для создания VPN?	ПК-8
7.	В чём заключаются маркетинговая и потребительная сущность VPN?	ПК-8
8.	Как понимается защищённость от потоков данных в VPN?	ПК-8
9.	Какие услуги по защите данных обеспечивают VPN?	ПК-8
10.	Что важно для конечных пользователей при использовании VPN?	ПК-8
11.	Каковы особенности современных сетей, на основе которых приходится создавать VPN?	ПК-8
12.	Какие требования предъявляются к создаваемой VPN?	ПК-8
13.	Каковы особенности построения VPN в различных сетях передачи данных (FR, ATM, X.25, TCP/IP)?	ПК-8
14.	Какие услуги предлагают провайдеры по построению VPN?	ПК-8
15.	В чём заключается механизм туннелирования в сетях? Каковы его особенности и схемы использования?	ПК-8
16.	Что такое VPN-агенты и каковы их функции?	ПК-8
17.	Дайте определение политики безопасности VPN и приведите несколько примеров.	ПК-8
18.	Поясните определения критериев безопасности применительно к задачам VPN.	ПК-8
19.	Какими средствами защиты информации нужно дополнить VPN, чтобы реализовать комплексную защиту?	ПК-8
20.	На каких уровнях модели OSI работают какие протоколы создания VPN?	ПК-8
21.	Что и какими средствами защищается на прикладном уровне?	ПК-8
22.	Какие протоколы выполняют защиту данных в VPN на канальном уровне? Сравните их возможности.	ПК-8
23.	Расскажите об особенностях протокола PPTP. Рассмотрите схемы его применения. Нарисуйте структуру пакета PPTP.	ПК-8
24.	Расскажите об особенностях протокола L2F.	ПК-8
25.	Расскажите об особенностях протокола L2TP. Рассмотрите схемы его применения. Сравните с протоколом PPTP.	ПК-8
26.	Какие протоколы выполняют защиту данных в VPN на сетевом уровне? Сравните их возможности.	ПК-8
27.	Расскажите об особенностях протокола IPSec и решаемых им задачах. Рассмотрите схемы его применения.	ПК-8
28.	Какие протоколы выполняют защиту данных в VPN на сеансовом уровне? Сравните их возможности.	ПК-8
29.	Расскажите об особенностях протокола SSL. Поясните работу протокола диалога SSL.	ПК-8
30.	Расскажите об особенностях протокола TLS.	ПК-8
31.	Расскажите об особенностях протокола SOCKS. Поясните обобщённую схему установления соединения по протоколу SOCKS. Сравните 4-ю и 5-ю версии протокола.	ПК-8
32.	Что понимается под термином управление криптографическими	ПК-8

	ключами? Какова основная цель и основные задачи управления ключами?	
33.	Что такое жизненный цикл ключа? Каковы его основные стадии?	ПК-8
34.	В каких состояниях пребывают криптографические ключи за время своего жизненного цикла? При каких условиях происходят переходы из одного состояния в другое?	ПК-8
35.	В чем отличие жизненного цикла секретных и открытых криптографических ключей?	ПК-8
36.	Что такое инфраструктура открытых ключей? Какова ее логическая и физическая структура?	ПК-8
37.	Какие основные логические модели инфраструктуры открытых ключей разработаны международными организациями? В чём заключаются их особенности?	ПК-8
38.	Каковы перспективы практического применения концепции инфраструктуры открытых ключей?	ПК-8
39.	Каковы основные способы распространения открытых ключей в криптосистемах?	ПК-8
40.	Изложите в общих чертах существо метода сертификации открытых ключей. В чём заключаются преимущества и недостатки этого метода?	ПК-8
41.	В чем различие между идентификационными и атрибутивными сертификатами?	ПК-8
42.	Какие основные стандарты, описывающие форматы сертификатов и списков аннулированных сертификатов, разработаны и приняты международными организациями?	ПК-8
43.	Какие требования предъявляются к продуктам построения VPN? Поясните их.	ПК-8
44.	Расскажите о вариантах реализации VPN, их преимуществах и недостатках. Приведите примеры продуктов.	ПК-8
45.	Какие функции в VPN выполняют шлюзы и клиенты?	ПК-8
46.	Какие сетевые средства реализуют протоколы создания VPN?	ПК-8
47.	Сравните достоинства и недостатки средств создания VPN различных категорий	ПК-8
48.	Расскажите о построении VPN на базе сетевой ОС. Приведите примеры.	ПК-8
49.	Расскажите о построении VPN на базе маршрутизаторов. Приведите примеры.	ПК-8
50.	Расскажите о построении VPN на базе МЭ. Приведите примеры.	ПК-8
51.	Дайте определение МЭ и расскажите об их назначении, компонентах, типах и схемах подключения в сети.	ПК-8
52.	Расскажите о построении VPN на базе ПО. Приведите примеры.	ПК-8
53.	Расскажите о построении VPN на базе аппаратных средств. Приведите примеры.	ПК-8
54.	Какие виды VPN Вам известны и какие задачи они решают?	ПК-8
55.	Расскажите об Intranet VPN. Приведите схему построения.	ПК-8
56.	Расскажите о Client/server VPN. Нарисуйте схему построения.	ПК-8
57.	Расскажите об Extranet VPN. Схематично представьте способ построения.	ПК-8
58.	Расскажите о VPN с удалённым доступом и их вариантах.	ПК-8
59.	Каковы назначение, особенности, состав и возможности аппаратно-программного комплекса защиты информации	ПК-8

	"Континент-К"?	
60.	Какие программные продукты компании "ЭЛВИС+" используются для построения VPN и как именно? Какой основной протокол управления ключами применяется в этих продуктах?	ПК-8
61.	Расскажите об VPN-решениях компании "Инфотекс". Каковы их особенности и функциональные возможности? В чём заключается технологий ViPNet?	ПК-8
62.	Какие функции по созданию VPN и как именно реализованы в семействе продуктов "Net-PRO" компании "Сигнал-КОМ"? На основе какого протокола осуществляется шифрование?	ПК-8
63.	Рассмотрите назначение и возможности продуктов МО ПНИЭИ "ШИП" и "Игла-2" с точки зрения построения VPN.	ПК-8
64.	Какие составляющие аппаратно-программного комплекса "ФПСУ-IP" компании "Амикон" и с какими особенностями используются для построения VPN? Что реализует VPN-экранирование?	ПК-8
65.	По каким основным показателям удобнее всего сравнивать продукты для создания VPN?	ПК-8

Примерные тестовые задания – проверка сформированности компетенций – ПК-8

1. Укажите примеры непреднамеренного несанкционированного воздействия на информацию:

а) ошибки пользователей и персонала

б) блокирование информации

в) сбои и отказы техники

г) искажение информации

д) уничтожение информации

е) природные явления

ж) утрата носителя информации

з) копирование информации

и) хищение носителя информации

2. Выберите протоколы туннелирования канального уровня модели OSI:

а) PPTP

б) PPPoE

в) ARP

г) L2F

д) L2TP

е) PPP

Примерные вопросы к зачёту – проверка сформированности компетенций – ПК-8

1. Анализ угроз сетевой безопасности. Проблемы безопасности IP-сетей.
2. Угрозы и уязвимости корпоративных проводных сетей.
3. Угрозы и уязвимости беспроводных сетей.
4. Способы обеспечения информационной безопасности.
5. Варианты построения виртуальных защищённых каналов. Средства обеспечения безопасности VPN.
6. Классификация сетей VPN.
7. Основные варианты архитектуры VPN.
8. Достоинства использования технологии VPN.
9. Канальный уровень модели OSI. Протокол PPTP.
10. Протокол L2F. Протокол L2TP.
11. Протокол SSL/TLS.

12. Протокол SOCKS.
13. Сетевой уровень модели OSI. Архитектура средств безопасности IPSec.
14. Защита передаваемых данных с помощью протоколов AH и ESP.
15. Протокол управления криптоключами.
16. Особенности реализации средств IPSec.
17. Управление идентификацией и доступом. Особенности управления доступом.
18. Организация защищённого удалённого доступа.
19. Протоколы аутентификации удалённых пользователей.
20. Централизованный контроль удалённого доступа. Управление доступом по схеме SSO.
21. Протокол Kerberos.
22. Инфраструктура управления открытыми ключами PKI. Принципы функционирования, логическая структура и компоненты PKI.
23. Построение сетей VPN на базе маршрутизаторов.
24. Создание защищённых туннелей с помощью межсетевых экранов.
25. Построение сетей VPN с помощью специализированного ПО.
26. Туннелирование на основе специальных аппаратных средств.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники
основные
дополнительные

Литература
основная

1. Запечников, С. В. Основы построения виртуальных частных сетей: Учебное пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. - Москва : Гор. линия-Телеком, 2011. - 249 с. (Специальность). ISBN 5-93517-139-2, 3000 экз. - Текст : электронный. - URL: <https://znanium.com/catalog/product/563048> (дата обращения: 24.03.2024). – Режим доступа: по подписке.
2. Елисеев, А. И. Технологии виртуальных частных сетей : учебное пособие / А. И. Елисеев, Ю. В. Минин. — Тамбов : ТГТУ, 2019. — 96 с. — ISBN 978-5-8265-2091-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/320063>. — Режим доступа: для авториз. пользователей.
3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/3032>. — Режим доступа: для авториз. пользователей.
4. Митюшин Д.А. Использование программного комплекса Cisco Packet Tracer v.7.3 в изучении сетевых технологий: учебно-практическое пособие (практикум) / Д. А. Митюшин ; Российский государственный гуманитарный университет. – М.: Изд-во РГГУ, 2021. – 217 с.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijJLa94T9>, свободный. – Загл. с экрана.
2. <https://telecom-sales.ru/content/stati/tehnologii-cisco-vpn-vidy-i-tipy-udalennogo-dostupa/>

3. <https://infotecs.ru/>
4. <https://www.signal-com.ru/>

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Cisco Packet Tracer v.7.2	Cisco Systems	свободное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
 - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
 - в форме аудиофайла.
- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
 - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
 - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - передвижными, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий – проверка сформированности компетенций – ПК-13

Практическая работа № 1 (10 ч.). Создание простого VPN канала

Практическая работа № 7 из учебного пособия [1].

Список литературы:

1. Митюшин Д.А. Использование программного комплекса Cisco Packet Tracer v.7.3 в изучении технологий защиты информации: Учебно-практическое пособие (практикум). М.: РГГУ, 2021. 220 с.

2. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9>, свободный. – Загл. с экрана.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с ППП MS Office 2007 или выше, СПО СРТ v.7.0.

Практическая работа № 2 (18 ч.). Разработка и создание сети сложной структуры территориально-распределённой компании. Создание VPN каналов

Практическая работа № 10 из учебного пособия [1].

Список литературы:

1. *Митюшин Д.А.* Использование программного комплекса Cisco Packet Tracer v.7.3 в изучении технологий защиты информации: Учебно-практическое пособие (практикум). М.: РГГУ, 2021. 220 с.
2. *Видео уроки Cisco Packet Tracer. Курс молодого бойца.* [Электронный ресурс] : Режим доступа : <https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9>, свободный. – Загл. с экрана.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с ППП MS Office 2007 или выше, СПО СРТ v.7.0.

По результатам практических занятий обучающиеся составляют отчёты. Отчёт составляется в электронной форме с использованием ПКП MS Office и выше и передаётся преподавателю посредством оговорённой формы связи.

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Организация виртуальных частных сетей» реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – Безопасность автоматизированных систем) кафедрой комплексной защиты информации.

Цель дисциплины: формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем; навыков организации работы по применению виртуальных частных сетей, оптимального выбора и интеграции сетевых протоколов виртуальных частных сетей (ВЧС).

Задачи: рассмотрение существа проблемы безопасной передачи информации в информационных системах, основных способов обеспечения конфиденциальности и целостности информации при её передаче, основных протоколов, применяемых для организации защищённых ВЧС, критериев выбора оптимальных схемных решений для организации защищённых ВЧС на канальном, сетевом и прикладном уровнях.

Дисциплина направлена на формирование следующих компетенций:

- ПК-8 Способен осуществлять мониторинг и аудит защищённости информации в автоматизированных системах.

В результате освоения дисциплины обучающийся должен:

Знать основные виды угроз безопасности информации при её передаче по компьютерным сетям; способы построения виртуальных каналов; протоколы организации ВЧС.

Уметь проводить анализ проблем безопасности передачи информации с точки зрения конфиденциальности и целостности; проводить анализ и выбор сетевых протоколов ВЧС.

Владеть приёмами настройки и применения современных сетевых протоколов ВЧС.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.