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
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Организация виртуальных частных сетей
Рабочая программа дисциплины
Составитель(и):
Составитель:
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

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

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№_10_ от__20.05.2021 г._____

ОГЛАВЛЕНИЕ

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. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-4.3 *Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем*	*ОПК-4.3.1* *Знает требования по установке, настройке, администрированию и обслуживанию программно-аппаратных и технических средств защиты информации автоматизированных систем*	*Знать:* • *основные виды угроз безопасности информации при её передаче по компьютерным сетям.* • *способы построения и архитектуру ВЧС, правила настройки и администрирования виртуальных каналов*
	ОПК-4.3.2 *Умеет настраивать программное обеспечение системы защиты информации, выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации*	*Уметь:* • *проводить настойку параметров защищённого канала*
	ОПК-4.3.3 *Владеет навыками по осуществлению планирования и организации работы персонала автоматизированной системы с учётом требований по защите информации*	*Владеть:* • *приёмами настройки и администрирования ВЧС типа «ЛВС-ЛВС» и «ЛВС-удалённый хост»*
ПК-8 *Способен осуществлять мониторинг и аудит защищённости информации в автоматизированных*	*ПК-8.1* *Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты*	*Знать:* • *криптографические методы, алгоритмы, используемые в ВЧС;* • *протоколы при организации*

системах	*информации в автоматизированных системах, организационные меры по защите информации*	*защищённых каналов 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:* • *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:* • *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 части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Сети и системы передачи информации», «Методы и средства криптографической защиты информации», «Безопасность вычислительных сетей».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Преддипломная практика».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _76__ ч., в том числе контактная работа обучающихся с преподавателем _40_ ч., промежуточная аттестация _-_ ч., самостоятельная работа обучающихся _36_ ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Основные угрозы информационной безопасности*	**8**	**2**					**2**	Опрос
2	*Определение, цели и задачи виртуальных частных сетей*	**8**	**2**					**2**	Опрос
3	*Защита виртуальных каналов на канальном и сеансовом уровнях модели OSI*	**8**	**2**					**2**	Опрос.
4	*Защита виртуальных каналов на сетевом уровне модели OSI*	**8**	**2**					**2**	Опрос.
5	*Инфраструктура защиты на прикладном уровне модели OSI*	**8**	**4**					**2**	Опрос.
6	*Средства защиты информации, дополняющие виртуальные частные сети*	**8**	**2**					**2**	Опрос.
7	*Программно-аппаратные комплексы для создания виртуальных частных сетей*	**8**	**2**					**2**	Опрос.
8	*Практическая работа № 1. Создание простого VPN канала*	**8**			**8**			**8**	Оценка выполнения практического задания
9	*Практическая работа № 2.* Разработка и создание сети сложной структуры тер-	**8**			**14**			**10**	Оценка выполнения практического задания

	риториально-распределённой компании. Создание *VPN* каналов								
	зачёт				**2**			**4**	*Зачёт по билетам*
	итого:		**16**		**24**			**36**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**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.
2	**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.
3	**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.
4	**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.
5	**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.
6	**Тема 6. Средства защиты информации, дополняющие виртуальные частные сети**	Межсетевое экранирование. Системы антивирусной защиты. Системы обнаружения вторжений. Комплексная защита информации.
7	**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 работу	**Всего**
Текущий контроль: *– опрос (темы 1-8)* *– практическая работа 1* *– практическая работа 2*	 *3 балла* *10 баллов* *26 баллов*	 *24 баллов* *10 баллов* *26 баллов*
Промежуточная аттестация *зачёт*		*40 баллов*
Итого за дисциплину *зачёт*		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1 – 8	ОПК-4.3.1, ОПК-4.3.2, ОПК-4.3.3, ПК-8.1, ПК-8.2, ПК-8.3	Опрос
2.	Практические занятия 1, 2	ОПК-4.3.1, ОПК-4.3.2, ОПК-4.3.3, ПК-8.1, ПК-8.2, ПК-8.3	План практического занятия

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 шкала	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/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. 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. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«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 выставляются 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 выставляются обучающемуся с учётом результатов текущей и промежуточной атте-

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		стации. 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 выставляются 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.	ОПК-4.3.1; ПК-8.1
2.	Какие задачи решает построение VPN, а какие – установка МЭ?	ОПК-4.3.1; ПК-8.1
3.	Каковы значения термина "частный" применительно к VPN?	ОПК-4.3.1; ПК-8.1
4.	В чем различие использования провайдеров связи и провайдеров Internet для создания VPN?	ОПК-4.3.1; ПК-8.1
5.	Возможно ли использование только каналов связи предприятия для создания его VPN?	ОПК-4.3.1; ПК-8.1
6.	Каковы преимущества и недостатки использования Internet для создания VPN?	ОПК-4.3.1; ПК-8.1
7.	В чем заключаются маркетинговая и потребительная сущность VPN?	ОПК-4.3.1; ПК-8.1
8.	Как понимается защищённость от потоков данных в VPN?	ОПК-4.3.1; ПК-8.1
9.	Какие услуги по защите данных обеспечивают VPN?	ОПК-4.3.1; ПК-8.1
10.	Что важно для конечных пользователей при использовании VPN?	ОПК-4.3.1; ПК-8.1

11.	Каковы особенности современных сетей, на основе которых приходится создавать VPN?	ОПК-4.3.1; ПК-8.1
12.	Какие требования предъявляются к создаваемой VPN?	ОПК-4.3.1; ПК-8.1
13.	Каковы особенности построения VPN в различных сетях передачи данных (FR, ATM, X.25, TCP/IP)?	ОПК-4.3.1; ПК-8.1
14.	Какие услуги предлагают провайдеры по построению VPN?	ОПК-4.3.1; ПК-8.1
15.	В чем заключается механизм туннелирования в сетях? Каковы его особенности и схемы использования?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
16.	Что такое VPN-агенты и каковы их функции?	ОПК-4.3.1; ПК-8.1
17.	Дайте определение политики безопасности VPN и приведите несколько примеров.	ОПК-4.3.1; ПК-8.1
18.	Поясните определения критериев безопасности применительно к задачам VPN.	ОПК-4.3.1; ПК-8.1
19.	Какими средствами защиты информации нужно дополнить VPN, чтобы реализовать комплексную защиту?	ОПК-4.3.1; ПК-8.1
20.	На каких уровнях модели OSI работают какие протоколы создания VPN?	ОПК-4.3.1; ПК-8.1
21.	Что и какими средствами защищается на прикладном уровне?	ОПК-4.3.1; ПК-8.1
22.	Какие протоколы выполняют защиту данных в VPN на канальном уровне? Сравните их возможности.	ОПК-4.3.1; ПК-8.1

Промежуточная аттестация (примерные вопросы для зачёта) – проверка сформированности компетенций – ОПК-4.3; ПК-8

1.	Расскажите об особенностях протокола PPTP. Рассмотрите схемы его применения. Нарисуйте структуру пакета PPTP.	ОПК-4.3.1; ПК-8.1; ПК-8.2; ПК-8.3
2.	Расскажите об особенностях протокола L2F.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
3.	Расскажите об особенностях протокола L2TP. Рассмотрите схемы его применения. Сравните с протоколом PPTP.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
4.	Какие протоколы выполняют защиту данных в VPN на сетевом уровне? Сравните их возможности.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
5.	Расскажите об особенностях протокола IPSec и решаемых им задачах. Рассмотрите схемы его применения.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
6.	Какие протоколы выполняют защиту данных в VPN на сеансовом уровне? Сравните их возможности.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
7.	Расскажите об особенностях протокола SSL. Поясните работу протокола диалога SSL.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
8.	Расскажите об особенностях протокола TLS.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
9.	Расскажите об особенностях протокола SOCKS. Поясните обобщённую схему установления соединения по протоколу	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1;

	SOCKS. Сравните 4-ю и 5-ю версии протокола.	ПК-8.2; ПК-8.3
10.	Что понимается под термином управление криптографическими ключами? Какова основная цель и основные задачи управления ключами?	ОПК-4.3.1; ОПК-4.3.2; ПК-8.1; ПК-8.2
11.	Что такое жизненный цикл ключа? Каковы его основные стадии?	ОПК-4.3.1; ПК-8.1
12.	В каких состояниях пребывают криптографические ключи за время своего жизненного цикла? При каких условиях происходят переходы из одного состояния в другое?	ОПК-4.3.1; ПК-8.1
13.	В чем отличие жизненного цикла секретных и открытых криптографических ключей?	ОПК-4.3.1; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
14.	Что такое инфраструктура открытых ключей? Какова ее логическая и физическая структура?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
15.	Какие основные логические модели инфраструктуры открытых ключей разработаны международными организациями? В чем заключаются их особенности?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
16.	Каковы основные способы распространения открытых ключей в криптосистемах?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
17.	Изложите в общих чертах существо метода сертификации открытых ключей. В чем заключаются преимущества и недостатки этого метода?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
18.	В чем различие между идентификационными и атрибутными сертификатами?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
19.	Какие основные стандарты, описывающие форматы сертификатов и списков аннулированных сертификатов, разработаны и приняты международными организациями?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
20.	Какие требования предъявляются к продуктам построения VPN? Поясните их.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
21.	Расскажите о вариантах реализации VPN, их преимуществах и недостатках. Приведите примеры продуктов.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
22.	Какие функции в VPN выполняют шлюзы и клиенты?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
23.	Какие сетевые средства реализуют протоколы создания VPN?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
24.	Сравните достоинства и недостатки средств создания VPN различных категорий.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
25.	Расскажите о построении VPN на базе сетевой ОС. Приведите примеры.	ОПК-4.3.1; ПК-8.1; ПК-8.3
26.	Расскажите о построении VPN на базе маршрутизаторов. Приведите примеры.	ОПК-4.3.1; ПК-8.1; ПК-8.3
27.	Расскажите о построении VPN на базе МЭ. Приведите примеры.	ОПК-4.3.1; ПК-8.1; ПК-8.3
28.	Дайте определение МЭ и расскажите об их назначении, компонентах, типах и схемах подключения в сети.	ОПК-4.3.1; ПК-8.1; ПК-8.3

29.	Расскажите о построении VPN на базе ПО. Приведите примеры.	ОПК-4.3.1; ПК-8.1; ПК-8.3
30.	Расскажите о построении VPN на базе аппаратных средств. Приведите примеры.	ОПК-4.3.1; ПК-8.1; ПК-8.3
31.	Какие виды VPN Вам известны и какие задачи они решают?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
32.	Расскажите об Intranet VPN. Приведите схему построения.	ОПК-4.3.1; ПК-8.1; ПК-8.3
33.	Расскажите о Client/server VPN. Нарисуйте схему построения.	ОПК-4.3.1; ПК-8.1; ПК-8.3
34.	Расскажите об Extranet VPN. Схематично представьте способ построения.	ОПК-4.3.1; ПК-8.1; ПК-8.3
35.	Расскажите о VPN с удалённым доступом и их вариантах.	ОПК-4.3.1; ПК-8.1; ПК-8.3
36.	Каковы назначение, особенности, состав и возможности аппаратно-программного комплекса защиты информации "Континент-К"?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
37.	Какие программные продукты компании "ЭЛВИС+" используются для построения VPN и как именно? Какой основной протокол управления ключами применяется в этих продуктах?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
38.	Расскажите об VPN-решениях компании "Инфотекс". Каковы их особенности и функциональные возможности? В чем заключается технологий ViPNet?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
39.	Какие функции по созданию VPN и как именно реализованы в семействе продуктов "Net-PRO" компании "Сигнал-КОМ"? На основе какого протокола осуществляется шифрование?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
40.	Рассмотрите назначение и возможности продуктов МО ПНИЭИ "ШИП" и "Игла-2" с точки зрения построения VPN.	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
41.	Какие составляющие аппаратно-программного комплекса "ФПСУ-IP" компании "Амикон" и с какими особенностями используются для построения VPN? Что реализует VPN-экранирование?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3
42.	По каким основным показателям удобнее всего сравнивать продукты для создания VPN?	ОПК-4.3.1; ОПК-4.3.2; ОПК-4.3.3; ПК-8.1; ПК-8.2; ПК-8.3

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Литература

Основная

1. *Комплексная защита* информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4 - Режим доступа: http://znanium.com/catalog/product/402686
2. *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.
3. *Панасенко С.П.* Виртуальные частые сети и другие способы защиты информации // Мир ПК. – 2002. – № 4. https://www.osp.ru/pcworld/2002/04/163195

Дополнительная

1. *Олифер В.Г.* Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М. [и др.] : Питер, 2008. – 957 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=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9, 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

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

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы

	Консультант Плюс, Гарант

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, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий – проверка сформированности компетенций – ОПК-4.3 и ПК-8

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических занятий соответствует программе дисциплины.

Практическая работа № 1 (8 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 сетевых технологий: учебно-практическое пособие (практикум) / Д. А. Митюшин ; Российский государственный гуманитарный университет. – М.: Изд-во РГГУ, 2021. – 217 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 (14 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 сетевых технологий: учебно-практическое пособие (практикум) / Д. А. Митюшин ; Российский государственный гуманитарный университет. – М.: Изд-во РГГУ, 2021. – 217 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 CPT v.7.0.

Приложение 1

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:

- ОПК-4.3 – Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает требования по установке, настройке, администрированию и обслуживанию программно-аппаратных и технических средств защиты информации автоматизированных систем
- Умеет настраивать программное обеспечение системы защиты информации, выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации
- Владеет навыками по осуществлению планирования и организации работы персонала автоматизированной системы с учётом требований по защите информации

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

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации
- 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
- Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.
Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.