ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом и.о. ректора
от «07» июня 2021 г. № 79

Б1.О.45 Виртуальные частные сети

рабочая программа дисциплины

Специальность/направление подготовки – 10.05.03 Информационная безопасность автоматизированных систем
Специализация/профиль – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – очная форма 5 лет, 6 месяцев
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5
Часов по учебному плану (УП) – 180

Формы промежуточной аттестации
очная форма обучения:
экзамен 9 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	9	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	85	**85**
– лекции	34	**34**
– практические (семинарские)	34	**34**
– лабораторные	17	**17**
Самостоятельная работа	59	**59**
Экзамен	36	**36**
Итого	180	**180**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем утвержденным Приказом Минобрнауки России от от 26.11.2020 № 1457.

Программу составил(и):
Старший преподаватель, Ю.О. Купитман

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «4» июня 2021 г. № 11-2

Зав. кафедрой, к.э.н., доцент Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели дисциплины

1	углублённое изучение криптографических протоколов и стандартов;
2	ознакомление обучающихся с основными техническими средствами построения виртуальных частных сетей (VPN)

1.2 Задачи дисциплины

1	ознакомление с понятиями в области криптографических протоколов и стандартов;
2	изучение основ построения VPN;
3	ознакомление обучающихся с основными практическими приемами построения VPN;
4	рассмотрение различных вариантов и схем создания VPN;
5	ознакомиться со стандартными протоколами VPN и управлением криптографическими ключами в VPN

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.

Цель достигается по мере решения в единстве следующих задач:

– формирование сознательного отношения к выбранной профессии;

– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;

– формирование психологии профессионала;

– формирование профессиональной культуры, этики профессионального общения;

– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Б1.О.31 Безопасность сетей ЭВМ
2	Б1.О.34 Документоведение
3	Б1.О.36 Сети и системы передачи информации
4	Б1.О.37 Защита информации от утечки по техническим каналам
5	Б1.О.42 Открытые информационные системы
6	Б1.О.43 Криптографические протоколы и стандарты
7	Б1.О.47 Информационные технологии
8	Б1.О.51 Кибербезопасность
9	Б1.О.54 Методы и средства криптографической защиты информации
10	Б1.О.55 Защита объектов критической информационной инфраструктуры

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б1.О.60 Защита информации от несанкционированного доступа
2	Б1.О.62 Моделирование процессов и систем защиты информации
3	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
4	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных	ОПК-9.1 Проводит анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных	Знать: методики оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов; все основные современные ИТ, средства технической защиты информации, сетей и систем передачи информации и тенденции их развития
		Уметь: применять на практике методики оценки защищенности автоматизированных систем
		Владеть: навыками безопасного использования

технологий, средств технической защиты информации, сетей и систем передачи информации		технических средств автоматизации; навыками документирования оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов
	ОПК-9.3 Знает текущее состояние и тенденции развития сетей и систем передачи информации	Знать: уровни защищённости автоматизированных систем; принципы эксплуатации систем и средств обеспечения информационной безопасности в вычислительных системах; основные протоколы и сервисы идентификации и аутентификации абонентов и объектов сети
		Уметь: составлять и организовывать на практике перечень работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; составлять и организовывать на практике перечень работ по вводу в эксплуатацию сетей и систем передачи информации
		Владеть: способностью формулировать принципы эксплуатации систем и средств обеспечения информационной безопасности; методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; методами организации выполнения работ по вводу в эксплуатацию сетей и систем передачи информации
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2 Умеет применять доверенное хранение, защиту каналов связи и электронного документооборота	Знать: российские и международные стандарты, описывающие криптографические функции; стандартные криптопротоколы; методы и средства организации защиты каналов связи и электронного документооборота
		Уметь: определять перечень нормативных актов и руководящих документов по использованию криптографических протоколов; проводить инструментальный мониторинг защищенности информации в VPN и выявлять каналы утечки информации
		Владеть: навыками применения криптопротоколов и стандартов для построения защищенных систем и защиты электронного документооборота; методами и средствами организации защиты каналов связи и электронного документооборота

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Базовые сведения о технологиях обеспечения информационной безопасности (ИБ) объектов.**						
1.1	Введение. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Виды контроля знаний.	9	1			4	ОПК-9.1
1.2	Состав и классификация средств обеспечения ИБ объектов. Место технологии построения виртуальных сетей в общей системе средств обеспечения ИБ объектов.	9	1	2	2	6	ОПК-9.3
2.0	**Раздел 2. Межсетевые экраны (МЭ).**						
2.1	Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Руководящий документ Гостехкомиссии РФ по МЭ. Профили защиты для МЭ. Основные типы МЭ: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, МЭ экспертного уровня. Персональные МЭ. Основные компоненты МЭ. Слабости МЭ. Выбор реализаций МЭ.	9	4	4	1	4	ОПК-9.1
2.2	Маршрутизаторы Cisco. Назначение и основные характеристики. Операционная система. Интерфейсы маршрутизаторов. Основные разделы и подразделы меню комплекса межсетевых экранов ФПСУ-IP. Идентификация и аутентификация комплекса в сети. Удаленное администрирование. Построение VPN на базе комплекса. Комплекс ФПСУ-IP-клиент.	9	4	4	2	6	ОПК-10.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
3.0	**Раздел 3. Виртуальные частные сети (VPN).**						
3.1	Различные подходы к определению VPN, определение компании Check Point Software Technologies. Цели и задачи применения VPN-технологий. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи. Специфика построения VPN. Критерии, предъявляемые к VPN. Политики безопасности для VPN.	9	2	4	2	4	ОПК-9.3
3.2	Туннелирование. Механизм туннелирования как основа построения VPN. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты. Функции VPN-агентов. Обработка входящих и исходящих пакетов. Различные варианты позиционирования и использования VPN-агентов.	9	4	2	1	4	ОПК-9.3
3.3	Классификация VPN компании Check Point по типу устанавливаемых соединений: Intranet VPN, ClientServer VPN, Extranet VPN, Remote Access VPN – определения, характерные черты и особенности использования. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности: доверенные, защищенные и смешанные VPN – определения, требования, технологии построения. VPN в сетях общего пользования. Специфика использования VPN в сетях Frame Realay, ATM, X.25, TCP/IP. Основные варианты создания VPN: защищенные, частные и промежуточные каналы.	9	4	2	1	6	ОПК-9.1
3.4	Варианты политик безопасности при использовании каналов Internet для построения VPN. Интеграция VPN и дополнительных средств защиты: использование PKI, криптографические модули, аудит, антивирусные средства и т.д. Варианты построения VPN. VPN на базе сетевой ОС, МЭ, маршрутизаторов, специализированного ПО, аппаратных средств – основные характеристики, сравнительный анализ.	9	4	4	2	4	ОПК-10.2
4.0	**Раздел 4. Стандартные протоколы создания VPN.**						
4.1	Протокол PPTP. Функции протокола. Компоненты PPTP. Сценарии работы протокола. Архитектура PPTP. Управляющее соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows 2000.	9	2	4	1	5	ОПК-10.2
4.2	Протокол L2TP. Основные функции и характеристики протокола. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP /IPSec инкапсуляция данных. Обработка входящих и исходящих данных. Настройка VPN на базе протокола E2TP в среде Windows 2000.	9	2	4	2	4	ОПК-10.2
4.3	Протокол IPSec. Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP. Инкапсуляция дан¬ных в транспортном и туннельном режимах работы. Форматы заголовков. Защищаемые поля IP-заголовка при использовании AH в транспортном режиме. Обработка	9	4	2	2	6	ОПК-10.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
	исходящих (поиск SA, гене¬рация порядкового номера, вычисление ICV и шифрование данных, фрагментация) и входящих (сборка, поиск SA, проверка порядкового номера, проверка ICV, расшифрование, проверка на со¬ответствие записи в SPD) пакетов. Использование комбинированных криптографических алгорит¬мов в ESP. Особенности использования расширенных (64-битных) порядковых номеров. Защита от повторной передачи пакетов. Согласование параметров безопасности с использованием прото¬кола IKE. Порядок обмена сообщениями IKE. Сообщения IKE_SA_INIT для согласования пара¬метров безопасности IKE_SA и обмена по протоколу Диффи-Хеллмана. Сообщения IKE_AUTH для аутентификации и установления CHILD_SA для защиты данных с помощью AH или ESP. Со¬общения CREATE_CHILD_SA для согласования дополнительных CHILD_SA в рамках данной IKE_SA. Сообщения INFORMATIONAL для сообщения информации о текущем состоянии или ошибках. Детали работы протокола (согласование версий протокола, использование порядковых номеров, генерирование ключевого материала, обработка ошибок и т.д.). Форматы основного заго¬ловка IKE и заголовков сообщений.						
5.0	**Раздел 5. Базовые сведения о виртуальных локальных сетях (VLAN).**						
5.1	Виды, протоколы и безопасность VLAN. VLAN с группировкой портов. VLAN с маркированными кадрами. VLAN на основе протоко¬лов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимуще¬ства VLAN.	9	2	2	1	6	ОПК-9.1
	Форма промежуточной аттестации – экзамен	9	36				ОПК-9.1 ОПК-9.3 ОПК-10.2
	Итого часов (без учёта часов на промежуточную аттестацию)		34	34	17	59	

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Бизин, Д. И. Виртуальные частные сети (VPN) : учебно-методическое пособие к выполнению лабораторных работ / Д. И. Бизин, О. Н. Коваленко. Омск : ОмГУПС, 2019. - 37с. - Текст: электронный. - URL: https://e.lanbook.com/book/165629 (дата обращения: 19.04.2023)	Онлайн
6.1.1.2	Елисеев, А. И. Технологии виртуальных частных сетей : учебное пособие / А. И. Елисеев, Ю. В. Минин. Тамбов : ТГТУ, 2019. - 96с. - Текст: электронный. - URL: https://e.lanbook.com/book/320063 (дата обращения: 19.04.2023)	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/

		онлайн
6.1.2.1	Мэйволд, Э. Безопасность сетей : учебное пособие - 2-е изд., испр. / Э. Мэйволд. Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 572с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 14.09.2022)	Онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Купитман, Ю.О. Методические указания по изучению дисциплины Б1.О.45 Виртуальные частные сети по специальности – 10.05.03 Информационная безопасность автоматизированных систем, специализация – № 5 Безопасность открытых информационных систем / Ю.О. Купитман ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 17 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_3882_1529_2021_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Научная электронная библиотека «КиберЛенинка» — https://cyberleninka.ru/	
6.2.2	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/	
6.2.3	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.2.4	Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/	
6.2.5	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/	
6.2.6	VPN: ещё раз просто о сложном https://habr.com/ru/articles/534250/	
6.2.7	Бытовой инфобез. Как выбрать VPN? https://habr.com/ru/companies/tomhunter/articles/689202/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01	
6.3.2.2	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html	
6.3.2.3	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/	
6.3.2.4	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.	
6.3.2.5	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01. прогр.средство защиты от НСД Secret Net4.0, клиент серв.безоп.Secret Net 4.0, сервер безопасности C Secret Net4.0	
6.3.2.10	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01. Packet Tracer УЧ. ПРОЦ. Универсальная общественная лицензия GNU, http://www.packettracernetwork.com/	
6.3.2.11	PuTTY свободно распространяемый клиент для различных протоколов удалённого доступа УЧ. ПРОЦ. http://www.putty.org/	
6.3.3 Информационные справочные системы		
6.3.3.1	Не предусмотрены	
6.4 Правовые и нормативные документы		
6.4.1	Не предусмотрены	

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80

2	Учебная аудитория Д-216 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации».«Безопасность программно-аппаратных средств защиты информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор (переносной), экран (переносной), компьютер измеритель шумов и вибрации 003-МЗ
4	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
5	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
6	Лаборатория Д-508 «Информационные системы и сетевые технологии».«Сети и системы передачи информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор (переносной), экран (переносной), компьютер коммутационная стойка – 1 шт. Сервер – 1 шт. cisco 2600 – 2 шт. switch catalyst 2900 – 2 шт. модем ZyXEL – 2 шт. Router cisco 1600 – 1 шт. Hub token ring – 1 шт. Тел. адаптер D-link DVG-7111S – 1 шт. Управляемый коммутатор 2 уровня D-link DES-1210-10/ME – 1 шт. Управляемый коммутатор 3 уровня D-link DGS-1500-28 -1 шт. Межсетевой экран D-link DFL-260E – 1 шт. Маршрутизатор D-Link DIR-100 - 1 шт. Беспроводная точка доступа D-Link DWL-3200AP – 1 шт. Голосовой шлюз D-Link DVG-7022S Gateway+Router с поддержкой SIP – 1 шт. IP-камера D-Link DCS-2130 – 1шт. Коммутатор D-link DES-1100-16 – 2 шт. Коммутатор D-link DES-3028 – 1 шт.
7	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на

	практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Виртуальные частные сети» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой

	дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Виртуальные частные сети» участвует в формировании компетенций:

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
9 семестр				
1.0	**Раздел 1. Базовые сведения о технологиях обеспечения информационной безопасности (ИБ) объектов**			
1.1	Текущий контроль	Введение. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Виды контроля знаний.	ОПК-9.1	Собеседование (устно)
1.2	Текущий контроль	Состав и классификация средств обеспечения ИБ объектов. Место технологии построения виртуальных сетей в общей системе средств обеспечения ИБ объектов.	ОПК-9.3	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
2.0	**Раздел 2. Межсетевые экраны (МЭ)**			
2.1	Текущий контроль	Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Руководящий документ Гостехкомиссии РФ по МЭ. Профили защиты для МЭ. Основные типы МЭ: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, МЭ экспертного уровня. Персональные МЭ. Основные компоненты МЭ. Слабости МЭ. Выбор реализаций МЭ.	ОПК-9.1	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
2.2	Текущий контроль	Маршрутизаторы Cisco. Назначение и основные характеристики. Операционная система. Интерфейсы маршрутизаторов. Основные разделы и подразделы меню комплекса межсетевых экранов ФПСУ-IP. Идентификация и аутентификация комплекса в сети. Удаленное администрирование. Построение VPN на базе комплекса. Комплекс ФПСУ-IP-клиент.	ОПК-10.2	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
3.0	**Раздел 3. Виртуальные частные сети (VPN)**			
3.1	Текущий контроль	Различные подходы к	ОПК-9.3	Доклад (устно)

		определению VPN, определение компании Check Point Software Technologies. Цели и задачи применения VPN-технологий. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи. Специфика построения VPN. Критерии, предъявляемые к VPN. Политики безопасности для VPN.		Лабораторная работа (письменно/устно) Собеседование (устно)
3.2	Текущий контроль	Туннелирование. Механизм туннелирования как основа построения VPN. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты. Функции VPN-агентов. Обработка входящих и исходящих пакетов. Различные варианты позиционирования и использования VPN-агентов.	ОПК-9.3	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
3.3	Текущий контроль	Классификация VPN компании Check Point по типу устанавливаемых соединений: Intranet VPN, ClientServer VPN, Extranet VPN, Remote Access VPN – определения, характерные черты и особенности использования. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности: доверенные, защищенные и смешанные VPN – определения, требования, технологии построения. VPN в сетях общего пользования. Специфика использования VPN в сетях Frame Realay, ATM, X.25, TCP/IP. Основные варианты создания VPN: защищенные, частные и промежуточные каналы.	ОПК-9.1	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
3.4	Текущий контроль	Варианты политик безопасности при использовании каналов Internet для построения VPN. Интеграция VPN и дополнительных средств защиты: использование PKI, криптографические модули, аудит, антивирусные средства и т.д. Варианты построения VPN. VPN на базе сетевой ОС, МЭ, маршрутизаторов, специализированного ПО, аппаратных средств – основные характеристики, сравнительный анализ.	ОПК-10.2	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
4.0	**Раздел 4. Стандартные протоколы создания VPN**			

4.1	Текущий контроль	Протокол PPTP. Функции протокола. Компоненты PPTP. Сценарии работы протокола. Архитектура PPTP. Управляющее соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows 2000.	ОПК-10.2	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
4.2	Текущий контроль	Протокол L2TP. Основные функции и характеристики протокола. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP /IPSec инкапсуляция данных. Обработка входящих и исходящих данных. Настройка VPN на базе протокола E2TP в среде Windows 2000.	ОПК-10.2	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
4.3	Текущий контроль	Протокол IPSec. Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP. Инкапсуляция дан¬ных в транспортном и туннельном режимах работы. Форматы заголовков. Защищаемые поля IP-заголовка при использовании AH в транспортном режиме. Обработка исходящих (поиск SA, гене¬рация порядкового номера, вычисление ICV и шифрование данных, фрагментация) и входящих (сборка, поиск SA, проверка порядкового номера, проверка ICV, расшифрование, проверка на со¬ответствие записи в SPD) пакетов. Использование комбинированных криптографических алгорит¬мов в ESP. Особенности использования расширенных (64-битных) порядковых номеров. Защита от повторной передачи пакетов. Согласование параметров безопасности с использованием прото¬кола IKE. Порядок обмена сообщениями IKE. Сообщения IKE_SA_INIT для согласования пара¬метров безопасности IKE_SA и обмена	ОПК-10.2	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)

		по протоколу Диффи-Хеллмана. Сообщения IKE_AUTH для аутентификации и установления CHILD_SA для защиты данных с помощью AH или ESP. Со¬общения CREATE_CHILD_SA для согласования дополнительных CHILD_SA в рамках данной IKE_SA. Сообщения INFORMATIONAL для сообщения информации о текущем состоянии или ошибках. Детали работы протокола (согласование версий протокола, использование порядковых номеров, генерирование ключевого материала, обработка ошибок и т.д.). Форматы основного заго¬ловка IKE и заголовков сообщений.		
5.0	**Раздел 5. Базовые сведения о виртуальных локальных сетях (VLAN)**			
5.1	Текущий контроль	Виды, протоколы и безопасность VLAN. VLAN с группировкой портов. VLAN с маркированными кадрами. VLAN на основе протоко¬лов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимуще¬ства VLAN.	ОПК-9.1	Доклад (устно) Лабораторная работа (письменно/устно) Собеседование (устно)
	Промежуточная аттестация	Раздел 1. Базовые сведения о технологиях обеспечения информационной безопасности (ИБ) объектов. Раздел 2. Межсетевые экраны (МЭ). Раздел 3. Виртуальные частные сети (VPN). Раздел 4. Стандартные протоколы создания VPN. Раздел 5. Базовые сведения о виртуальных локальных сетях (VLAN).	ОПК-9.1 ОПК-9.3 ОПК-10.2	Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов
3	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Образец задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (образец экзаменационного билета) к экзамену
2	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме экзамена. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	Обучающийся правильно ответил на теоретические вопросы.	Высокий

	Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	
«хорошо»	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме экзамена

Критерии оценивания	Шкала оценивания
Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования	«отлично»
Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования	«хорошо»
Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования	«удовлетворительно»
Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования	«неудовлетворительно»

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ

«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Доклад

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»		Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»		Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	«не зачтено»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль доклада не передана

Лабораторная работа

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»		Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	«не зачтено»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания,

		практические умения и навыки

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

1. Что такое протокол SSH? Зачем он нужен?
2. Что такое Telnet? В чём отличие от SSH?
3. Как происходит аутентификация?
4. Расскажите кратко об алгоритме RSA.
5. Что такое SVI? Как он настраивается?
6. Какой командой создаётся новый пользователь вместе с паролем?
7. Как поставить пароль на вход в настройки через консоль?
8. Как поставить пароль на привилегированный режим?
9. Расскажите о VTY.
10. Расскажите пошагово настройку ssh.
11. Что выведет данная команда ssh -l net_admin 172.16.0.100?
12. Что выведет команда sh crypto key mypubkey rsa?
13. Какая команда покажет текущие ssh соединения?
14. Какие VLAN существуют по умолчанию в коммутаторе и к каким из них принадлежат его интерфейсы?
15. Можно ли в сети с несколькими коммутаторами при конфигурировании VLAN обойтись без использования стандарта IEEE802.1Q?
16. Каково назначение функции Port Security?
17. В чем преимущество каналов EtherChannel?
18. Для чего необходим протокол STP?
19. Может ли администратор каким-либо образом повлиять на расчет покрывающего дерева в сети?
20. Для чего и каким образом конфигурируются статические маршруты?
21. В каких случаях целесообразно использовать маршруты по умолчанию?
22. Каково назначение протокола CDP, в чем преимущества и недостатки его использования в сети?
23. Каковы основные возможности протокола управления сетью SNMP?

3.2 Типовые контрольные темы для написания докладов

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов тем для написания докладов.

1. Развитие сетей связи.
2. Эталонная модель взаимодействия открытых систем OSI.
3. Организации стандартизации в области телекоммуникаций.
4. Линии связи на основе симметричных кабелей.
5. Линии связи на основе коаксиальных кабелей.
6. Линии связи на основе волоконно-оптических кабелей.
7. Источники оптического излучения: лазеры, светодиоды и пр.
8. Фотоприемники.

9. Оптические компоненты.
10. Структурированные кабельные системы SCS.
11. Преобразование аналоговых сигналов в цифровые и обратно: АЦП и ЦАП.
12. Алгоритмы низкоскоростной передачи речевых сигналов.
13. Кодирование дискретных сообщений.
14. Помехоустойчивые коды.
15. Семейство протоколов HDLC.
16. Виды модуляции и манипуляции.
17. Методы разделения каналов.
18. Методы множественного доступа.
19. Модемы: классификация, виды, назначение.
20. Стандарты RS-232, V.24 и V.25.
21. Обзор мирового и российского рынков профессиональных и потребительских модемов.
22. Сравнительный анализ модемных технологий.
23. Линейное кодирование и технологии цифровых абонентских линий xDSL. Стандарт G.992.2 (G.lite).
24. Асимметричные цифровые абонентские линии ADSL.
25. Сети с коммутацией каналов.
26. Взаимоувязанная сеть связи России.
27. Нумерация абонентских линий на телефонной сети общего пользования.
28. Основные понятия теории телетрафика.
29. Построение коммутационных полей автоматических телефонных станций.
30. Построение коммутационных полей цифровых АТС.
31. Системы сигнализации в телефонных сетях.
32. Устройство и принцип действия аналоговых и цифровых телефонных аппаратов.
33. Система сигнализации №7 (SS7).
34. Транзит SS7 по IP-сетям.
35. Конверторы сигнализации.
36. Особенности распространения радиоволн различных диапазонов.
37. Антенны.
38. Радиорелейные системы передачи.
39. Беспроводные абонентские линии (Radio in Local Loop).
40. Системы спутниковой связи.
41. Низкоорбитальные спутниковые системы.
42. Непосредственное телевизионное вещание с ИСЗ.
43. Глобальные системы определения координат GPS и ГЛОНАСС.
44. Стандарты телевидения PAL, SECAM, NTSC.
45. Цифровое телевидение.
46. Телевидение высокой четкости HDTV.
47. Стандарты сжатия видеосигналов.
48. Сотовые системы подвижной связи.
49. Стандарт GSM.
50. Стандарт CDMA.
51. Системы персонального радиовызова (пейджинг).
52. Транкинговые системы связи.
53. Системы беспроводных телефонов.
54. Сети с коммутацией пакетов.
55. Сети X.25.
56. Сети Frame Relay.
57. Цифровые сети интегрального обслуживания ISDN.
58. Системы передачи плезиохронной иерархии PDH.
59. Системы передачи синхронной иерархии SDH.

3.3 Типовые задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

Лабораторная работа № 1. Frame Relay (point-to-point, point-to-multipoint).

Цель: изучить основы построения сети на технологии Frame Relay.

Задачи:

1. Просмотр исходной конфигурации.
2. Обеспечение Frame Relay соединения.
3. Конфигурирование статической маршрутизации и маршрутизации по умолчанию.
4. Проверка соединения.

Контрольные вопросы:

1. Что такое Frame Relay? Опишите принцип его работы.
2. Что такое MPLS?
3. Что такое DLCI?
4. Как настраивается Frame Realay?
5. Что такое DTE и DCE? Какой командой можно определить, к какому концу провода V.35 подключено устройство?
6. Опишите структуру кадра Frame Relay.
7. Для чего нуже6н протокол Inverse ARP?
8. Что такое подынтерфейс? Как его настроить?
9. Что выводит команда show frame-relay map?
10. Что выводит команда show frame-relay lmi?
11. Что выводит команда show frame-relay pvc?
12. Как можно проверить работоспособность Frame Relay?

Лабораторная работа № 2. Межсетевой экран.

Цель: изучить основы конфигурации межсетевого экрана и фильтрации траффика.

Задачи:

1. Подключение к веб-серверу.
2. Предотвращение незашифрованных сеансов HTTP
3. Доступ к межсетевому экрану на сервере электронной почты.

Контрольные вопросы:

1. Что такое межсетевой экран? Зачем он нужен?
1. Является ли межсетевой экран firewall'ом и брандмауэром? Или это разные вещи?
2. Какие виды МЭ выделяют и как, в общем, они функционируют?
3. Опишите фильтрующие МЭ.
4. Опишите МЭ сетевого уровня.
5. Опишите МЭ прикладного уровня.
6. Дайте краткий обзор возможностей Outpost Firewall Pro 4.0.
7. Охарактеризуйте имеющиеся у Outpost Firewall Pro 4.0 подключаемые модули.
8. Какие политики имеются у Outpost?
9. К каким группам может быть отнесено конкретное приложение в Outpost? Охарактеризуйте каждую из них.
10. Какие возможности имеются у Kerio WinRoute Firewall 6.3.1?

11. Сравните возможности межсетевых экранов Kerio WinRoute Firewall 6.3.1 и Outpost Firewall Pro 4.0. Какие у них имеются достоинства и недостатки?

Лабораторная работа №3. Настройка NAT.

Цель: изучить принципы конфигурации NAT.

Задачи:

1. создание компьютерной сети в рабочей области логической топологии;
2. настраивание на компьютерах и локальном сервере ip-адресов;
3. создание сегментов локальной сети посредством vlan на коммутаторе и sub-интерфейсов на маршрутизаторе;
4. подключение локальной сети к провайдеру;
5. настройка перегруженного NAT (PAT);
6. настройка access-листа;
7. настройка статического NAT.

Контрольные вопросы:

1. Что такое NAT? Для чего он нужен?
2. Что такое публичные и приватные IP-адреса?
3. Расскажите про статический NAT.
4. Расскажите про динамический NAT.
5. Расскажите про Many-to-One NAT.
6. Расскажите очерёдность настройки NAT вместе с командами.
7. Что такое обратная маска? Для чего она?
8. Какие достоинства у NAT?
9. Какие минусы?

Лабораторная работа №4. Настройка VPN на виртуальных машинах.

Цель: изучить технологии виртуальных частных сетей для организации защищенных каналов связи через сети общего пользования (Интернет), получить практические навыки настройки виртуальных частных сетей на примере программного продукта OpenVPN.

Задачи:

1. Настроить безопасное взаимодействие двух IP-сетей между собой через сеть общего пользования (Интернет), средствами программного продукта OpenVPN.
2. Создать ключи и сертификаты безопасности.
3. Настроить конфигурационный файл VPN-сервера и VPN-клиента.

Контрольные вопросы:

1. Что такое Certificate Authority? Для чего он нужен?
2. Какие существуют ключи и сертификаты в OpenVPN?
3. Чем отличается конфигурация сервера и клиентов OpenVPN?
4. Объясните строки в конфигурационном файле

```
local 192.168.200.1
port 3579
proto udp
```

Лабораторная работа №5. Защита периметра сети.

Цель: изучение основных технологий межсетевого экранирования, методов и средств управления безопасностью информационных потоков на межсетевых экранах и сетевых маршрутизаторах.

Задачи:

1. Настроить сеть по схеме. Выдать всем устройствам IP-адреса, настроить маршрутизацию.

2. Настроить правила управления доступом серверов и рабочих станций из ЛВС в сеть Интернет и из нее к серверам АС, расположенным в ДМЗ согласно табл. 2.

3. Реализовать механизм первичной фильтрации пакетов на пограничном маршрутизаторе IBR.

4. Настроить политику управления доступом к данным серверам на основе порядка функционирования WWW- и DNS-служб.

Контрольные вопросы:

1. Определить в схеме СПД механизмы и средства обеспечения отказоустойчивости и масштабирования. Перечислить задачи, решаемые на каждом уровне иерархической модели данной СПД.

2. Найти и изучить описание всех команд, используемых для настройки протокола OSPF.

3. Для каждого маршрутизатора определить его характеристики, роли и свойства в рамках протокола OSPF.

Лабораторная работа №6. Защита инфраструктуры маршрутизации.

Цель: обучение методам и средствам проектирования и защиты инфраструктуры маршрутизации отказоустойчивых иерархических компьютерных сетей на основе протокола маршрутизации OSPF.

Задачи:

1. Настроить сеть по схеме. Выдать всем устройствам IP-адреса, настроить маршрутизацию.

2. Провести настройки маршрутизаторов для защиты маршрутизации.

3. Ввести в сеть ложный маршрутизатор и проверить, что он не может участвовать в маршрутизации.

Контрольные вопросы:

1. Определить в схеме СПД механизмы и средства обеспечения отказоустойчивости и масштабирования. Перечислить задачи, решаемые на каждом уровне иерархической модели данной СПД.

2. Найти и изучить описание всех команд, используемых для настройки протокола OSPF.

3. Для каждого маршрутизатора определить его характеристики, роли и свойства в рамках протокола OSPF.

Лабораторная работа №7. Защита сетевой инфраструктуры.

Цель: изучение методов и средств защиты сетевой инфраструктуры от НСД, а также принципов проектирования сетей управления.

Задачи:

1. Настроить сеть по схеме. Выдать всем устройствам IP-адреса, настроить маршрутизацию.

2. Настроить подключение к устройствам по протоколу SSH.

3. Настроить протокол SNMP.

4. Настроить access list.

5. Проверить работоспособность.

Контрольные вопросы:

1. В сети одного из филиалов банка построить сеть внутриполосного управления.

2. Убедиться в невозможности доступа в сеть управления из ЛВС передачи данных и наоборот.

Лабораторная работа №8. Настройка VPN туннеля по протоколу PPTP.

Цель: изучить технологии виртуальных частных сетей, построенных на протоколе PPTP.

Задачи:

1. Настроить две виртуальные машины – Windows Server и Windows 10 и настроить связь между ними.
2. Установить на сервере VPN-PPTP.
3. Проверить работоспособность на клиенте.

Контрольные вопросы:

1. Что такое PPTP? В чём его отличие от L2TP и IPSec?
2. Перечислите основные шаги, необходимые для установки VPN сервера.
3. Возможно ли использование сертификатов для шифрования трафика VPN?
4. В каком из протоколов VPN используется алгоритм Диффи –Хеллмана?
5. Может ли Windows 10 выступать в роли VPN сервера

Лабораторная работа №9 Настройка VPN туннеля по протоколу L2TP.

Цель: изучить технологии виртуальных частных сетей, построенных на протоколе L2TP.

Задачи:

1. Настроить две виртуальные машины – Windows Server и Windows 10 и настроить связь между ними.
2. Установить на сервере VPN- L2TP.
3. Проверить работоспособность на клиенте.

Контрольные вопросы:

1. Что такое L2TP? В чём его отличие от PPTP и IPSec?
2. По какому алгоритму шифрования работает L2TP?
3. Может ли работать L2TP без IPSec?
4. На каком уровне работает L2TP?
5. Какие два типа туннеля поддерживает L2TP?

Лабораторная работа №10. Настройка сетей VPN.

Цель: научиться настраивать виртуальные частные сети с использованием IPsec для трафика.

Задачи:

Часть 1. Включение функций безопасности.

Часть 2. Настройка параметров IPsec на маршрутизаторе R1.

Часть 3. Настройка параметров IPsec на маршрутизаторе R3.

Часть 4. Проверка работы VPN IPsec.

Контрольные вопросы:

1. Что такое VPN? Для чего оно нужно?
2. Какие самые часто использующиеся технологии организации VPN-канала существуют?
3. Что такое PPTP?
4. Что такое OpenVPN?
5. Что такое WireGuard?
6. Что такое IPSec?
7. Перечислите протоколы, с которыми работает IPSec.
8. Расскажите, как создаётся защищённое соединение в IPSec?
9. Расскажите отличия ESP от AH.
10. Два режима работы IPSec.
11. Расскажите пошагово, как настроить маршрутизатор для создания туннеля.
12. Что выводит команда show crypto ipsec sa?

Лабораторная работа №11. Настройка Private VLAN.

Цель: изучить особенности построения приватных VLAN.
Задачи:
1. Настроить сеть по схеме.
2. Настроить на коммутаторах VLAN и отдельно Private VLAN.
3. Проверить работоспособность.

Контрольные вопросы:
1. Назначение и основные характеристики коммутатора.
2. Что такое VLAN? Какие они дают преимущества?
3. На каком уровне модели OSI работает коммутатор?
4. Способы создания VLAN.
5. Что такое VTP?
6. Что такое VID и PVID?
7. Какие команды вы использовали для конфигурирования коммутатора?
8. Как можно просмотреть сконфигурированные VLAN?
9. Как организовать связь между ПК, расположенных в одной Vlan, но на разных коммутаторах?
10. Что дает использование trunk?
11. Можно ли создать Vlan, не входя в базу данных Vlan?

3.4 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-9.1	Введение. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Виды контроля знаний.	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-9.3	Состав и классификация средств обеспечения ИБ объектов. Место технологии построения виртуальных сетей в общей системе средств обеспечения ИБ объектов.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1	Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Руководящий документ Гостехкомиссии РФ по МЭ. Профили защиты для МЭ. Основные типы МЭ: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, МЭ экспертного уровня. Персональные МЭ. Основные компоненты МЭ. Слабости МЭ. Выбор реализаций МЭ.	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-10.2	Маршрутизаторы Cisco. Назначение и основные характеристики. Операционная система. Интерфейсы маршрутизаторов. Основные разделы и подразделы меню комплекса межсетевых экранов ФПСУ-IP. Идентификация и аутентификация комплекса в сети. Удаленное администрирование. Построение VPN на базе комплекса. Комплекс ФПСУ-IP-клиент.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 – ЗТЗ
ОПК-9.3	Различные подходы к определению VPN, определение компании Check Point Software Technologies. Цели и задачи применения VPN-технологий. Преимущества VPN по	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	2 – ОТЗ

	сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи. Специфика построения VPN. Критерии, предъявляемые к VPN. Политики безопасности для VPN.		3 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 – ЗТЗ
ОПК-9.3	Туннелирование. Механизм туннелирования как основа построения VPN. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты. Функции VPN-агентов. Обработка входящих и исходящих пакетов. Различные варианты позиционирования и использования VPN-агентов.	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1	Классификация VPN компании Check Point по типу устанавливаемых соединений: Intranet VPN, ClientServer VPN, Extranet VPN, Remote Access VPN – определения, характерные черты и особенности использования. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности: доверенные, защищенные и смешанные VPN – определения, требования, технологии построения. VPN в сетях общего пользования. Специфика использования VPN в сетях Frame Realay, ATM, X.25, TCP/IP. Основные варианты создания VPN: защищенные, частные и промежуточные каналы.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-10.2	Варианты политик безопасности при использовании каналов Internet для построения VPN. Интеграция VPN и дополнительных средств защиты: использование PKI, криптографические модули, аудит, антивирусные средства и т.д. Варианты построения VPN. VPN на базе сетевой ОС, МЭ, маршрутизаторов, специализированного ПО, аппаратных средств – основные характеристики, сравнительный анализ.	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-10.2	Протокол PPTP. Функции протокола. Компоненты PPTP. Сценарии работы протокола. Архитектура PPTP. Управляющее соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows 2000.	Знание	1 – ОТЗ 3 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	1 – ОТЗ 1 – ЗТЗ
ОПК-10.2	Протокол L2TP. Основные функции и характеристики протокола. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP /IPSec инкапсуляция данных. Обработка входящих и исходящих данных. Настройка VPN на базе протокола E2TP в среде Windows 2000.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-10.2	Протокол IPSec. Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP. Инкапсуляция дан¬ных в транспортном и туннельном режимах работы. Форматы заголовков. Защищаемые поля IP-заголовка при использовании AH в транспортном режиме. Обработка исходящих (поиск SA, гене¬рация порядкового номера, вычисление ICV и шифрование данных, фрагментация) и входящих (сборка, поиск SA, проверка порядкового номера, проверка ICV, расшифрование, проверка на со¬ответствие записи в SPD) пакетов. Использование комбинированных криптографических алгорит¬мов в ESP. Особенности использования расширенных (64-битных) порядковых	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ

	номеров. Защита от повторной передачи пакетов. Согласование параметров безопасности с использованием прото¬кола IKE. Порядок обмена сообщениями IKE. Сообщения IKE_SA_INIT для согласования пара¬метров безопасности IKE_SA и обмена по протоколу Диффи-Хеллмана. Сообщения IKE_AUTH для аутентификации и установления CHILD_SA для защиты данных с помощью AH или ESP. Со¬общения CREATE_CHILD_SA для согласования дополнительных CHILD_SA в рамках данной IKE_SA. Сообщения INFORMATIONAL для сообщения информации о текущем состоянии или ошибках. Детали работы протокола (согласование версий протокола, использование порядковых номеров, генерирование ключевого материала, обработка ошибок и т.д.). Форматы основного заго¬ловка IKE и заголовков сообщений.		
ОПК-9.1	Виды, протоколы и безопасность VLAN. VLAN с группировкой портов. VLAN с маркированными кадрами. VLAN на основе протоко¬лов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимуще¬ства VLAN.	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 1 – ЗТЗ
		Итого	50 – ОТЗ 50 – ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

1. SSH расшифровывается как:
   a) secure shell
   b) shell of secure
   c) security service host
   d) security system host

2. VLAN расшифровывается как:
   a) valid local authentication network
   b) virtual local area network
   c) virtual linear authentication network
   d) valuable local advance network

3. Программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами, называется _____.

4. Напишите команду, которой можно вывести текущие ssh соединения.

5. Установите соответствие между термином и его определением.

1. Коммутатор	a. Базовая станция, предназначенная для обеспечения беспроводного доступа к уже существующей сети или создания новой беспроводной сети.
2. Повторитель	b. Сетевое оборудование, предназначенное для увеличения расстояния сетевого соединения и его расширения за пределы одного сегмента или для организации двух ветвей
3. Маршрутизатор	c. Устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети
4. Точка доступа	d. Специализированное устройство, которое пересылает пакеты между различными сегментами сети

1. _____
2. _____
3. _____
4. _____

6. Расскажите, что такое ПАК ФПСУ-IP.

7. Выберите протоколы туннелирования, используемые в VPN:
   a) SMTP
   b) L2TP
   c) TCP
   d) FTP
   e) Telnet
   f) PPTP
   g) HTTP
   h) IPSec

8. Специальная технология, определяющая способ упаковки, передачи и распаковки данных при передаче по VPN-соединению, называется _____.

9. Включение всего пакета одного протокола внутрь пакета другого протокола в качестве передаваемой информации, это…
   a) декапсуляция;
   b) инкапсуляция;
   c) коммутация;
   d) виртуализация.

10. Выберите протоколы, составляющие ядро IPSec:
   a) IEEE 802.1q
   b) TCP
   c) ESP
   d) AH
   e) OSPF
   f) SSH
   g) DNS
   h) IKE
   i) SMTP

11. Можно ли межсетевой экран назвать Firewall?
   a) да
   b) нет
   c) затрудняюсь ответить

12. Установите соответствие между режимами работы и их описанием в Cisco IOS:

1. Пользовательский режим	a. доступны команды, позволяющие получить полную информацию о конфигурации оборудования и его состоянии
2. Привилегированный режим	d. доступны команды конфигурирования оборудования и команды перехода в режимы конфигурирования его подсистем
3. Конфигурационный режим	b. доступны только простые команды, не влияющие на конфигурацию оборудования.

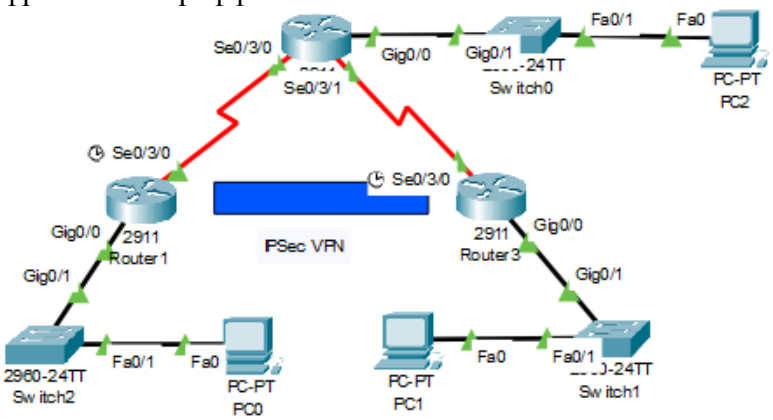
1. _____
2. _____
3. _____

13. Установите соответствие между режимами работы и приглашением командной строки в Cisco IOS:

1. Пользовательский режим	a. Router(config)#
2. Привилегированный режим	d. Router>
3. Конфигурационный режим	b. Router#

1. _____
2. _____
3. _____

14. Напишите консольную команду присвоения IP-адреса интерфейсу маршрутизатора.
15. Внимательно рассмотрите рисунок.
15.1 При настроенном туннелировании между R1 и R3 будет ли R2, находящийся между ними, видеть зашифрованный траффик?



a) да
b) нет
c) затрудняюсь ответить

15.2. Будет ли настроенный VPN препятствовать маршрутизации внутри сети от PC0 до PC2 или от PC0 до PC3?

a) да
b) нет
c) затрудняюсь ответить

16. Напишите два режима работы протокола IPSec.
17. Расскажите, какую информацию выведет команда:

```
R1# show crypto ipsec sa
```

18. Каким образом настроить L2-коммутатор, чтобы к нему можно было подключиться через SSH?

a) настроить SVI и задать ему IP-адрес как обычному интерфейсу
b) настроить VTY и задать ему IP-адрес как обычному интерфейсу
c) задать обычному интерфейсу коммутатора IP-адрес
d) коммутаторы L2-уровня невозможно настроить для SSH
e) затрудняюсь ответить

3.5 Перечень теоретических вопросов к экзамену

(для оценки знаний)

1. Различные подходы к определению VPN.
2. Цели и задачи применения VPN-технологий.
3. Механизм туннелирования как основа построения VPN.

4. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования.

5. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных.

6. Обработка входящих и исходящих пакетов.

7. Классификация VPN компании Check Point по типу устанавливаемых соединений. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности

8. VPN в сетях общего пользования.

9. Специфика использования VPN в сетях Frame Realay, ATM, X.25, TCP/IP

10. Функции протокола PPTP. Компоненты PPTP. Сценарии работы протокола.

11. Архитектура PPTP. Протокол L2TP: основные функции и характеристики протокола.

12. Управление L2TP-туннелем

13. Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec

14. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec

15. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов

16. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP

17. Использование комбинированных криптографических алгоритмов в ESP

18. Что такое криптографический ключ

19. Виды криптографических ключей

20. Процедуры использования ключей

21. Средство построения VPN АПКШ «Континент»

22. Средство построения VPN ViPNet

23. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования.

24. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных.

25. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec.

26. Функции протокола PPTP. Компоненты PPTP. Сценарии работы протокола.

27. Архитектура PPTP.

28. Протокол L2TP: основные функции и характеристики протокола.

29. Управление L2TP-туннелем.

30. Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec.

31. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec.

32. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов.

33. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP.

3.6 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

1. Последовательно напишите консольные команды, которые нужно ввести в CLI маршрутизатора для присвоения IP-адреса интерфейсу.
2. Перечислите три способа создания VLAN на коммутаторе Cisco с написанием команд.
3. Перечислите отличия проводов Cupper Cross-Over и Cupper Stright. Как они представлены в Cisco Packet Tracer?
4. Перечислите все семь уровней эталонной модели OSI. Расскажите, на каком уровне работает точка доступа, на каком маршрутизатор и на каком коммутатор. Какие данные передаются на каждом уровне?
5. Последовательно опишите действия для подключения к сетевому оборудованию через консоль.
6. Последовательно опишите действия, выполняемые при настройке SSH.
7. Последовательно опишите действия, выполняемые при настройке IPSec.
8. Напишите команду, которой можно проверить работоспособность VPN по IPSec.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Доклад	Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите
Лабораторная работа	Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено. Преподаватель на лабораторной работе, предшествующей занятию проведения защиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы. Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия

Для организации и проведения промежуточной аттестации составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике фондов оценочных средств.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

Образец экзаменационного билета

<table>
<tr><td>ИРГУПС
2023-2024
учебный год</td><td>Экзаменационный билет № 1
по дисциплине «<u>Виртуальные частные сети</u>»</td><td>Утверждаю:
Заведующий кафедрой
«ИСиЗИ» ИрГУПС
Кириллова Т.К.</td></tr>
<tr><td colspan="3">1. Различные подходы к определению VPN.
2. Управление L2TP-туннелем.
3. Виды криптографических ключей.
4. Архитектура PPTP.</td></tr>
</table>