1920

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Филиал федерального государственного бюджетного образовательного
учреждения высшего образования
«Кубанский государственный университет»
в г. Славянске-на-Кубани

УТВЕРЖДАЮ

Проректор по учебной работе,
качеству образования – первый
проректор

_____Т.А. Хагуров

«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.03.03 БЕЗОПАСНОСТЬ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

специальность 09.02.06 Сетевое и системное администрирование

Краснодар 2025

Рабочая программа учебной дисциплины МДК.03.03 БЕЗОПАСНОСТЬ СЕТЕВОЙ ИНФРАСТРУКТУРЫ разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.06 Сетевое и системное администрирование (технологический профиль), утвержденного приказом Министерства образования и науки Российской Федерации от «10» июля 2023 г. № 519, (зарегистрирован в Министерстве юстиции России 15.08.2023 г. рег. № 74796), и примерной основной образовательной программы по специальности 09.02.06 Сетевое и системное администрирование, утвержденной протоколом Федерального учебно-методического объединения по УГПС 09.00.00 №3 от 15.07.2021 г. (зарегистрировано в государственном реестре примерных основных образовательных программ регистрационный номер 5, приказ ФГБОУ ДПО ИРПО № П-24 от 02.02.2022 г.).

Дисциплина	МДК.03.03 БЕЗОПАСНОСТЬ СЕТЕВОЙ ИНФРАСТРУКТУРЫ	
Форма обучения	очная	
Учебный год	2025-2026	
3,4 курс	6 семестр	7 семестр
всего 252 часа, в том числе:		
лекции	40 ч.	66 ч.
практические занятия	40 ч.	44 ч.
самостоятельные занятия	–	–
консультация	–	–
промежуточная аттестация	–	12 ч.
форма итогового контроля	зачет	экзамен

Составитель: преподаватель _____ Р.Р. Сабиров

Утверждена на заседании предметной (цикловой) комиссии физико-математических дисциплин и специальных дисциплин УГС 09.00.00 Информатика и вычислительная техника протокол № 10 от «29» мая 2025 г.

Председатель предметной (цикловой) комиссии:

_____ М.С. Бушуев

«29» мая 2025 г.

Рецензенты:

Технический директор
ООО «Техностарт» _____ И.Г. Колодезный

Технический директор
ООО «ПРАЙ» _____ Б.А. Шишкин

ЛИСТ
согласования рабочей программы по учебной дисциплине
МДК.03.03 «Безопасность сетевой инфраструктуры»

Специальность среднего профессионального образования:
09.02.06 Сетевое и системное администрирование

СОГЛАСОВАНО:

Нач. УМО филиала _____ А.С. Демченко
«29» мая 2025 г.

Заведующая библиотекой филиала _____ Н.И. Головлева
«29» мая 2025 г.

Нач. ИВЦ (программно-
информационное обеспечение
образовательной программы) _____ В.А. Ткаченко
«29» мая 2025 г.

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Область применения программы

Рабочая программа учебной дисциплины «Безопасность сетевой инфраструктуры» является частью основной профессиональной образовательной программы в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее ФГОС СПО) для специальности 09.02.06 Сетевое и системное администрирование.

1.2 Место дисциплины в структуре программы подготовки специалистов среднего звена

Дисциплина «Безопасность сетевой инфраструктуры» относится к профессиональному модулю «Эксплуатация объектов сетевой инфраструктуры».

1.3 Цели и задачи учебной дисциплины - требования к результатам освоения дисциплины

В результате изучения профессионального модуля обучающийся должен

иметь практический опыт в:

- Проектировать архитектуру локальной сети в соответствии с поставленной задачей.
- Использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей.
- Настраивать протоколы динамической маршрутизации.
- Определять влияния приложений на проект сети.
- Анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети.
- Устанавливать и настраивать сетевые протоколы и сетевое оборудование в соответствии с конкретной задачей.
- Выбирать технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры.
- Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.
- Выполнять поиск и устранение проблем в компьютерных сетях.
- Отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны.
- Настраивать коммутацию в корпоративной сети.
- Обеспечивать целостность резервирования информации.
- Обеспечивать безопасное хранение и передачу информации в глобальных и локальных сетях.
- Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.
- Выполнять поиск и устранение проблем в компьютерных сетях.

– Отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны.

– Фильтровать, контролировать и обеспечивать безопасность сетевого трафика.

– Определять влияние приложений на проект сети.

– Мониторинг производительности сервера и протоколирования системных и сетевых событий.

– Использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей.

– Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.

– Создавать подсети и настраивать обмен данными;

– Выполнять поиск и устранение проблем в компьютерных сетях.

– Анализировать схемы потоков трафика в компьютерной сети.

– Оценивать качество и соответствие требованиям проекта сети.

– Оформлять техническую документацию.

– Определять влияние приложений на проект сети.

– Анализировать схемы потоков трафика в компьютерной сети.

– Оценивать качество и соответствие требованиям проекта сети

уметь:

– Проектировать локальную сеть.

– Выбирать сетевые топологии.

– Рассчитывать основные параметры локальной сети.

– Применять алгоритмы поиска кратчайшего пути.

– Планировать структуру сети с помощью графа с оптимальным расположением узлов.

– Использовать математический аппарат теории графов.

– Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

– Выбирать сетевые топологии.

– Рассчитывать основные параметры локальной сети.

– Применять алгоритмы поиска кратчайшего пути.

– Планировать структуру сети с помощью графа с оптимальным расположением узлов.

– Использовать математический аппарат теории графов.

– Использовать многофункциональные приборы и программные средства мониторинга.

– Использовать программно-аппаратные средства технического контроля

– Использовать программно-аппаратные средства технического контроля.

– Читать техническую и проектную документацию по организации сегментов сети.

– Контролировать соответствие разрабатываемого проекта нормативно-технической документации.

– Использовать программно-аппаратные средства технического контроля.

– Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.

– Читать техническую и проектную документацию по организации сегментов сети.

– Контролировать соответствие разрабатываемого проекта нормативно-технической документации.

– Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.

знать:

– Общие принципы построения сетей.

- Сетевые топологии.
- Многослойную модель OSI.
- Требования к компьютерным сетям.
- Архитектуру протоколов.
- Стандартизацию сетей.
- Этапы проектирования сетевой инфраструктуры.
- Элементы теории массового обслуживания.
- Основные понятия теории графов.
- Алгоритмы поиска кратчайшего пути.
- Основные проблемы синтеза графов атак.
- Системы топологического анализа защищенности компьютерной сети.
- Основы проектирования локальных сетей, беспроводные локальные сети.
- Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.
- Средства тестирования и анализа.
- Базовые протоколы и технологии локальных сетей.
- Общие принципы построения сетей.
- Сетевые топологии.
- Стандартизацию сетей.
- Этапы проектирования сетевой инфраструктуры.
- Элементы теории массового обслуживания.
- Основные понятия теории графов.
- Основные проблемы синтеза графов атак.
- Системы топологического анализа защищенности компьютерной сети.
- Архитектуру сканера безопасности.
- Принципы построения высокоскоростных локальных сетей.
- Требования к компьютерным сетям.
- Требования к сетевой безопасности.
- Элементы теории массового обслуживания.
- Основные понятия теории графов.
- Основные проблемы синтеза графов атак.
- Системы топологического анализа защищенности компьютерной сети.
- Архитектуру сканера безопасности.
- Требования к компьютерным сетям.
- Архитектуру протоколов.
- Стандартизацию сетей.
- Этапы проектирования сетевой инфраструктуры.
- Организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей.
- Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.
- Средства тестирования и анализа.
- Программно-аппаратные средства технического контроля.
- Принципы и стандарты оформления технической документации
- Принципы создания и оформления топологии сети.
- Информационно-справочные системы для замены (поиска) технического оборудования

Максимальная учебная нагрузка обучающегося 202 часов, в том числе:

– обязательная аудиторная учебная нагрузка обучающегося 190 часа;
– итоговая аттестация 12 часов.

1.4. Перечень планируемых результатов обучения по дисциплине (Перечень формируемых компетенций)

Освоение дисциплины «Безопасность сетевой инфраструктуры» способствует формированию у студентов следующих профессиональных компетенций:

ПК 3.1. Осуществлять проектирование сетевой инфраструктуры
ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств
ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств
ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры
ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем

Одновременно с профессиональными компетенциями у студентов, обучающихся по дисциплине «Безопасность сетевой инфраструктуры» создаются предпосылки для формирования общих компетенций:

ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04 Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09 Пользоваться профессиональной документацией на государственном и

иностранном языках

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы.

Вид учебной работы	Всего часов	Семестры	
		6	7
Обязательная учебная нагрузка (всего)	190	80	110
В том числе:			
занятия лекционного типа	106	40	66
практические занятия (практикумы)	84	40	44
Курсовое проектирование			
Самостоятельная работа (всего)			
Вид итоговая аттестация (экзамен)	12	–	12
Общая трудоемкость 244 часов	202	80	122

2.2 Структура дисциплины

Наименование разделов и тем	**Количество аудиторных часов**			**Самостоя-тельная работа обучающегося (час)**
	Всего	**Теоретическое обучение**	**Практические и лабораторные занятия**	
Тема 3.1. Безопасность компьютерных сетей	82	46	36	–
Тема 3.2. Обеспечение сетевой безопасности	108	60	48	–
Всего	190	106	84	–

2.3 Тематический план и содержание учебной дисциплины МДК.03.03 Безопасность сетевой инфраструктуры

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)** (если предусмотрены)	**Объем, акад. ч / в том числе в форме практической подготовки, акад ч**
Тема 3.1. Безопасность компьютерных сетей	**Содержание**	82/36
	1. **Фундаментальные принципы безопасной сети** Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	46
	2. **Безопасность сетевых устройств OSI** Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.	
	3. **Авторизация, аутентификация и учет доступа (AAA)** Свойства AAA. Локальная AAA аутентификация. Server-based AAA	
	4. **Реализация технологий брандмауэра ACL.**	

	Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах.	
	5. **Реализация технологий предотвращения вторжения** IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	
	6. **Безопасность локальной сети** Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN	
	7. **Криптографические системы** Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей	
	8. **Реализация технологий VPN** VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN с использованием CLI. Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN	
	9. **Управление безопасной сетью** Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности.	
	10. **Безопасность облачных вычислений** Особенности безопасности облачных вычислений, риски и угрозы. Защита от атак в облачной среде, использование механизмов контроля доступа, мониторинга и аудита, а также методов криптографической защиты данных.	
	11. Межсетевая безопасность Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей.	
	12. Безопасность веб-приложений и мобильных устройств Особенности уязвимостей веб-приложений, методы их эксплуатации, а также средства защиты. Разработка безопасных веб-приложений, использование методов автоматического тестирования и уязвимости. Угрозы безопасности мобильных устройств, методы защиты от вредоносных программ, защита данных и коммуникаций, а также безопасное использование мобильных устройств.	
	13. Защита от социальной инженерии Методы социальной инженерии, опасности, связанные с подделкой и манипулированием данными, а также методы защиты и обучения персонала.	

	В том числе практических занятий и лабораторных работ	**36**
	Практическое занятие 1. Социальная инженерия	36
	Практическое занятие 2. Исследование сетевых атак и инструментов проверки защиты сети	
	Практическое занятие 3. Настройка безопасного доступа к маршрутизатору	
	Практическое занятие 4. Обеспечение административного доступа AAA и сервера Radius	
	Практическое занятие 5. Настройка политики безопасности брандмауэров	
	Практическое занятие 6. Настройка системы предотвращения вторжений (IPS)	
	Практическое занятие 7. Настройка безопасности на втором уровне на коммутаторах	
	Практическое занятие 8. Исследование методов шифрования	
	Практическое занятие 9. Настройка Site-to-SiteVPN используя интерфейс командной строки	
	Практическое занятие 10. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	
	Практическое занятие 11. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM	
	Практическое занятие 12. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM	
	Практическое занятие 13. НастройкаClientless Remote Access SSL VPNs используя ASDM	
	Практическое занятие 14. Настройка AnyConnect Remote Access SSL VPN используя ASDM	
	Практическое занятие 15. Комплексная лабораторная работа по безопасности	
Тема 3.2. Обеспечение сетевой безопасности	**Содержание**	108/48
	1. Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть.	600
	2. Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.	
	3. Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	
	4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.	
	5. Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.	

	6. Введение системы обнаружения и предотвращения сетевых вторжений.	
	7. Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.	
	8. Использование системы управления доступом для контроля доступа к корпоративной сети.	
	9. Обеспечение безопасности Wi-Fi-сетей.	
	10. Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.	
	11. Защита от атак типа "фишинг".	
	12. Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.	
	13. Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	
	14. Защита от DDoS-атак.	
	15. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.	
	16. Защита от внутренних угроз безопасности.	
	17. Обеспечение безопасности облачных сервисов.	
	18. Организация мониторинга сетевой безопасности и аудита.	
	19. Введение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.	
	20. Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.	
	В том числе практических занятий и лабораторных работ	**48**
	Практическое занятие 1. Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами.	48
	Практическое занятие 2. Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	
	Практическое занятие 3. Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	
	Практическое занятие 4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз.	

	Практическое занятие 5. Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.	
	Практическое занятие 6. Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.	
	Практическое занятие 7. Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	
	Практическое занятие 8. Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети.	
	Практическое занятие 9. Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов.	
	Практическое занятие 10. Разработка и внедрение мер по обеспечению безопасности электронной почты в корпоративной сети: настройка антивирусного программного обеспечения, проверка на наличие вредоносных вложений, обучение пользователей основам безопасности электронной почты.	
	Практическое занятие 11. Обучение пользователям основам защиты от атак типа "фишинг".	
	Практическое занятие 12. Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ.	
	Практическое занятие 13. Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	
	Практическое занятие 14. Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	
	Практическое занятие 15. Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.	
	Практическое занятие 16. Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.	
	Практическое занятие 17.Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика,	

	аутентификация пользователей.	
	Практическое занятие 18. Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности.	
	Практическое занятие 19. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети: настройка политик безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах.	
	Практическое занятие 20. Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.	
	Промежуточная аттестация	9
	Итог	202

2.4 Содержание разделов дисциплины

2.4	**.1 Занятия лекционного типа**		
№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	**Тема 3.1. Безопасность компьютерных сетей**	**Фундаментальные принципы безопасной сети** Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак. **Безопасность сетевых устройств OSI** Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности. **Авторизация, аутентификация и учет доступа (AAA)** Свойства AAA. Локальная AAA аутентификация. Server-based AAA **Реализация технологий брандмауэра ACL.** Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах. **Реализация технологий предотвращения вторжения** IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS **Безопасность локальной сети** Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN **Криптографические системы** Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей **Реализация технологий VPN** VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN с использованием CLI. Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN **Управление безопасной сетью** Принципы безопасности сетевого дизайна. Безопасная архитектура.	У,Р

		Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности. **Безопасность облачных вычислений** Особенности безопасности облачных вычислений, риски и угрозы. Защита от атак в облачной среде, использование механизмов контроля доступа, мониторинга и аудита, а также методов криптографической защиты данных. **Межсетевая безопасность** Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей. **Безопасность веб-приложений и мобильных устройств** Особенности уязвимостей веб-приложений, методы их эксплуатации, а также средства защиты. Разработка безопасных веб-приложений, использование методов автоматического тестирования и уязвимости. Угрозы безопасности мобильных устройств, методы защиты от вредоносных программ, защита данных и коммуникаций, а также безопасное использование мобильных устройств. **Защита от социальной инженерии** Методы социальной инженерии, опасности, связанные с подделкой и манипулированием данными, а также методы защиты и обучения персонала.	
2	**Тема 3.2. Обеспечение сетевой безопасности**	Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть. Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам. Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети. Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях. Введение системы обнаружения и предотвращения сетевых вторжений. Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа. Использование системы управления доступом для контроля доступа к корпоративной сети. Обеспечение безопасности Wi-Fi-сетей. Реализация мер по обеспечению безопасности электронной почты в корпоративной сети. Защита от атак типа "фишинг". Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ. Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности. Защита от DDoS-атак. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети. Защита от внутренних угроз безопасности. Обеспечение безопасности облачных сервисов. Организация мониторинга сетевой безопасности и аудита. Введение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы. Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.	У,Р

2.4.2 Занятия семинарского типа

- не предусмотрены

2.4	.3 Практические занятия (Лабораторные занятия)		
№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	**Тема 3.1. Безопасность компьютерных сетей**	Практическое занятие 1. Социальная инженерия Практическое занятие 2. Исследование сетевых атак и инструментов проверки защиты сети Практическое занятие 3. Настройка безопасного доступа к маршрутизатору Практическое занятие 4. Обеспечение административного доступа AAA и сервера Radius Практическое занятие 5. Настройка политики безопасности брандмауэров Практическое занятие 6. Настройка системы предотвращения вторжений (IPS) Практическое занятие 7. Настройка безопасности на втором уровне на коммутаторах Практическое занятие 8. Исследование методов шифрования Практическое занятие 9. Настройка Site-to-SiteVPN используя интерфейс командной строки Практическое занятие 10. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки Практическое занятие 11. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM Практическое занятие 12. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM Практическое занятие 13. НастройкаClientless Remote Access SSL VPNs используя ASDM Практическое занятие 14. Настройка AnyConnect Remote Access SSL VPN используя ASDM Практическое занятие 15. Комплексная лабораторная работа по безопасности	Т, Пр.Р
2	**Тема 3.2. Обеспечение сетевой безопасности**	Практическое занятие 1. Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами. Практическое занятие 2. Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам. Практическое занятие 3. Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. Практическое занятие 4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз. Практическое занятие 5. Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях. Практическое занятие 6. Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности. Практическое занятие 7. Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	Т, Пр.Р

		Практическое занятие 8. Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети. Практическое занятие 9. Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов. Практическое занятие 10. Разработка и внедрение мер по обеспечению безопасности электронной почты в корпоративной сети: настройка антивирусного программного обеспечения, проверка на наличие вредоносных вложений, обучение пользователей основам безопасности электронной почты. Практическое занятие 11. Обучение пользователям основам защиты от атак типа "фишинг". Практическое занятие 12. Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ. Практическое занятие 13. Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности. Практическое занятие 14. Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. Практическое занятие 15. Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями. Практическое занятие 16. Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика. Практическое занятие 17.Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей. Практическое занятие 18. Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности. Практическое занятие 19. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети: настройка политик безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах. Практическое занятие 20. Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.	

2.4.4 Содержание самостоятельной работы (Примерная тематика рефератов)

– Не предусмотрено

2.4.5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

– Не предусмотрено

3 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для обучения организации администрирования компьютерных систем предусматривается использование в учебном процессе активных и интерактивных форм проведения аудиторных и внеаудиторных занятий с целью формирования и развития профессиональных навыков обучающихся.

В процессе обучения применяются образовательные технологии личностно-деятельностного, развивающего и проблемного обучения. Обязателен лабораторный практикум по разделам дисциплины.

В учебном процессе наряду с традиционными образовательными технологиями используются компьютерное тестирование, тематические презентации, интерактивные технологии.

3.1 Образовательные технологии при проведении лекций

Тема	Виды применяемых образовательных технологий	Кол-во часов
Тема 3.1. Безопасность компьютерных сетей	Технология развивающего обучения Аудиовизуальные технологии	46(30*)
Тема 3.2. Обеспечение сетевой безопасности	Технология развивающего обучения Аудиовизуальные технологии	60 (40*)
Всего по дисциплине (в том числе интерактивное обучение*)		106(70*)

3.2 Образовательные технологии при проведении практических и лабораторных занятий

Тема	Виды применяемых образовательных технологий	Кол-во часов
Тема 3.1. Безопасность компьютерных сетей	Технология развивающего обучения	36(34*)
Тема 3.2. Обеспечение сетевой безопасности	Технология личностно-деятельностного обучения	48(42*)
Всего по дисциплине (в том числе интерактивное обучение*)		84(76*)

4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Лаборатории «Информационных технологий», «Направляющих систем» оснащенные в соответствии с п. 6.1.2.3 примерной образовательной программы по специальности 09.02.06 Сетевое и системное администрирование.

Мастерские «Монтажа и настройки объектов сетевой инфраструктуры, «Ремонта и обслуживания устройств инфокоммуникационных систем» оснащенные в соответствии с п. 6.1.2.4. примерной образовательной программы по специальности 09.02.06 Сетевое и системное администрирование.

Оснащенные базы практики, в соответствии с п 6.1.2.5 примерной образовательной программы по специальности 09.02.06 Сетевое и системное администрирование.

4.2 Перечень необходимого программного обеспечения

1. 7-zip(лицензия на англ. http://www.7-zip.org/license.txt)
2. Adobe Acrobat Reade (лицензия -https://get.adobe.com/reader/?loc=ru&promoid=KLXME)
3. Adobe Flash Player (лицензия- https://get.adobe.com/reader/?loc=ru&promoid=KLXME)
4. Apache Open Office (лицензия- http://www.openoffice.org/license.html)
5. Free Commander (лицензия- https://freecommander.com/ru/%d0%bb%d0%b8%d1%86%d0%b5%d0%bd%d0%b7%d0%b8%d1%8f/)
6. Google Chrome (лицензия- https://www.google.ru/chrome/browser/privacy/eula_text.html)
7. LibreOffice(в свободном доступе)
8. Mozilla Firefox (лицензия- https://www.mozilla.org/en-US/MPL/2.0/)
9. VirtualBox (в свободном доступе)

5 ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИ ТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1 Основная литература

1. Назаров, А. В. Безопасность сетевой инфраструктуры : учебник / А. В. Назаров, А. Н. Енгалычев, В. П. Мельников. - Москва : КУРС ; ИНФРА-М, 2020. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-06-6. - URL: https://znanium.com/catalog/product/1071722.

2. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/book/seti-i-telekommunikacii-456638 .

5.2 Дополнительная литература

1. Ковган, Н М. Компьютерные сети : учебное пособие : [16+] / Н. М. Ковган. – Минск : РИПО, 2019. – 180 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599948.– Библиогр. в кн. – ISBN 978-985-503-947-2. – Текст : электронный.

2. Кузин, А. В. Компьютерные сети : учебное пособие / А. В. Кузин, Д. А. Кузин. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 190 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-453-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088380.– Режим доступа: по подписке

3. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А. В. Васильков, И. А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1082470.Режим доступа: по подписке.

4. Тенгайкин, Е. А. Организация сетевого администрирования. Сетевые операционные системы, серверы, службы и протоколы. Практические работы : учебное пособие / Е. А. Тенгайкин. — Санкт-Петербург : Лань, 2020. — 100 с. — ISBN 978-5-8114-4763-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139326 . — Режим доступа: для авториз. пользователей.

5. Тенгайкин, Е. А. Организация сетевого администрирования. Сетевые операционные системы, серверы, службы и протоколы. Лабораторные работы : учебное пособие / Е. А. Тенгайкин. — Санкт-Петербург : Лань, 2020. — 128 с. — ISBN 978-5-8114-4734-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/136178 . — Режим доступа: для авториз. пользователей.

5.3 Периодические издания

1. Computerworld Россия. – URL: http://dlib.eastview.com/browse/publication/64081/udb/2071.
2. Windows IT Pro / Re. – URL: http://dlib.eastview.com/browse/publication/64079/udb/2071.
3. БИТ. Бизнес & информационные технологии – URL : http://dlib.eastview.com/browse/publication/66752/udb/2071.
4. Вестник Московского Университета. Серия 15. Вычислительная математика и кибернетика. - URL: https://dlib.eastview.com/browse/publication/9166.
5. Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. URL: https://dlib.eastview.com/browse/publication/71227/udb/2630.
6. Виртуализация. Облачные структуры. Системы хранения данных. – URL : https://dlib.eastview.com/browse/publication/84826/udb/2071.
7. Журнал сетевых решений LAN. – URL: http://dlib.eastview.com/browse/publication/64078/udb/2071.
8. Защита персональных данных. – URL : https://dlib.eastview.com/browse/publication/90727/udb/2071.
9. Информатика и образование. - URL: http://dlib.eastview.com/browse/publication/18946/udb/1270.
10. Информатика, вычислительная техника и инженерное образование. - URL: https://www.elibrary.ru/title_about.asp?id=32586.
11. Информационно-управляющие системы. – URL: http://dlib.eastview.com/browse/publication/71235.
12. Мир больших данных. – URL : https://dlib.eastview.com/browse/publication/90728/udb/2071.
13. Новые информационные технологии в автоматизированных системах https://elibrary.ru/title_about.asp?id=32949.
14. Прикладная информатика. – URL: https://e.lanbook.com/journal/2067#journal_name.
15. Проблемы передачи информации. – URL: http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&wshow=contents&option_lang=rus
16. Системный администратор. – URL: https://dlib.eastview.com/browse/publication/66751/udb/2071.
17. Системный анализ и прикладная информатика. – URL: https://e.lanbook.com/journal/2420#journal_name.
18. Управление проектами и программами. – URL : https://grebennikon.ru/journal-20.html#volume2019-3.

5.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Электронно-библиотечные системы (ЭБС)

1. ЭБС «BOOK.ru» [учебная литература, журналы]. – URL: https://www.book.ru.
2. ЭБ ОИЦ «Академия» [учебные издания по общеобразовательным дисциплинам СПО для первого курса, включенных в ФПУ]. – URL: https://academia-moscow.ru/elibrary/.
3. ЭБС «Университетская библиотека онлайн» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы; коллекция медиа-материалов: аудиокниги, аудиофайлы, видеокурсы, экспресс-подготовка к экзаменам, презентации, тесты, карты, онлайн-энциклопедии, словари]. – URL: http://www.biblioclub.ru/.
4. ЭБС «ZNANIUM» [учебные, научные, справочные, научно-популярные издания различных издательств, журналы]. – URL: https://znanium.ru/.
5. ЭБС «Лань» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы]. – URL: http://e.lanbook.com/.
6. Образовательная платформа «Юрайт» [учебники и учебные пособия издательства «Юрайт», медиа-материалы, тесты]. – URL: https://urait.ru/.

Профессиональные базы данных

1. Виртуальный читальный зал Российской государственной библиотеки (РГБ). – URL: https://ldiss.rsl.ru/.
2. Национальная электронная библиотека (НЭБ) [включает Электронную библиотеку диссертаций РГБ] : [федеральная государственная информационная система Министерства культуры РФ]. – URL: https://rusneb.ru/ (полный доступ к объектам НЭБ – в локальной сети с компьютеров библиотеки филиала).
3. Научная электронная библиотека «eLIBRARY.RU» [российские научные журналы, труды конференций; Российская национальная база данных научного цитирования (РИНЦ)]. – URL: http://www.elibrary.ru/.
4. Универсальные базы данных «ИВИС» [российские научные журналы по вопросам педагогики и образования, экономики и финансов, информационным технологиям, экономике и предпринимательству, общественным и гуманитарным наукам, индивидуальные издания, Вестники МГУ, СПбГУ, статистические издания России и стран СНГ]. – URL: https://eivis.ru/basic/details.
5. Полнотекстовая коллекция журналов на платформе РЦНИ. Национальная платформа периодических научных изданий. – URL: https://journals.rcsi.science/.
6. Общероссийский портал «Math-Net.Ru» : информационная система доступа к научной информации по математике, физике, информационным технологиям и смежным наукам / Математический институт имени В. А. Стеклова РАН. – URL: http://www.mathnet.ru/.
7. Президентская библиотека им. Б.Н. Ельцина. – URL: https://www.prlib.ru/.

Информационные справочные системы

1. КонсультантПлюс: справочная правовая система (доступ – в локальной сети с компьютеров библиотеки филиала).

Ресурсы свободного доступа

1. Официальный интернет-портал правовой информации. Государственная система правовой информации. – URL: http://pravo.gov.ru/

2. КонсультантПлюс : некоммерческая интернет-версия справочной правовой системы. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=home&utm_csource=online&utm_cmedium=button.

3. Министерство науки и высшего образования Российской Федерации (Минобрнауки России) - официальный сайт. – URL: https://www.minobrnauki.gov.ru

4. Министерство просвещения Российской Федерации - официальный сайт. – URL: https://edu.gov.ru

5. Портал «Культура.РФ» : гуманитарный просветительский проект, посвященный культуре России [кино, музеи, музыка, театры, архитектура, литература, персоны, традиции, лекции-онлайн] : сайт / Министерство культуры РФ. – URL: https://www.culture.ru/.

6. Справочно-информационный портал «Грамота.ру» / Министерство цифрового развития, связи и массовых коммуникаций РФ. – URL: http://www.gramota.ru/.

7. Лекториум [раздел «Медиатека» – открытый видеоархив лекций на русском языке]: образовательная платформа : сайт. – URL: https://www.lektorium.tv/medialibrary.

8. Научная электронная библиотека «КиберЛенинка» [российские научные журналы]. – URL: http://cyberleninka.ru/.

9. Большая российская энциклопедия: [электронная версия] / Министерство культуры РФ. – URL: https://bigenc.ru/.

10. Лингвистический проект «СЛОВАРИ.РУ» / Институт русского языка им. В. В. Виноградова РАН. – URL: http://slovari.ru/start.aspx?s=0&p=3050.

Собственные электронные образовательные и информационные ресурсы

1. База информационных потребностей [КубГУ и филиалов] (разделы: Научные публикации преподавателей и обучающихся; Информация об участии преподавателей и обучающихся в научных конференциях; Темы выпускных квалификационных работ студентов). – URL: https://infoneeds.kubsu.ru/infoneeds/.

2. Электронная библиотека информационных ресурсов филиала [КубГУ в г. Славянске-на-Кубани]. – URL: http://sgpi.ru/bip.php.

3. Поступления литературы в библиотеки филиалов : [электронный каталог библиотек филиалов КубГУ]. – URL: http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=1.

4. Электронная библиотека трудов учёных КубГУ. – URL: http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=6.

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учащиеся для полноценного освоения курса «Безопасность сетевой инфраструктуры» должны составлять конспекты как при прослушивании его теоретической (лекционной) части, так и при подготовке к практическим (семинарским) занятиям. Желательно, чтобы конспекты лекций и семинаров записывались в логической последовательности изучения курса и содержались в одной тетради. Это обеспечит более полную подготовку как к текущим учебным занятиям, так и сессионному контролю знаний.

Самостоятельная работа учащихся является важнейшей формой учебно-познавательного процесса. Цель заданий для самостоятельной работы - закрепить и расширить знания, умения, навыки, приобретенные в результате изучения дисциплины; овладеть умением использовать полученные знания в практической работе; получить первичные навыки профессиональной деятельности по установке, настройке и обслуживанию технических и программно-аппаратных средств компьютерных сетей.

Задания для самостоятельной работы выполняются в письменном виде во внеаудиторное время. Работа должна носить творческий характер, при ее оценке преподаватель в первую очередь оценивает обоснованность и оригинальность выводов. В письменной работе по теме задания учащийся должен полно и всесторонне рассмотреть все аспекты темы, четко сформулировать и аргументировать свою позицию по исследуемым вопросам.

Отчеты по лабораторным и практическим занятиям должны содержать полные ответы на поставленные задания, необходимые таблицы должны быть заполнены. Защита лабораторных работ будет включать в себя просмотр письменных отчетов, устный опрос.

Общие правила выполнения письменных работ

На первом занятии студенты должны быть проинформированы о необходимости соблюдения норм академической этики и авторских прав в ходе обучения. В частности, предоставляются сведения:

1. общая информация об авторских правах;
2. правила цитирования;
3. правила оформления ссылок;

Все имеющиеся в тексте сноски тщательно выверяются и снабжаются «адресами».

Недопустимо включать в свою работу выдержки из работ других авторов без указания на это, пересказывать чужую работу близко к тексту без отсылки к ней, использовать чужие идеи без указания первоисточников (это касается и информации, найденной в Интернете). Все случаи плагиата должны быть исключены.

Список использованной литературы должен включать все источники информации, изученные и проработанные студентом в процессе выполнения работы, и должен быть составлен в соответствии с ГОСТ Р 7.0.5-2008 «Библиографическая ссылка. Общие требования и правила».

6. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

7.1 Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Компетенции	Наименование оценочного средства
1.	**Тема 3.1. Безопасность компьютерных сетей**	ОК 1-9, ПК 3.1 – 3.5	Проверка конспектов, практ. работа, тест
2.	**Тема 3.2. Обеспечение сетевой безопасности**	ОК 1-9, ПК 3.1 – 3.5	Проверка конспектов, практ. работа, тест

7.2 Критерии оценки результатов обучения

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических работ, тестирования, собеседования по результатам выполнения лабораторных работ, а также решения задач, составления рабочих таблиц и подготовки сообщений к уроку. Знания студентов на практических занятиях оцениваются отметками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Код и наименование ПК и ОК, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять проектирование сетевой инфраструктуры ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем	Определение профессиональной задачи и этапов ее выполнения Эффективный поиск информации для решения профессиональной задачи Определение ресурсов для решения профессиональной задачи Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «хорошо» -алгоритм разработан,	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Защита отчетов по практическим и лабораторным работам Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной

	оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	программы
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различными контекстам	Подбор вариантов решения конкретной профессиональной задачи или проблемы	Оценка полноты перечня подобранных вариантов
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Демонстрация навыков использования информационных порталов в сети Интернет, включая официальные информационно-правовые порталы	Оценка полноты перечня подобранных вариантов
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	Демонстрация интереса к выбранной специальности, к инновационным технологиям в области профессиональной деятельности	Участие в мероприятиях (олимпиады, конкурсы профессионального мастерства, стажировки и др.), проводимых как образовательным заведением, так и ведущими предприятиями отрасли
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	Демонстрировать навыки межличностного общения с соблюдением общепринятых правил со сверстниками в образовательной группе, с преподавателями во время обучения, с руководителями производственной практики	Экспертное наблюдение поведенческих навыков в ходе обучения
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	Демонстрация навыков грамотной устной и письменной речи	Экспертное наблюдение навыков устного и письменного общения в ходе обучения
ОК 06. Проявлять	Формирование чувства	Участие в

гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению; взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации; нетерпимости к коррупционным проявлениям	мероприятиях патриотической направленности, в проведении военно-спортивных игр; участие в программах антикоррупционной направленности
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	Формирование бережного отношения к природе и окружающей среде	Экспертное наблюдение демонстрации навыков соблюдения правил экологической безопасности в ведении профессиональной деятельности; формирование навыков эффективных действий в чрезвычайных ситуациях
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Формирование бережного отношения к здоровью	Участие в спортивных мероприятиях, проводимых образовательным учреждением; ведение здорового образа жизни
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	Демонстрация умения составлять тексты документов, относящихся к профессиональной деятельности, на государственном и иностранном языках	Экспертная оценка соблюдения правил составления документов

7.3 Оценочные средства для проведения текущей аттестации

Текущий контроль может проводиться в форме:

-фронтальный опрос

-индивидуальный устный опрос

-письменный контроль

-тестирование по теоретическому материалу

-практическая (лабораторная) работа

-защита выполненного задания,

Форма аттестации	Знания	Умения	Владения (навыки)	Личные качества студента	Примеры оценочных средств
Устный (письменный) опрос по темам	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков работы с литературными источниками	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Контрольные вопросы по темам прилагаются
Практические (лабораторные) работы	Контроль знания теоретических основ информатики и информационных технологий, возможностей и принципов использования современной компьютерной техники.	Оценка умения работать с современной компьютерной техникой, использовать возможности вычислительной техники и программного обеспечения при решении практических задач.	Оценка навыков работы с техническими средствами информатизации, специальными программными средствами	Оценка способности оперативно и качественно решать поставленные на практических работах задачи и аргументировать результаты	Темы работ прилагаются
Тестирование	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков логического анализа и синтеза при сопоставлении конкретных понятий	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Вопросы прилагаются

Контрольная работа. Контрольная работа является набором практических заданий и задач по темам изучаемой дисциплины, позволяющих формировать знания, а также умения обучающихся в области физики.

Примеры задач и вопросов к контрольной работе:

1. Опишите понятия активное и пассивное сетевое оборудование. Приведите примеры.
2. Что называется расширяемостью сети?
3. Что называется масштабируемостью сети?
4. Понятие технической и проектной документации.
5. Паспорт технического устройства. Руководство по эксплуатации.

Примеры тестовых заданий:

1. Что НЕ является каналом передачи данных?

а. витая пара

б. коаксиальный кабель

в. алюминиевая жила

г. оптоволокно

2. Что помогает более гибко настраивать сеть при её расширении?

а. нормативы

б. инструменты

в. приборы

г. стандарты

3. Что понимают под физической инфраструктурой сети?

а. сетевое оборудование, соединенное кабелем

б. топологию со всем сетевым оборудованием и транспортными технологиями

в. ПК с прописанными IP- адресами

г. сетевое оборудование, каналы связи и протоколы передачи данных

4. Основная и наиболее протяженная часть компьютерной сети - это

а. сегмент

б. телефонная линия связи

в. структурированная кабельная система

г. патч - панель

5. Быстро проверить качество работы только что настроенной локальной сети поможет

а. кабельный тестер

6. утилита ping

в. сетевая операционная система

г. протокол TCP/IP 4версии

7.4 Оценочные средства для проведения промежуточной аттестации

Форма аттестации	Знания	Умения	Владение (навыки)	Личные качества студента	Примеры оценочных средств
Итоговая аттестация					

Зачет	Контроль знания базовых положений в области администрирования компьютерных систем	Оценка умения понимать специальную терминологию	Оценка навыков логического сопоставления и характеристики объектов	Оценка способности грамотно и четко излагать материал	Вопросы прилагаются
Экзамен	Контроль знания базовых положений в области администрирования компьютерных систем	Оценка умения решать типовые задачи в области эксплуатации объектов сетевой инфраструктуры	Оценка навыков логического мышления при решении задач в области эксплуатации объектов сетевой инфраструктуры	Оценка способности грамотно и четко излагать ход решения задач в области эксплуатации объектов сетевой инфраструктуры	Вопросы прилагаются

7.4.1 Примерные вопросы для проведения промежуточной аттестации

Вопросы экзамена

1. Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть.
2. Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.
3. Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.
4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.
5. Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.
6. Введение системы обнаружения и предотвращения сетевых вторжений.
7. Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.
8. Использование системы управления доступом для контроля доступа к корпоративной сети.
9. Обеспечение безопасности Wi-Fi-сетей.
10. Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.
11. Защита от атак типа "фишинг".
12. Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.
13. Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.
14. Защита от DDoS-атак.
15. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.
16. Защита от внутренних угроз безопасности.
17. Обеспечение безопасности облачных сервисов.
18. Организация мониторинга сетевой безопасности и аудита.
19. Введение системы контроля целостности файлов для защиты от изменения

или внедрения вредоносных программ в файловые системы.

20. Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.

7.4.2 Примерные задачи для проведения промежуточной аттестации

1. Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами.
2. Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.
3. Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.
4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз.
5. Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.
6. Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.
7. Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.
8. Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети.
9. Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов.
10. Разработка и внедрение мер по обеспечению безопасности электронной почты в корпоративной сети: настройка антивирусного программного обеспечения, проверка на наличие вредоносных вложений, обучение пользователей основам безопасности электронной почты.
11. Обучение пользователям основам защиты от атак типа "фишинг".
12. Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ.
13. Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.
14. Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.
15. Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.
16. Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.

17. Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей.

18. Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности.

19. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети: настройка политик безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах.

20. Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.

8 ДОПОЛНИТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль - это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную.

Процесс контроля работы сети обычно делят на два этапа - мониторинг и анализ.

На этапе *мониторинга* выполняется более простая процедура - процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется этап *анализа,* под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Классификация средств мониторинга и анализа.

Все многообразие средств, применяемых для анализа и диагностики вычислительных сетей, можно разделить на несколько крупных классов.

Агенты систем управления, поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме.

Встроенные системы диагностики и управления (Embedded systems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления многосегментным повторителем Ethernet, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам повторителя и некоторые другие. Как правило, встроенные модули управления «по совместительству» выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

Анализаторы протоколов (Protocol analyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа графика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях, - обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

Экспертные системы. Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании Network General. Работа экспертных систем состоит в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.

Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

Сетевые мониторы (называемые также сетевыми анализаторами) предназначены для тестирование кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях графика - средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т. п. Эти устройства являются наиболее интеллектуальными устройствами из всех четырех групп устройств данного класса, так как работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях.

Устройства для сертификации кабельных систем выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы.

Кабельные сканеры используются для диагностики медных кабельных систем.

Тестеры предназначены для проверки кабелей на отсутствие физического

Многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

Анализаторы протоколов.

Анализатор протоколов представляет собой либо специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать технологии сети (Ethernet, Token Ring, FDDI, Fast Ethernet). Анализатор подключается к сети точно так же, как и обычный узел. Отличие состоит в том, что

анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция - только адресованные ей. Для этого сетевой адаптер анализатора протоколов переводится в режим *"беспорядочного» захвата - promiscuous mode.*

Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и программного обеспечения, декодирующего протокол канального уровня, с которым работает сетевой адаптер, а также наиболее распространенные протоколы верхних уровней, например IP, TCP, ftp, telnet, HTTP, IPX, NCP, NetBEUI, DECnet и т. п. В состав некоторых анализаторов может входить также экспертная система, которая позволяет выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Анализаторы протоколов имеют некоторые общие свойства. Возможность (кроме захвата пакетов) измерения среднестатистических показателей трафика в сегменте локальной сети, в котором установлен сетевой адаптер анализатора. Обычно измеряется коэффициент использования сегмента, матрицы перекрестного трафика узлов, количество хороших и плохих кадров, прошедших через сегмент.

Возможность работы с несколькими агентами, поставляющими захваченные пакеты из разных сегментов локальной сети. Эти агенты чаще всего взаимодействуют с анализатором протоколов по собственному протоколу прикладного уровня, отличному от SNMP или CMIP.

Наличие развитого графического интерфейса, позволяющего представить результаты декодирования пакетов с разной степенью детализации.

Фильтрация захватываемых и отображаемых пакетов. Условия фильтрации задаются в зависимости от значения адресов назначения и источника, типа протокола или значения определенных полей пакета. Пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет и упрощает анализ, так как исключает захват или просмотр ненужных в данный момент пакетов.

Использование триггеров. Триггеры - это задаваемые администратором некоторые условия начала и прекращения процесса захвата данных из сети. Такими

условиями могут быть: время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Триггеры могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее расходовать ограниченный объем буфера захвата.

Многоканальность. Некоторые анализаторы протоколов позволяют проводить одновременную запись пакетов от нескольких сетевых адаптеров, что удобно для сопоставления процессов, происходящих в разных сегментах сети. Возможности анализа проблем сети на физическом уровне у анализаторов протоколов минимальные, поскольку всю информацию они получают от стандартных сетевых адаптеров. Поэтому они передают и обобщают информацию физического уровня, которую сообщает им сетевой адаптер, а она во многом зависит от типа сетевого адаптера. Некоторые сетевые адаптеры сообщают более детальные данные об ошибках кадров и интенсивности коллизий в сегменте, а некоторые вообще не передают такую информацию верхним уровням протоколов, на которых работает анализатор протоколов.

С распространением серверов Windows NT все более популярным становится анализатор Network Monitor фирмы Microsoft. Он является частью сервера управления системой SMS, а также входит в стандартную поставку Windows NT Server, начиная с версии 4.0 (версия с усеченными функциями). Network Monitor в версии SMS является многоканальным анализатором протоколов, поскольку может получать данные от

нескольких агентов Network Monitor Agent, работающих в среде Windows NT Server, однако в каждый момент времени анализатор может работать только с одним агентом, так что сопоставить данные разных каналов с его помощью не удастся. Network Monitor поддерживает фильтры захвата (достаточно простые) и дисплейные фильтры, отображающие нужные кадры после захвата (более сложные). Экспертной системой Network Monitor не располагает.

Сетевые анализаторы.

Сетевые анализаторы представляют собой эталонные измерительные приборы для диагностики и сертификации кабелей и кабельных систем. Они могут с высокой точностью измерить все электрические параметры кабельных систем, а также работают на более высоких уровнях стека протоколов. Сетевые анализаторы генерируют синусоидальные сигналы в широком диапазоне частот, что позволяет измерять на приемной паре амплитудно-частотную характеристику и перекрестные наводки, затухание и суммарное затухание. Сетевой анализатор представляет собой лабораторный прибор больших размеров, достаточно сложный в обращении.

Многие производители дополняют сетевые анализаторы функциями статистического анализа графика - коэффициента использования сегмента, уровня широковещательного графика, процента ошибочных кадров, а также функциями анализатора протоколов, которые обеспечивают захват пакетов разных протоколов в соответствии с условиями фильтров и декодирование пакетов.

Кабельные сканеры и тестеры.

Основное назначение *кабельных сканеров* - измерение электрических и механических параметров кабеля, параметра NEXT, затухания импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле. Точность измерений, произведенных этими устройствами, ниже, чем у сетевых анализаторов, но вполне достаточна для оценки соответствия кабеля стандарту.

Для определения местоположения неисправности кабельной системы (обрыва короткого замыкания, неправильно установленного разъема и т. д.) используете метод «отраженного импульса» (Time Domain Reflectometry, TDR). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс почти отсутствует.

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в кабеле (Nominal Velocity of Propagation, NVP) обычно задается в процентах от скорости света вакууме. Современные сканеры содержат в себе электронную таблицу данных с NVP для всех основных типов кабелей, что дает возможность пользователю устанавливать эти параметры самостоятельно после предварительной калибровки.

Кабельные сканеры - это портативные приборы, которые обслуживающий персонал может постоянно носить с собой.

Кабельные тестеры - наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

Многофункциональные портативные приборы мониторинга.

В последнее время начали выпускаться многофункциональные портативные приборы, которые объединяют в себе возможности кабельных сканеров, анализаторов протоколов и даже некоторые функции систем управления, сохраняя в то же время такое важное свойство, как портативность. Многофункциональные приборы мониторинга имеют специализированный физический интерфейс, позволяющим выявлять проблемы и тестировать кабели на физическом уровне, который дополняется микропроцессором с программным обеспечением для выполнения высокоуровневых функций.

Рассмотрим типичный набор функций и свойств такого прибора, который оказывается очень полезным для диагностики причин разнообразных неполадок в сети происходящих на всех уровнях стека протоколов, от физического до прикладного.

Интерфейс пользователя.

Прибор обычно предоставляет пользователю удобный и интуитивно понятный интерфейс, основанный на системе меню. Графический интерфейс пользователя реализован на многострочном жидкокристаллическом дисплее и индикаторах состояния на светодиодах, извещающих пользователя о наиболее общих проблемах наблюдаемых сетей. Имеется обширный файл подсказок оператору с уровневым доступом в соответствии с контекстом. Информация о состоянии сети представляется таким образом, что пользователи любой квалификации могут ее быстро понять.

Функции проверки аппаратуры и кабелей.

Многофункциональные приборы сочетают наиболее часто используемые на практике функции кабельных сканеров с рядом новых возможностей тестирования.

Сканирование кабеля.

Функция позволяет измерять длину кабеля, расстояние до самого серьезного дефекта и распределение импеданса по длине кабеля. При проверке неэкранированной витой пары могут быть выявлены следующие ошибки: расщепленная пара, обрывы, короткое замыкание и другие виды нарушения соединения.

Для сетей Ethernet на коаксиальном кабеле эти проверки могут быть осуществлены на работающей сети.

Функция определения распределения кабельных жил.

Осуществляет проверку правильности подсоединения жил, наличие промежуточных разрывов и перемычек на витых парах. На дисплей выводится перечень связанных между собой контактных групп.

Функция определения карты кабелей.

Используется для составления карты основных кабелей и кабелей, ответвляющихся от центрального помещения.

Автоматическая проверка кабеля.

В зависимости от конфигурации возможно определить длину, импеданс, схему подключения жил, затухание и параметр NEXT на частоте до 100 МГц. Автоматическая проверка выполняется для:

- коаксиальных кабелей;

- экранированной витой пары с импедансом 150 Ом;
- неэкранированной витой пары с сопротивлением 100 Ом.

Целостность цепи при проверке постоянным током.

Эта функция используется при проверке коаксиальных кабелей для верификации правильности используемых терминаторов и их установки.

Определение номинальной скорости распространения.

Функция вычисляет номинальную скорость распространения (Nominal Velocity of Propagation, NVP) по кабелю известной длины и дополнительно сохраняет полученные результаты в файле для определяемого пользователем типа кабеля (User Defined cable type) или стандартного кабеля.

Комплексная автоматическая проверка пары «сетевой адаптер-концентратор»

Этот комплексный тест позволяет последовательно подключить прибор между конечным узлом сети и концентратором. Тест дает возможность автоматически определить местонахождение источника неисправности - кабель, концентратор, сетевой адаптер или программное обеспечение станции.

Автоматическая проверка сетевых адаптеров.

Проверяет правильность функционирования вновь установленных или «подозрительных» сетевых адаптеров. Для сетей Ethernet по итогам проверки сообщаются: MAC-адрес, уровень напряжения сигналов (а также присутствие и полярность импульсов Link Test для 10BASE-T). Если сигнал не обнаружен на сетевом адаптере, то тест автоматически сканирует соединительный разъем и кабель для их диагностики.

Функции сбора статистики.

Эти функции позволяют в реальном масштабе времени проследить за изменением наиболее важных параметров, характеризующих «здоровье» сегментов сети. Статистика обычно собирается с разной степенью детализации по разным группам.

Сетевая статистика.

В этой группе собраны наиболее важные статистические показатели - коэффициент использования сегмента (utilization), уровень коллизий, уровень ошибок и уровень широковещательного графика. Превышение этими показателями определенных порогов в первую очередь говорят о проблемах в том сегменте сети, к которому подключен многофункциональный прибор.

Статистика ошибочных кадров.

Эта функция позволяет отслеживать все типы ошибочных кадров для определенной технологии. Например, для технологии Ethernet характерны следующие типы ошибочных кадров.

Укороченные кадры (Short frames). Это кадры, имеющие длину, меньше допустимой, то есть меньше 64 байт. Иногда этот тип кадров дифференцируют на два класса - просто короткие кадры (short), у которых имеется корректная контрольная сумма, и «коротышки» (runts), не имеющие корректной контрольной суммы. Наиболее вероятными причинами появления укороченных кадров являются неисправные сетевые адаптеры и их драйверы.

Удлиненные кадры (Jabbers). Это кадры, имеющие длину, превышающую допустимое значение в 1518 байт с хорошей или плохой контрольной суммой. Удлиненные кадры являются следствием затянувшейся передачи, которая появляется из-за неисправностей сетевых адаптеров.

Кадры нормальных размеров, но с плохой контрольной суммой (Bad FCS) и кадры с ошибками выравнивания по границе байта. Кадры с неверной контрольной суммой являются следствием множества причин - плохих адаптеров, помех на кабелях, плохих контактов, некорректно работающих портов повторителей, мостов, коммутаторов и маршрутизаторов. Ошибка выравнивания всегда сопровождается ошибкой по контрольной сумме, поэтому некоторые средства анализа графика не делают между ними различий. Ошибка выравнивания может быть следствием прекращения передачи кадра при распознавании коллизии передающим адаптером.

Кадры-призраки (ghosts) являются результатом электромагнитных наводок на кабеле. Они воспринимаются сетевыми адаптерами как кадры, не имеющие нормального признака начала кадра - 10101011. Кадры-призраки имеют длину более 72 байт, в противном случае они классифицируются как удаленные коллизии. Количество обнаруженных кадров-призраков в большой степени зависит от точки подключения сетевого анализатора. Причинами их возникновения являются петли заземления и другие проблемы с кабельной системой. Знание процентного распределения общего количества ошибочных кадров по их типам может многое подсказать администратору о возможных причинах неполадок в сети. Даже небольшой процент ошибочных кадров может привести к значительному снижению полезной пропускной способности сети, если протоколы, восстанавливающие искаженные кадры, работают с большими тайм-аутами ожидания квитанций. Считается, что в нормально работающей сети процент ошибочных кадров не должен превышать 0,01 %, то есть не более 1 ошибочного кадра из 10 000.

Статистика по коллизиям.

Эта группа характеристик дает информацию о количестве и видах коллизий, отмеченных на сегменте сети, позволяет определить наличие и местонахождение проблемы. Анализаторы протоколов обычно не могут дать дифференцированной картины распределения общего числа коллизий по их отдельным типам, в то же время знание преобладающего типа коллизий может помочь понять причину плохой работы сети.

Ниже приведены основные типы коллизий сети Ethernet.

Локальная коллизия (Local Collision). Является результатом одновременной передачи двух или более узлов, принадлежащих к тому сегменту, в котором производятся измерения. Если многофункциональный прибор не генерирует кадры, то в сети на витой паре или волоконно-оптическом кабеле локальные коллизии не фиксируются. Слишком высокий уровень локальных коллизий является следствием проблем с кабельной системой.

Удаленная коллизия (Remote Collision). Эти коллизии происходят на другой стороне повторителя (по отношению к тому сегменту, в котором установлен измерительный прибор). В сетях, построенных на многопортовых повторителях (lOBase-T, lOBase-FL/FB, 100Base-TX/FX/T4, Gigabit Ethernet), все измеряемые коллизии являются удаленными (кроме тех случаев, когда анализатор сам генерирует кадры и может быть виновником коллизии). Не все анализаторы протоколов и средства мониторинга одинаковым образом фиксируют удаленные коллизии. Это происходит

из-за того, что некоторые измерительные средства и системы не фиксируют коллизии, происходящие при передаче преамбулы.

Поздняя коллизия (Late Collision). Это коллизия, которая происходит после передачи первых 64 байт кадра (по протоколу Ethernet коллизия должна обнаруживаться при передаче первых 64 байт кадра). Результатом поздней коллизии будет кадр, который имеет длину более 64 байт и содержит неверное значение контрольной суммы. Чаще всего это указывает на то, что сетевой адаптер, являющийся источником конфликта, оказывается не в состоянии правильно прослушивать линию и поэтому не может вовремя остановить передачу. Другой причиной поздней коллизии является слишком большая длина кабельной системы или слишком большое количество промежуточных повторителей, приводящее к превышению максимального значения времени двойного оборота сигнала.

Средняя интенсивность коллизий в нормально работающей сети должна быть меньше 5 %. Большие всплески (более 20 %) могут быть индикатором кабельных проблем.

Распределение используемых сетевых протоколов.

Эта статистическая группа относится к протоколам сетевого уровня. На дисплее отображается список основных протоколов в убывающем порядке относительно процентного соотношения кадров, содержащих пакеты данного протокола к общему числу кадров в сети.

Основные отправители (Top Sendes)

Функция позволяет отслеживать наиболее активные передающие узлы локальной сети. Прибор можно настроить на фильтрацию по единственному адресу и выявить список основных отправителей кадров для данной станции. Данные отражаются на дисплее в виде диаграммы вместе с перечнем основных отправителей кадров.

Основные получатели (Top Receivers).

Функция позволяет следить за наиболее активными узлами-получателями сети. Информация отображается в виде, аналогичном приведенному выше.

Основные генераторы широковещательного трафика (Top broadcasted)

Функция выявляет станции сети, которые больше остальных генерируют кадры с широковещательными и групповыми адресами.

Генерирование трафика (Traffic Generation).

Прибор может генерировать график для проверки работы сети при повышенной нагрузке. Трафик может генерироваться параллельно с активизированными функциями *Сетевая статистика. Статистика ошибочных кадров* и *Статистика по коллизиям.*

Пользователь может задать параметры генерируемого трафика, такие как интенсивность и размер кадров. Для тестирования мостов и маршрутизаторов прибор может автоматически создавать заголовки IP- и IPX-пакетов, и все что требуется от оператора - это внести адреса источника и назначения.

В ходе испытаний пользователь может увеличить на ходу размер и частоту следования кадров с помощью клавиш управления курсором. Это особенно ценно при поиске источника проблем производительности сети и условий возникновения отказов.

Функции анализа протоколов.

Обычно портативные многофункциональные приборы поддерживают декодирование и анализ только основных протоколов локальных сетей, таких как протоколы стеков TCP/IP, Novell NetWare, NetBIOS и Banyan VINES.

В некоторых многофункциональных приборах отсутствует возможность декодирования захваченных пакетов, как в анализаторах протоколов, а в место этого собирается статистика о наиболее важных пакетах, свидетельствующих о наличии проблем в сетях. Например, при анализе протоколов стека TCP/IP собирается статистика по пакетам протокола ICMP, с помощью которого маршрутизаторы сообщают конечным узлам о возникновении разного рода ошибок. Для ручной проверки достижимости узлов сети в приборы включается поддержка утилиты IP Ping, а также аналогичных по назначению утилит NetWare Ping и NetBIOS Ping.

Мониторинг локальных сетей на основе коммутаторов.

Наблюдение за графиком.

Так как перегрузки процессоров портов и других обрабатывающих элементов коммутатора могут приводить к потерям кадров, то функция наблюдения за распределением графика в сети, построенной на основе коммутаторов, очень важна.

Однако если сам коммутатор не снабжен встроенным агентом SNMP для каждого своего порта, то задача слежения за графиком, традиционно решаемая в сетях с разделяемыми средами с помощью установки в сеть внешнего анализатора протоколов, очень усложняется.

Обычно в традиционных сетях анализатор протоколов или многофункциональный прибор подключался к свободному порту концентратора, что позволяло ему наблюдать за всем графиком, передаваемым между любыми узлами сети.

Если же анализатор протокола подключить к свободному порту коммутатора, то он не зафиксирует почти ничего, так как кадры ему передавать никто не будет, а чужие кадры в его порт также направляться не будут. Единственный вид трафика, который будет фиксировать анализатор, - это график широковещательных пакетов, которые будут передаваться всем узлам сети, а также трафик кадров с неизвестными коммутатору адресами назначения. В случае когда сеть разделена на виртуальные сети, анализатор протоколов будет фиксировать только широковещательный трафик своей виртуальной сети.

Чтобы анализаторами протоколов можно было по-прежнему пользоваться и в коммутируемых сетях, производители коммутаторов снабжают свои устройства функцией зеркального отображения графика любого порта на специальный порт. К специальному порту подключается анализатор протоколов, а затем на коммутатор подается команда через его модуль SNMP-управления для отображения трафика какого-либо порта на специальный порт.

Наличие функции зеркализации портов частично снимает проблему, но оставляет некоторые вопросы. Например, как просматривать одновременно трафик двух портов или трафик порта, работающего в полнодуплексном режиме.

Более надежным способом слежения за графиком, проходящим через порты коммутатора, является замена анализатора протокола на агенты RMON MIB для каждого порта коммутатора.

Агент RMON выполняет все функции хорошего анализатора протокола для протоколов Ethernet и Token Ring, собирая детальную информацию об интенсивности графика, различных типах плохих кадров, о потерянных кадрах, причем самостоятельно

строя временные ряды для каждого фиксируемого параметра. Кроме того, агент RMON может самостоятельно строить матрицы перекрестного графика между узлами сети, которые очень нужны для анализа эффективности применения коммутатора.

Так как агент RMON, реализующий все 9 групп объектов Ethernet, стоит весьма дорого, то производители для снижения стоимости коммутатора часто реализуют только первые несколько групп объектов RMON MIB. Другим приемом снижения стоимости коммутатора является использование одного агента RMON для нескольких портов. Такой агент по очереди подключается к нужному порту, позволяя снять с него требуемые статистические данные.

Управление виртуальными сетями.

Виртуальные локальные сети VLAN порождают проблемы для традиционных систем управления на платформе SNMP как при их создании, так и при наблюдении за их работой.

Как правило, для создания виртуальных сетей требуется специальное программное обеспечение компании-производителя, которое работает на платформе системы управления, например HP Open View. Сами платформы систем управления этот процесс поддержать не могут в основном из-за долгого отсутствия стандарта на виртуальные сети. Можно надеяться, что появление стандарта 802.1Q изменит ситуацию в этой области.

Наблюдение за работой виртуальных сетей также создает проблемы для традиционных систем управления. При создании карты сети, включающей виртуальные сети, необходимо отображать как физическую структуру сети, так и ее логическую структуру, соответствующую связям отдельных узлов виртуальной сети. При этом по желанию администратора система управления должна уметь отображать соответствие логических и физических связей в сети, то есть на одном физическом канале должны отображаться все или отдельные пути виртуальных сетей.

К сожалению, многие системы управления либо вообще не отображают виртуальные сети, либо делают это очень неудобным для пользователя способом, что вынуждает обращаться к менеджерам компаний-производителей для решения этой задачи.

Выводы

Мониторинг и анализ сети представляют собой важные этапы контроля работы сети. Для выполнения этих этапов разработан ряд средств, применяемых автономно в тех случаях, когда применение интегрированной системы управления экономически неоправданно.

В состав автономных средств мониторинга и анализа сети входят встроенные средства диагностики, анализаторы протоколов, экспертные системы, сетевые анализаторы, кабельные сканеры и тестеры, многофункциональные приборы.

Анализаторы протоколов чаще всего представляют собой специальное программное обеспечение для персональных компьютеров и ноутбуков, которое переводит сетевой адаптер компьютера в режим «беспорядочного» захвата всех кадров. Анализатор протоколов выполняет декодирование захваченных кадров для вложенных пакетов протоколов всех уровней, включая прикладной.

Сетевые анализаторы представляют собой прецизионные приборы для сертификации кабельных систем по международным стандартам. Кроме того, эти устройства могут выполнять некоторые функции анализаторов протоколов.

Кабельные сканеры являются портативными приборами, которые могут измерить электрические параметры кабелей, а также обнаружить место повреждения кабеля. Кабельные тестеры представляют собой наиболее простые портативные приборы, способные обнаружить неисправность кабеля.

Многофункциональные портативные приборы сочетают в себе функции кабельных сканеров и анализаторов протоколов. Они снабжены многострочными дисплеями, контекстно-чувствительной системой помощи, встроенным микропроцессором с программным обеспечением и позволяют выполнять комплексную проверку сегментов сети на всех уровнях, от физического (что не умеют делать анализаторы протоколов), до прикладного. Отличаются от анализаторов протоколов поддержкой только базового набора протоколов локальных сетей.

РЕЦЕНЗИЯ

на рабочую программу учебной дисциплины
МДК.03.03 Безопасность сетевой инфраструктуры
для специальности 09.02.06 Сетевое и системное администрирование

Рабочая программа учебной дисциплины МДК.03.03 Безопасность сетевой инфраструктуры соответствует ФГОС по специальности среднего профессионального образования 09.02.06 «Сетевое и системное администрирование», утвержденного приказом Министерства образования и науки Российской Федерации от «10» июля 2023 г. № 519, зарегистрирован в Министерстве юстиции 15.08.2023 г. (рег. № 74796), и примерной основной образовательной программе по специальности 09.02.06 Сетевое и системное администрирование.

В рабочую программу учебной дисциплины включены разделы «Паспорт рабочей программы учебной дисциплины», «Структура и содержание учебной дисциплины», «Образовательные технологии», «Условия реализации программы учебной дисциплины», «Перечень основных и дополнительных информационных источников, необходимых для освоения дисциплины», «Методические рекомендации обучающимся по освоению дисциплины», «Оценочные средства для контроля успеваемости» и «Дополнительное обеспечение дисциплины».

Структура и содержание рабочей программы соответствуют целям образовательной программы СПО по специальности 09.02.06 «Сетевое и системное администрирование» и будущей профессиональной деятельности студента.

Объем рабочей программы учебной дисциплины полностью соответствует учебному плану подготовки по данной специальности. В программе четко сформулированы цели обучения, а также прогнозируемые результаты обучения по дисциплине.

На основании проведенной экспертиза можно сделать заключение, что рабочая программа учебной дисциплины МДК.03.03 Безопасность сетевой инфраструктуры по специальности 09.02.06 «Сетевое и системное администрирование» соответствует требованиям стандарта, профессиональным требованиям, а также современным требованиям рынка труда.

Технический директор ООО «ПРАЙ»
« » 20 г.

Б.А. Шишкин

РЕЦЕНЗИЯ

на рабочую программу учебной дисциплины
МДК.03.03 Безопасность сетевой инфраструктуры
для специальности 09.02.06 Сетевое и системное администрирование

Рабочая программа учебной дисциплины МДК.03.03 Безопасность сетевой инфраструктуры соответствует ФГОС по специальности среднего профессионального образования 09.02.06 «Сетевое и системное администрирование», утвержденного приказом Министерства образования и науки Российской Федерации от «10» июля 2023 г. № 519, зарегистрирован в Министерстве юстиции 15.08.2023 г. (рег. № 74796), и примерной основной образовательной программе по специальности 09.02.06 Сетевое и системное администрирование.

В рабочую программу учебной дисциплины включены разделы «Паспорт рабочей программы учебной дисциплины», «Структура и содержание учебной дисциплины», «Образовательные технологии», «Условия реализации программы учебной дисциплины», «Перечень основных и дополнительных информационных источников, необходимых для освоения дисциплины», «Методические рекомендации обучающимся по освоению дисциплины», «Оценочные средства для контроля успеваемости» и «Дополнительное обеспечение дисциплины».

Структура и содержание рабочей программы соответствуют целям образовательной программы СПО по специальности 09.02.06 «Сетевое и системное администрирование» и будущей профессиональной деятельности студента.

Объем рабочей программы учебной дисциплины полностью соответствует учебному плану подготовки по данной специальности. В программе четко сформулированы цели обучения, а также прогнозируемые результаты обучения по дисциплине.

На основании проведенной экспертиза можно сделать заключение, что рабочая программа учебной дисциплины МДК.03.03 Безопасность сетевой инфраструктуры по специальности 09.02.06 «Сетевое и системное администрирование» соответствует требованиям стандарта, профессиональным требованиям, а также современным требованиям рынка труда.

Технический директор
ООО «ТехноСтарт» И.Г. Колодезный

« » 20 г.