

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**  
**ТЕЛЕКОММУНИКАЦИЙ**  
**ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»**  
**(СПбГУТ)**

**Санкт-Петербургский колледж телекоммуникаций**

---

УТВЕРЖДАЮ

Первый проректор – проректор  
по учебной работе

\_\_\_\_\_ Г.М. Машков

«\_\_\_» \_\_\_\_\_ 2020 г.

Регистрационный № 11.04.20/127

**РАБОЧАЯ ПРОГРАММА**

**ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ**

---

(наименование профессионального модуля)

программа подготовки специалистов среднего звена

09.02.02 Компьютерные сети  
(код и наименование специальности)

квалификация  
техник по компьютерным сетям

Санкт-Петербург

2020

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.03) среднего профессионального образования по специальности 09.02.02 Компьютерные сети, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 25 июня 2020 г., протокол № 6.

Составитель:

Преподаватель \_\_\_\_\_ Н.В. Кривоносова  
(подпись)

СОГЛАСОВАНО

Главный специалист НТБ УИОР \_\_\_\_\_ Р.Х. Ахтреева  
(подпись)

ОБСУЖДЕНО

на заседании предметной (цикловой) комиссии № 4 (компьютерных сетей и программно-аппаратных средств)  
«08» апреля 2020 г., протокол № 8

Председатель предметной (цикловой) комиссии:

\_\_\_\_\_ К.В. Лебедева  
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций  
«17» апреля 2020 г., протокол № 4

Зам. директора по УР колледжа СПб ГУТ

\_\_\_\_\_ О.В. Колбанёва  
(подпись)

СОГЛАСОВАНО

Директор колледжа СПб ГУТ

\_\_\_\_\_ Т.Н. Сиротская  
(подпись)

СОГЛАСОВАНО

Директор департамента ОКОД

\_\_\_\_\_ С.И. Ивасишин  
(подпись)

СОГЛАСОВАНО

СОГЛАСОВАНО

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

## **СОДЕРЖАНИЕ**

<b>1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>стр. 4</b>
<b>2. РЕЗУЛЬТАТ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>6</b>
<b>3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>6</b>
<b>4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>42</b>
<b>5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>48</b>
<b>ПРИЛОЖЕНИЕ 1. ИНФОРМАЦИОННЫЕ РЕСУРСЫ, ИСПОЛЬЗУЕМЫЕ ПРИ ВЫПОЛНЕНИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ</b>	<b>52</b>

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 1.1. Область применения программы

Рабочая программа профессионального модуля (далее программа) – является частью основной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.02 **Компьютерные сети** в части освоения основного вида деятельности: **Эксплуатация объектов сетевой инфраструктуры** и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.

ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.

ПК 3.3. Эксплуатация сетевых конфигураций.

ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.

ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.

ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Программа профессионального модуля может быть использована в дополнительном профессиональном образовании (курсы повышения квалификации и переподготовки), а также для всех форм получения образования: очной, очно - заочной (вечерней) и экстерната, для всех типов и видов образовательных учреждений, реализующих ППССЗ СПО по специальности 09.02.02 Компьютерные сети с квалификацией «Техник по компьютерным сетям».

## 1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

### **иметь практический опыт:**

- обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;
- удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;
- организации бесперебойной работы системы по резервному копированию и восстановлению информации;
- поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры;

### **уметь:**

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры;
- осуществлять диагностику и поиск неисправностей технических средств;
- выполнять действия по устранению неисправностей в части, касающейся полномочий техника;
- тестировать кабели и коммуникационные устройства;
- выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;
- правильно оформлять техническую документацию;
- наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;

- устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;

**знать:**

- архитектуру и функции систем управления сетями, стандарты систем управления;
- задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;
- средства мониторинга и анализа локальных сетей;
- классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;
- правила эксплуатации технических средств сетевой инфраструктуры;
- расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;
- методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;
- основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем (ИС), требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;
- основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

**1.3. Количество часов на освоение программы профессионального модуля:**

всего – **750** часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося – **332** часов,

учебной и производственной практики – **108+144 часа**

самостоятельной работы обучающегося – **166** часов

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом деятельности **Эксплуатация объектов сетевой инфраструктуры**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ПК 3.1.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей
ПК 3.2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях
ПК 3.3.	Эксплуатировать сетевые конфигурации
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации
ПК 3.5.	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования
ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Тематический план профессионального модуля Эксплуатация объектов сетевой инфраструктуры

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6	Раздел 1. Эксплуатация объектов сетевой инфраструктуры	282	212	70		70	-	72	-
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6	Раздел 2. Безопасность функционирования информационных систем	180	132	48	-	48	-	36	-
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6	Раздел 3. Эксплуатация систем IP-телефонии	180	96	48		48	-		-
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6	Производственная практика (по профилю специальности), часов	144							144
	<b>Всего:</b>	<b>750</b>	<b>498</b>	<b>166</b>	<b>-</b>	<b>166</b>		<b>108</b>	<b>144</b>

### 3.2. Тематический план и содержание профессионального модуля Эксплуатация объектов сетевой инфраструктуры

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения	
1	2	3	4	
Раздел 1. Эксплуатация объектов сетевой инфраструктуры		246		
МДК 03.01. Эксплуатация объектов сетевой инфраструктуры		210		
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры. Профилактические работы	<b>Содержание учебного материала</b>		20	
	1	<b>Занятие № 1. Физические аспекты эксплуатации</b> 1. Физическое вмешательство в инфраструктуру сети; 2. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки		2
	2	<b>Занятие № 2. Логические (информационные) аспекты эксплуатации</b> 1. Несанкционированное ПО (в том числе сетевое) 2. Паразитная нагрузка		2
	3	<b>Занятие № 3. Расширяемость сети. Масштабируемость сети</b> 1. Добавление отдельных элементов сети (пользователи, компьютеры, приложения, службы) 2. Нарастивание длины сегментов сети 3. Замена существующей аппаратуры на более мощную. 4. Увеличение количества узлов сети 5. Увеличение протяженности связей между объектами сети		2



4	<b>Занятие № 4. Техническая и проектная документация</b> 1. Паспорт технических устройств 2. Руководство по эксплуатации. 3. Физическая карта всей сети 4. Логическая схема компьютерной сети		2
5	<b>Занятие № 5. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры</b> 1. Комплекс организационно-технических мероприятий 2. Выявление и своевременная замена элементов инфраструктуры		2
6	<b>Занятие № 6. Проверка объектов сетевой инфраструктуры и профилактические работы</b> 1. Проверка физических компонентов 2. Проверка документации и требований 3. Проверка списка совместимого оборудования		2
7	<b>Занятие № 7. Проведение регулярного резервирования</b> 1. Обслуживание физических компонентов 2. Контроль состояния аппаратного обеспечения, 3. Организация удалённого оповещения		2
8	<b>Занятие № 8. Принципы локализации неисправностей</b> 1. Контрольно-измерительная аппаратура 2. Сервисные платы и комплексы 3. Программные средства диагностики		2
9	<b>Занятие № 9. Профилактические работы</b> 1. Номенклатура и особенности работы тест-программ 2. Диагностика неисправностей средств сетевых коммуникаций 3. Контроль функционирования аппаратно-программных комплексов		2
10	<b>Занятие № 10. Работа с нестабильной сетью</b> 1. Действия при неработающей сети, при медленной сети 2. Действия при нестабильно работающей сети		2
<b>Лабораторные работы</b>		30	
1.1	<b>Занятие № 11. Поддержка пользователей в сети</b>		
1.2	<b>Занятие № 12. Создание пользователей в домене (создание пароля, создание групп и распределение пользователей по группам)</b>		
1.3	<b>Занятие № 13. Настройка прав доступа</b>		

1.4	<b>Занятие № 14.</b> Оформление технической документации, правила оформления документов		
1.5	<b>Занятие № 15.</b> Настройка аппаратного и программного обеспечения сети.		
1.6	<b>Занятие № 16.</b> Настройка сетевой карты (имя компьютера, рабочая группа, введение компьютера в домен)		
1.7	<b>Занятие № 17.</b> Выполнение мониторинга и анализа работы локальной сети с помощью программных средств		
1.8	<b>Занятие № 18.</b> Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы, коммутационное оборудование)		
1.9	<b>Занятие № 19.</b> Работа контрольно-измерительной аппаратуры.		
1.10	<b>Занятие № 20.</b> Замена расходных материалов.		
1.11	<b>Занятие № 21.</b> Мелкий ремонт периферийного оборудования		
1.12	<b>Занятие № 22.</b> Программная диагностика неисправностей.		
1.13	<b>Занятие № 23.</b> Аппаратная диагностика неисправностей		
1.14	<b>Занятие № 24.</b> Поиск неисправностей технических средств.		
1.15	<b>Занятие № 25.</b> Выполнение действий по устранению неисправностей.		

	<p><b>Самостоятельная работа обучающихся</b> преподавателя Подготовка к лабораторно-практическим работам с использованием методических рекомендаций; оформление лабораторно-практических работ, отчетов и подготовка к их защите.</p> <p><b>Примерная тематика внеаудиторной работы</b></p> <ol style="list-style-type: none"> <li>1. Физическая, логическая инфраструктуры.</li> <li>2. Сетевые подключения, протоколы, адресация, система имён.</li> <li>3. Автоматическое назначение частных IP-адресов.</li> <li>4. Маршрутизация и инфраструктура сети Windows Server</li> <li>5. Установка сетевых компонентов Windows, установка Active Directory в сети Windows.</li> <li>6. Разбиение на подсети, механизм разбиения на подсети, определение емкости подсети.</li> <li>7. Технические регламенты, виды документов для технических осмотров, методы и принципы проверки различного оборудования, методы резервирования, программы для резервирования информации, BackUp.</li> <li>8. Маршрутизация в Windows Server.</li> <li>9. Управление общими свойствами IP-маршрутизации.</li> <li>10. Основные сведения о NAT, различие между NAT и ICS.</li> <li>11. Удалённый доступ по телефонной линии, авторизация подключений удалённого доступа</li> <li>12. Поиск неисправностей по принципу локализации неисправностей конкретного оборудования.</li> <li>13. Изучить и понять принцип работы новых контрольно-измерительных аппаратов</li> </ol>	25					
<p><b>Тема 1.2. Управление сетями</b></p>	<p><b>Содержание учебного материала</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td data-bbox="510 1102 607 1278" style="width: 5%; text-align: center;">1</td> <td data-bbox="607 1102 1664 1278"> <p><b>Занятие № 26. Архитектура системы управления</b></p> <ol style="list-style-type: none"> <li>1. Структура системы управления</li> <li>2. Архитектура в концепции TMN</li> <li>3. Централизованное управление</li> <li>4. Децентрализованное управление</li> </ol> </td> </tr> <tr> <td data-bbox="510 1278 607 1425" style="text-align: center;">2</td> <td data-bbox="607 1278 1664 1425"> <p><b>Занятие № 27. Уровни управления</b></p> <ol style="list-style-type: none"> <li>1. Концепции управления</li> <li>2. Задачи управления</li> <li>3. Стандарты управления</li> </ol> </td> </tr> </table>	1	<p><b>Занятие № 26. Архитектура системы управления</b></p> <ol style="list-style-type: none"> <li>1. Структура системы управления</li> <li>2. Архитектура в концепции TMN</li> <li>3. Централизованное управление</li> <li>4. Децентрализованное управление</li> </ol>	2	<p><b>Занятие № 27. Уровни управления</b></p> <ol style="list-style-type: none"> <li>1. Концепции управления</li> <li>2. Задачи управления</li> <li>3. Стандарты управления</li> </ol>	50	2
1	<p><b>Занятие № 26. Архитектура системы управления</b></p> <ol style="list-style-type: none"> <li>1. Структура системы управления</li> <li>2. Архитектура в концепции TMN</li> <li>3. Централизованное управление</li> <li>4. Децентрализованное управление</li> </ol>						
2	<p><b>Занятие № 27. Уровни управления</b></p> <ol style="list-style-type: none"> <li>1. Концепции управления</li> <li>2. Задачи управления</li> <li>3. Стандарты управления</li> </ol>						

3	<b>Занятие № 28. Многоуровневая архитектура управления TMN</b> 1. Управление бизнесом, услугами, сетью, элементами сети 2. Уровень элементов сети		2
4	<b>Занятие № 29. Области управления</b> 1. Области управления ошибками 2. Области управления конфигурацией		2
5	<b>Занятие № 30. Области управления</b> 1. Области управления доступом 2. Области управления производительностью 3. Области управления безопасностью		2
6	<b>Занятие № 31. Протоколы управления</b> 1. SNMP 2. CMIP		2
7	<b>Занятие № 32. Протоколы управления</b> 1. TMN 2. LNMP 3. ANMP		2
8	<b>Занятие № 33. Управление отказами</b> 1. Понятие отказа сети 2. Правила управления отказами		2
9	<b>Занятие № 34. Выявление, определение и устранение последствий сбоев и отказов в работе сети</b> 1. Определение сбоя в сети 2. Определение отказа сети 3. Устранение последствий сбоя или отказа в сети		2
10	<b>Занятие № 35. Работа с конфигурацией сети</b> 1. Учёт работы сети 2. Управление конфигурацией		2
11	<b>Занятие № 36. Регистрация, управление используемыми ресурсами и устройствами</b> 1. Конфигурирование компонентов сети 2. Сетевые адреса и идентификаторы 3. Управление параметрами сетевых операционных систем		2

12	<b>Занятие № 37. Управление сетью</b> 1. Управление производительностью сети 2. Управление безопасностью сети		2
13	<b>Занятие № 38. Статистика работы сети в реальном времени</b> 1. Минимизация заторов и узких мест 2. Выявление складывающихся тенденций и планирование ресурсов для будущих нужд. 3. Контроль доступа, сохранение целостности данных и журналирование		2
14	<b>Занятие № 39. Анализаторы протоколов</b> 1. Программные или аппаратно-программные системы 2. Функции мониторинга 3. Анализ трафика в сетях		2
15	<b>Занятие № 40. Оборудование для диагностики и сертификации кабельных систем</b> 1. Сетевые мониторы 2. Приборы для сертификации кабельных систем 3. Кабельные сканеры и тестеры		2
16	<b>Занятие № 41. Экспертные системы</b> 1. Выявление причин аномальной работы сетей 2. Возможные способы приведения сети в работоспособное состояние		2
17	<b>Занятие № 42. Встроенные системы диагностики и управления</b> 1. Сетевые мониторы 2. Средняя интенсивность общего трафика сети, средняя интенсивность потока пакетов с определённым типом ошибки. 3. Программно-аппаратный модуль, установленный в коммуникационное оборудование 4. Программный модуль, встроенный в операционные системы		2
18	<b>Занятие № 43. Резервное копирование данных</b> 1. Наименование операций 2. Требования к системе резервного копирования 3. Схемы ротации 4. Хранение резервной копии 5. Причины утери информации 6. Затруднения при резервном копировании		2

19	<b>Занятие № 44. Хранилищ данных</b> 1. Принципы работы хранилищ данных. 2. Принципы построения. 3. Основные компоненты хранилища данных		2
20	<b>Занятие № 45. Технологии управления информацией.</b> 1. OLAP-технология 2. Требования к управлению информацией 3. Возможности систем обработки данных		2
21	<b>Занятие № 46. Понятие баз данных</b> 1. Основные понятия, принцип работы. 2. СУБД 3. Администрирование БД		2
22	<b>Занятие № 47. Принципы планирования восстановления работоспособности сети при аварийной ситуации</b> 1. Список критичный пользовательских ИТ-сервисов 2. Определение точек отказа 3. Зависимости точек отказа		2
23	<b>Занятие № 48. Допущения при разработке схемы послеаварийного восстановления.</b> 1. Основные требования к политике организации схемы послеаварийного восстановления 2. Правила послеаварийного восстановления		2
24	<b>Занятие № 49. Организация работ по восстановлению функционирования системы</b> 1. Понятие быстрого восстановления 2. Этапы работ по восстановлению 3. Принципы планирования восстановления 4. Организация работ по восстановлению функционирования системы		2
25	<b>Занятие № 50. План восстановления системы</b> 1. Порядок уведомления о чрезвычайных событиях. 2. Активация. 3. Возврат к нормальному функционированию системы		2
<b>Лабораторные работы</b>		40	
1.16	<b>Занятие № 51. Анализ сетевого трафика средствами сетевого монитора</b>		
1.17	<b>Занятие № 52. Основные сведения о сетевом мониторе</b>		

1.18	<b>Занятие № 53.</b> Запись данных средствами сетевого монитора.		
1.19	<b>Занятие № 54.</b> Устранение неполадок с помощью Ping и PathPing.		
1.20	<b>Занятие № 55.</b> Диагностика сети и Netdiag		
1.21	<b>Занятие № 56.</b> Удалённое администрирование		
1.22	<b>Занятие № 57.</b> Восстановление работоспособности сетевой инфраструктуры.		
1.23	<b>Занятие № 58.</b> Авторизация подключений удалённого доступа		
1.24	<b>Занятие № 59.</b> Использование консоли. Производительность.		
1.25	<b>Занятие № 60.</b> Мониторинг сетевого трафика с помощью утилиты Netstat		
1.26	<b>Занятие № 61.</b> Тестирование кабелей.		
1.27	<b>Занятие № 62.</b> Тестирование коммутационного оборудования		
1.28	<b>Занятие № 63.</b> Операции по резервному копированию данных.		
1.29	<b>Занятие № 64.</b> Операции по восстановлению данных		
1.30	<b>Занятие № 65.</b> Организация бесперебойной работы системы резервного копирования.		
1.31	<b>Занятие № 66.</b> Восстановление информации		
1.32	<b>Занятие № 67.</b> Восстановление работоспособности сети после сбоя.		
1.33	<b>Занятие № 68.</b> Разработка плана восстановления		
1.34	<b>Занятие № 69.</b> Использование схемы послеаварийного восстановления сети.		
1.35	<b>Занятие № 70.</b> Возврат к нормальному функционированию системы		

	<p><b>Самостоятельная работа обучающихся</b>  Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите</p> <p><b>Примерная тематика внеаудиторной работы</b></p> <ol style="list-style-type: none"> <li>1. Основные сведения о политиках удалённого доступа.</li> <li>2. Устранение неполадок при подключениях удалённого доступа.</li> <li>3. Реализация процедур безопасного администрирования сети.</li> <li>4. Оснастка</li> <li>5. Шаблоны безопасности.</li> <li>6. Схемы обжимки витой пары.</li> <li>7. Устройство пакета, передаваемого по сети.</li> <li>8. Использование бесклассовой междоменной маршрутизации.</li> <li>9. Маски подсети переменной длины.</li> <li>10. Проверка существующего IP-адреса, ручная настройка адреса.</li> <li>11. DNS, NetBIOS. DNS в сетях Windows Server</li> <li>12. Механизм работы DNS-запросов.</li> <li>13. Настройка параметров DNS-сервера. Средства устранения неполадок DNS</li> <li>14. Изучение утилиты Acronis, изучение безопасной зоны Acronis.</li> <li>15. Создание контрольной точки восстановления с помощью Acronis.</li> <li>16. Создание базы данных на примере учебной группы.</li> <li>17. Разработка плана восстановления работоспособности сети на примере одной взятой организации (колледжа, офиса)</li> </ol>																								
<p><b>Учебная практика</b>  <b>УП.ПМ.03.01</b></p>	<p><b>Содержание учебного материала</b></p> <table border="1" data-bbox="510 1018 1664 1442"> <tr> <td><b>1</b></td> <td>Использование активного оборудования сети</td> </tr> <tr> <td><b>2</b></td> <td>Использование пассивного оборудования сети</td> </tr> <tr> <td><b>3</b></td> <td>Устранение паразитирующей нагрузки в сети</td> </tr> <tr> <td><b>4</b></td> <td>Заполнение технической документации</td> </tr> <tr> <td><b>5</b></td> <td>Построение физической карты локальной сети</td> </tr> <tr> <td><b>6</b></td> <td>Работа по созданию пользователей в домене</td> </tr> <tr> <td><b>7</b></td> <td>Работа по редактированию пользователей в домене</td> </tr> <tr> <td><b>8</b></td> <td>Работа по удалению пользователей в домене</td> </tr> <tr> <td><b>9</b></td> <td>Работа в домене с группами: создание групп</td> </tr> <tr> <td><b>10</b></td> <td>Работа в домене с группами: объединение в группы, удаление групп</td> </tr> <tr> <td><b>11</b></td> <td>Регламенты технических осмотров</td> </tr> </table>	<b>1</b>	Использование активного оборудования сети	<b>2</b>	Использование пассивного оборудования сети	<b>3</b>	Устранение паразитирующей нагрузки в сети	<b>4</b>	Заполнение технической документации	<b>5</b>	Построение физической карты локальной сети	<b>6</b>	Работа по созданию пользователей в домене	<b>7</b>	Работа по редактированию пользователей в домене	<b>8</b>	Работа по удалению пользователей в домене	<b>9</b>	Работа в домене с группами: создание групп	<b>10</b>	Работа в домене с группами: объединение в группы, удаление групп	<b>11</b>	Регламенты технических осмотров	<p><b>72</b></p>	
<b>1</b>	Использование активного оборудования сети																								
<b>2</b>	Использование пассивного оборудования сети																								
<b>3</b>	Устранение паразитирующей нагрузки в сети																								
<b>4</b>	Заполнение технической документации																								
<b>5</b>	Построение физической карты локальной сети																								
<b>6</b>	Работа по созданию пользователей в домене																								
<b>7</b>	Работа по редактированию пользователей в домене																								
<b>8</b>	Работа по удалению пользователей в домене																								
<b>9</b>	Работа в домене с группами: создание групп																								
<b>10</b>	Работа в домене с группами: объединение в группы, удаление групп																								
<b>11</b>	Регламенты технических осмотров																								



	12	Профилактические работы в объектах сетевой инфраструктуры		
	13	Мониторинг и анализ сети с помощью программных и аппаратных средств		
	14	Структура системы управления, архитектура системы управления		
	15	Управление областями сети: ошибками		
	16	Управление областями сети: конфигурацией		
	17	Управление областями сети: доступом		
	18	Управление областями сети: производительностью		
	19	Управление областями сети: безопасностью		
	20	Работа с протоколами SNMP, CMIP		
	21	Работа с протоколами TMN, LNMP		
	22	Работа с протоколом ANMP		
	23	Отслеживание работы сети		
	24	Работа с сервером, чтение логов, работа над ошибками		
	25	Работа с сервером; контроль доступа		
	26	Работа с сервером: сохранение целостности данных		
	27	Работа с сервером: журналирование		
	28	Удалённое администрирование рабочих станций с сервера		
	29	Удалённое администрирование сервера с рабочих станций, программы для удалённого доступа		
	30	Анализ трафика сети		
	31	Работа с кабельными сканерами и тестерами		
	32	Работа со встроенными сканерами диагностики и управления		
	33	Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных таблиц		
	34	Восстановление сети после сбоя		
	35	Создание плана восстановления сети		
	36	Использование в работе контрольно-измерительной аппаратуры, сервисных плат, комплексов		
<b>Раздел 2. Безопасность функционирования информационных систем</b>			<b>180</b>	

<b>МДК 03.02</b> <b>Безопасность</b> <b>функционирования</b> <b>информационных</b> <b>систем</b>			<b>144=</b> <b>(48ч+48чПЗ+</b> <b>48чСР</b>	
<b>Тема 2.1.Основы</b> <b>информационной</b> <b>безопасности</b> <b>(8ч+4ч.ПЗ)</b>	<b>Содержание учебного материала</b>		<b>8</b>	
	1	<b>Занятие № 1. Понятие информационной безопасности</b> 1. Понятие информационной безопасности, характеристика ее составляющих. 2. Место информационной безопасности в системе национальной безопасности. Концептуальная модель защиты информации. 3. Проблемы информационной безопасности в сфере телекоммуникаций: объекты защиты; виды защиты; системы защиты информации.		1
	2	<b>Занятие № 2. Классификация угроз ИБ</b> 1. Классификация и анализ угроз информационной безопасности в телекоммуникационных системах. 2. Виды уязвимости информации и формы ее проявления		1
	3	<b>Занятие № 3. Защищаемые информационные активы</b> 1. Понятие о конфиденциальной информации (грифы, закон о государственной тайне, закон о личной тайне, закон о коммерческой тайне). 2. Категорирование информации		2
	4	<b>Занятие № 4. Основные принципы построения систем защит информации</b> 1. Уровни информационной безопасности – законодательно-правовой, административно-организационный, программно-технический. 2. Принципы построения систем защиты информации.		2
	<b>Практические занятия</b>		<b>4</b>	
	2.1	<b>Занятие № 5. Анализ рисков информационной безопасности</b>		
2.2	<b>Занятие № 6. Обеспечение информационной безопасности в ведущих зарубежных странах</b>			

	<p><b>Самостоятельная работа обучающихся</b> Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите</p> <p><b>Тематика домашних заданий</b></p> <ol style="list-style-type: none"> <li>1. Составление доклада о Стандарте шифрования ГОСТ 28147-89</li> <li>2. Подготовка реферата по теме «Абсолютный шифр».</li> <li>3. Схема «Простая замена».</li> <li>4. Схема «Простая замена с ключом».</li> <li>5. Схема «Система Цезаря с ключом».</li> <li>6. Схема «Символьное кодирование».</li> <li>7. Подготовка реферата по теме «Основные процедуры цифровой подписи».</li> <li>8. Подготовка реферата по теме «Комбинированная криптосистема».</li> <li>9. Схема симметричное шифрование.</li> <li>10. Выполнение реферата по теме «Криптология».</li> <li>11. Подготовка презентаций по теме «Криптоанализ».</li> </ol>	<b>6</b>	
<b>Тема 2.2. Правовое обеспечение информационной безопасности (8ч+4ч.ПЗ)</b>	<p><b>Содержание учебного материала</b></p>	<b>8</b>	
	<p>1 <b>Занятие № 7. Нормативно-правовая рамка отрасли защиты информации</b></p> <ol style="list-style-type: none"> <li>1. Информация как объект права.</li> <li>2. Нормативно-правовые основы информационной безопасности в РФ.</li> </ol>		2
	<p>2 <b>Занятие № 8. Нормативно-правовая рамка отрасли защиты информации</b></p> <ol style="list-style-type: none"> <li>1. Конституционные гарантии прав граждан в области информационной безопасности.</li> <li>2. Понятие и виды защищаемой информации по законодательству РФ.</li> </ol>		2
	<p>3 <b>Занятие № 9. Защита государственной тайны. Категорирование информации</b></p> <ol style="list-style-type: none"> <li>1. Система защиты государственной тайны.</li> <li>2. Правовой режим защиты государственной тайны.</li> </ol>		2
	<p>4 <b>Занятие № 10. Стандартизация информационной безопасности</b></p> <ol style="list-style-type: none"> <li>1. Лицензирование и сертификация в области защиты информации.</li> <li>2. Стандартизация информационной безопасности.</li> </ol>		2
<p><b>Практические занятия</b></p>	<b>4</b>		
<p>2.3 <b>Занятие № 11. Изучение нормативно-правовой базы ИБ</b></p>			

	2.4	<b>Занятие № 12.</b> Построение концепции информационной безопасности предприятия		
	<p><b>Самостоятельная работа обучающихся</b>  Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите</p> <p><b>Тематика домашних заданий:</b></p> <ol style="list-style-type: none"> <li>1. Оформление в виде конспекта основных положений криптографии.</li> <li>2. Разработка схемы Механизма арбитраж.</li> <li>3. Изучение структуры Симметричной системы шифрования.</li> <li>4. Составление схемы сервера приложений.</li> <li>5. Оформление в виде конспекта основных положений процесса генерации ключей.</li> <li>6. Подготовка схемы Абонентское шифрование.</li> <li>7. Разработка схемы. Пакетное шифрование.</li> <li>8. Разработка схемы Аутентификация данных</li> <li>9. Оформление в виде конспекта основных положений представления алфавита в двоичном коде</li> <li>10. Подготовка схемы функционирования электронных платежных систем.</li> <li>11. Оформление в виде конспекта основ кодирования.</li> <li>12. Разработка схемы. Однонаправленных хеш-функций.</li> <li>13. Разработка схемы шифрования с открытым ключом.</li> <li>14. Оформление в виде конспекта материала по Шифрованию методами замены.</li> <li>15. Оформление в виде конспекта материала об Абонентском шифровании.</li> <li>16. Разработка схемы Матричной перестановки.</li> <li>17. Оформление в виде конспекта материала о криптоанализе.</li> <li>18. Подготовка к практическому занятию «Кодирование».</li> <li>19. Разработка схемы Частотного анализа.</li> <li>20. Разработка схемы криптоанализа.</li> </ol>			
<b>Тема 2.3.</b> <b>Организационное обеспечение информационной безопасности</b>	<b>Содержание учебного материала</b>		<b>6</b>	
	1	<b>Занятие № 13. Понятие политики безопасности</b> <ol style="list-style-type: none"> <li>1. Сущность и сферы действия организационной защиты информации.</li> <li>2. Механизмы обеспечения информационной безопасности.</li> <li>3. Разработка политики безопасности.</li> </ol>		2

<b>(6ч+6ч ПЗ)</b>	2	<b>Занятие № 14. Анализ угроз информационной безопасности</b> 1. Проведение анализа угроз и расчета рисков в области информационной безопасности. 2. Выбор механизмов и средств обеспечения информационной безопасности. 3. Модели защиты информационных систем.		2
	3	<b>Занятие № 15. Организационное обеспечение информационной безопасности</b> 1. Правила организации работ подразделений защиты информации. 2. Разработка инструкций по работе со средствами защиты. 3. Организация работы персонала с конфиденциальной информацией.		2
	<b>Практические занятия</b>			<b>6</b>
	2.5	<b>Занятие № 16.</b> Аудит информационной безопасности предприятия		
	2.6	<b>Занятие № 17.</b> Разработка положений о защите персональных данных работников предприятий		
	2.7	<b>Занятие № 18.</b> Разработка политики безопасности предприятия		

	<p><b>Самостоятельная работа обучающихся</b>  Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите</p> <p><b>Тематика домашних заданий:</b></p> <ol style="list-style-type: none"> <li>1. Подготовка к практическому занятию «Простая замена».</li> <li>2. Оформление в виде конспекта материала о Компьютерном шифровании.</li> <li>3. Оформление в виде конспекта материала о Гаммировании.</li> <li>4. Подготовка к практическому занятию «Протоколы управления маршрутизацией».</li> <li>5. Подготовка материала о криптографических протоколах.</li> <li>6. Подготовка к практическому занятию «Абсолютный шифр. Шифроблокнот».</li> <li>7. Подготовка материала о Таблице Виженера.</li> <li>8. Поиск и оформление в виде конспекта материалов по теме «Персональный идентификационный номер»</li> <li>9. Разработка структуры генерации ключей.</li> <li>10. Оформление в виде конспекта материала о Структурной схеме шифрования с открытым ключом.</li> <li>11. Оформление в виде конспекта основных руководящих документов об автоматизированных системах.</li> <li>12. Разработка схемы классификации автоматизированных систем.</li> <li>13. Изучение концепции автоматизированной системы.</li> <li>14. Составление схемы подсистема защиты от несанкционированного доступа.</li> <li>15. Оформление в виде конспекта основных признаков несанкционированного доступа к информации.</li> <li>16. Разработка схемы Парольной аутентификации.</li> <li>17. Оформление в виде конспекта основных положений общеметодологических принципов формирования теории защиты.</li> <li>18. Составление перечня задач теории защиты.</li> <li>19. Принципы построения защиты в сетях  Оформление в виде конспекта вопросов, касающихся понятия стратегии защиты информации и особенностей стратегических решений</li> </ol>	6	
Тема 2.4. Программно-	Содержание учебного материала	12	

аппаратные средства защиты информации (12ч+18 ПЗ)	1	<b>Занятие № 19. Защита информации в ТКС</b> 1. Информационная безопасность в телекоммуникационных и информационно-коммуникационных сетях. 2. Основные направления ЗИ в ТКС		2	
	2	<b>Занятие №20. Защищенность ТКС</b> 1. Структурные схемы систем защиты информации в типовых информационных системах. 2. Показатели защищенности телекоммуникационных систем.		2	
	3	<b>Занятие № 21. Аудит защищенности ТКС</b> 1. Сервисы, обеспечивающие информационную безопасность в многоканальных телекоммуникационных системах и в сетях электросвязи 2. Ограничение физического доступа к автоматизированным системам 3. Идентификация и аутентификация пользователей 4. Ограничение доступа в систему; разграничение доступа 5. Регистрация событий (аудит);		2	
	4	<b>Занятие № 22. Основы криптографии</b> 1. Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. 2. Подсистемы безопасности.		2	
	5	<b>Занятие № 23. Вредоносное ПО</b> 1. Типовые удаленные сетевые атаки и их характеристика. 2. Компьютерные вирусы и защита от них. 3. Антивирусные программы и комплексы.		2	
	6	<b>Занятие № 24. Защита от вредоносного ПО</b> 1. Построение систем антивирусной защиты телекоммуникационных систем и сетей. 2. Программное обеспечения для борьбы с вредоносным ПО		2	
	<b>Практические занятия</b>			<b>18</b>	
	2.8	<b>Занятие № 25.</b> Методы защиты информации. Шифр простой перестановки			
	2.9	<b>Занятие № 26.</b> Методы защиты информации. Шифр Цезаря			
	2.10	<b>Занятие № 27.</b> Резервное копирование информации			

	2.11	<b>Занятие № 28.</b> Основные признаки присутствия на компьютере вредоносных программ		
	2.12	<b>Занятие № 29.</b> Одноразовые блокноты		
	2.13	<b>Занятие № 30.</b> Сеть Фейстеля		
	2.14	<b>Занятие № 31.</b> Шифрование с открытым ключом и электронная цифровая подпись на GPG. Метод шифрования с открытым ключом RSA		
	2.15	<b>Занятие № 32.</b> Оценка защищенности информации по акустическому каналу		
	2.16	<b>Занятие № 33.</b> Оценка защищенности информации по электромагнитному каналу		
	<b>Самостоятельная работа обучающихся</b> Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите <b>Тематика домашних заданий:</b> 1. Оформление в виде конспекта основных положений аппаратных средств защиты информации. 2. Оформление в виде конспекта основных видов контроля безопасности. 3. Подготовка плана Аудита. Оформление в виде конспекта основных положений математической защиты информации. 4. Составление перечня методов кодирования информации.		<b>15</b>	
<b>Тема 5. Защита компьютерных сетей (14 ч.+16 ПЗ)</b>	<b>Содержание учебного материала</b>		<b>14</b>	
	1	<b>Занятие № 34. Технологии защиты данных</b> 1. Технологии защиты данных. 2. Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография).		2
	2	<b>Занятие № 35. Аутентификация</b> 1. Различные технологии аутентификации. 2. Технологии защиты межсетевого обмена данных. 3. Технология обеспечения безопасности сетевых операционных систем. 4. Основы технологии виртуальных защищенных сетей VPN.		2



	3	<b>Занятие № 36. Технологии обнаружения вторжений</b> 1. Технология обнаружения вторжений (анализ защищенности и обнаружения сетевых атак). 2. Требования по защите от несанкционированного доступа 3. Технические средства обеспечения безопасности многоканальных телекоммуникационных систем		2
	4	<b>Занятие № 37. Защита корпоративных сетей</b> 1. Многоуровневая защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. 2. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Internet.		2
	5	<b>Занятие № 38. Защита корпоративных сетей</b> 1. Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. 2. Методы перехвата и навязывания информации. Методы внедрения программных закладок.		2
	6	<b>Занятие № 39. Понятие компьютерного вируса</b> 1. Компьютерные вирусы как особый класс разрушающих программных воздействий. 2. Защита от разрушающих программных воздействий. 3. Антивирусная защита в сетях. 4. Понятие изолированной программной среды. 5. Рекомендации по защите информации Internet		2

	7	<b>Занятие № 40. Организация защиты корпоративной информации</b> 1. Организационные требования к системам информационной защиты ИС. 2. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. 3. Требования по применению способов, методов и средств защиты информации. 4. Требования к документированию событий в системе и выявлению несанкционированного доступа. 5. Организация аудита информационной безопасности ИС и предприятия в целом.		2
<b>Практические занятия</b>				
	2.17	<b>Занятие № 41.</b> Виды и конфигурирования VPN-туннелей	16	
	2.18	<b>Занятие № 42.</b> Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации		
	2.19	<b>Занятие № 43.</b> Исследование защищенности беспроводных сетей передачи данных		
	2.20	<b>Занятие № 44.</b> Программные средства анализа сетей с коммутацией пакетов. Анализ сетевого трафика с помощью программы «Wireshark»		
	2.21	<b>Занятие № 45.</b> Процедура аутентификации пользователя на основе пароля		
	2.22	<b>Занятие № 46.</b> Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA		
	2.23	<b>Занятие № 47.</b> Алгоритмы предупреждения и обнаружения вирусных угроз		
	2.24	<b>Занятие № 48.</b> Организация инженерно-технической защиты информации		

	<p><b>Самостоятельная работа обучающихся</b>          Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите</p> <p><b>Тематика домашних заданий:</b></p> <ol style="list-style-type: none"> <li>1. Подготовка реферата по теме «Аутентификация абонентов при входе в систему и при установлении соединения».</li> <li>2. Схема: Алгоритмы цифровой подписи.</li> <li>3. Составление доклада «Азбука Морзе».</li> <li>4. Подготовка презентаций по теме «Операции с ключами».</li> <li>5. Составление доклада о критериях защиты информации.</li> <li>6. Подготовка реферата по теме «Линейная структура защиты информации».</li> <li>7. Схема «Классы защиты автоматизированных систем».</li> <li>8. Схема «Нормативно-правовое регулирование защиты информации».</li> </ol>	<b>15</b>																								
<p><b>Учебная практика</b>  <b>УП.ПМ.03.02</b></p>	<p><b>Содержание учебного материала</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 5%; text-align: center;"><b>1</b></td> <td>Технические средства защиты информации в телефонных линиях</td> </tr> <tr> <td style="text-align: center;"><b>2</b></td> <td>Диагностика сетевых подключений с помощью встроенных утилит операционной системы Microsoft Windows</td> </tr> <tr> <td style="text-align: center;"><b>3</b></td> <td>Диагностика сетевых подключений с помощью встроенных утилит операционной системы семейства Unix</td> </tr> <tr> <td style="text-align: center;"><b>4</b></td> <td>Определение среднего коэффициента загрузки дуплексного канала передачи на реальной сети Fast Ethernet с помощью пакетного анализатора</td> </tr> <tr> <td style="text-align: center;"><b>5</b></td> <td>Wireshark: выделение ключевых кадров, сохранение данных захвата, просмотр кадра в отдельном окне, печать.</td> </tr> <tr> <td style="text-align: center;"><b>6</b></td> <td>Wireshark: анализ протоколов Ethernet и ARP</td> </tr> <tr> <td style="text-align: center;"><b>7</b></td> <td>Wireshark: анализ протоколов IP и ICMP</td> </tr> <tr> <td style="text-align: center;"><b>8</b></td> <td>Wireshark : анализ протокола TCP</td> </tr> <tr> <td style="text-align: center;"><b>9</b></td> <td>Работа на оборудовании объединенных сетей по обеспечению защиты информации</td> </tr> <tr> <td style="text-align: center;"><b>10</b></td> <td>Установка, настройка специализированного оборудования по защите информации;</td> </tr> <tr> <td style="text-align: center;"><b>11</b></td> <td>Выявление возможных атак на автоматизированные системы;</td> </tr> <tr> <td style="text-align: center;"><b>12</b></td> <td>Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;</td> </tr> </table>	<b>1</b>		Технические средства защиты информации в телефонных линиях	<b>2</b>	Диагностика сетевых подключений с помощью встроенных утилит операционной системы Microsoft Windows	<b>3</b>	Диагностика сетевых подключений с помощью встроенных утилит операционной системы семейства Unix	<b>4</b>	Определение среднего коэффициента загрузки дуплексного канала передачи на реальной сети Fast Ethernet с помощью пакетного анализатора	<b>5</b>	Wireshark: выделение ключевых кадров, сохранение данных захвата, просмотр кадра в отдельном окне, печать.	<b>6</b>	Wireshark: анализ протоколов Ethernet и ARP	<b>7</b>	Wireshark: анализ протоколов IP и ICMP	<b>8</b>	Wireshark : анализ протокола TCP	<b>9</b>	Работа на оборудовании объединенных сетей по обеспечению защиты информации	<b>10</b>	Установка, настройка специализированного оборудования по защите информации;	<b>11</b>	Выявление возможных атак на автоматизированные системы;	<b>12</b>	Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;
<b>1</b>	Технические средства защиты информации в телефонных линиях																									
<b>2</b>	Диагностика сетевых подключений с помощью встроенных утилит операционной системы Microsoft Windows																									
<b>3</b>	Диагностика сетевых подключений с помощью встроенных утилит операционной системы семейства Unix																									
<b>4</b>	Определение среднего коэффициента загрузки дуплексного канала передачи на реальной сети Fast Ethernet с помощью пакетного анализатора																									
<b>5</b>	Wireshark: выделение ключевых кадров, сохранение данных захвата, просмотр кадра в отдельном окне, печать.																									
<b>6</b>	Wireshark: анализ протоколов Ethernet и ARP																									
<b>7</b>	Wireshark: анализ протоколов IP и ICMP																									
<b>8</b>	Wireshark : анализ протокола TCP																									
<b>9</b>	Работа на оборудовании объединенных сетей по обеспечению защиты информации																									
<b>10</b>	Установка, настройка специализированного оборудования по защите информации;																									
<b>11</b>	Выявление возможных атак на автоматизированные системы;																									
<b>12</b>	Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;																									

	<b>13</b>	Конфигурирование автоматизированных систем и информационно-коммуникационных сетей;		
	<b>14</b>	Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей;		
	<b>15</b>	Организации защиты в различных операционных системах и средах.		
	<b>16</b>	Администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи		
	<b>17</b>	Настройка и конфигурирование VPN-туннелей L2, IP SEC L3, защищенные приложения L4 SSL, SSH		
	<b>18</b>	Аутентификация и идентификация с использованием сетевых операционных систем		
<b>Раздел 3. Эксплуатация систем IP-телефонии</b>			<b>180</b>	
<b>МДК.03.03. Эксплуатация систем IP-телефонии</b>			<b>144=(48+48ч. ПЗ)+48ч.СР</b>	
<b>Тема 3. 1. Организация, принципы построения и функционирования сетей IP-телефонии 28 (22+6ч.ПЗ)+ 14 ч.СР</b>	<b>Содержание учебного материала</b>		22	2
	<b>1</b>	<b>Занятие № 1. Организация телефонной сети общего пользования</b> 1. TDM-телефония, основные понятия. 2. Формирование сетей ТФОП. 3. Состав оборудования ТФОП. 4. Включение абонентских и соединительных линий в ЦСК.		
	<b>2</b>	<b>Занятие № 2. Сигнализация в телефонных сетях.</b> 1. Виды сигналов. 2. Абонентская сигнализация. 3. Внутростанционная сигнализация 4. Межстанционная сигнализации.		
	<b>3</b>	<b>Занятие № 3. Принцип построения транспортных сетей.</b> 1. Технологии мультиплексирования. 2. Транспортные сети на базе основе PDH, 3. Транспортные сети на базе основе SHD 4. Транспортные сети на базе основе WDM.		

	<p><b>4</b>     <b>Занятие № 4. Передача речи по IP-сети.</b>  1. Причины появления IP-телефонии.  2. Особенности IP-телефонии.  3. Особенности передачи речевой информации по IP-сетям.  4. Взаимодействие протоколов VoIP.</p>		
	<p><b>5</b>     <b>Занятие № 5. Принципы кодирования речи</b>  1. Цифровые процессы обработки сигналов для речевых кодеков,  2. Основные алгоритмы кодирования речи, используемые в IP-телефонии.  3. Кодеки, стандартизированные ITU-T: G.711, G.723.1, G.726, G.728, G.729.</p>		
	<p><b>6</b>     <b>Занятие № 6. Качество передачи речевой информации по IP-сети</b>  1. Основные характеристики, обеспечивающие качество передачи речевой информации.  2. Анализ характеристик функционирования пакетных сетей.</p>		
	<p><b>7</b>     <b>Занятие № 7. Внедрение и улучшение качества обслуживания в сетях VoIP</b>  1. Механизмы обеспечения качества обслуживания  2. Протокол резервирования ресурсов RSVP  3. Обслуживание очередей.</p>		
	<p><b>8</b>     <b>Занятие № 8. Построение сетей IP-телефонии</b>  1. Классификация сетей IP-телефонии: по способу связи оконечных устройств, по масштабу.  2. Сети на основе Softswitch.  3. Типовые схемы построения корпоративных сетей IP-телефонии: IP-Centrex, IP-PBX, Cisco CallManager, архитектура AVVID  IPCC - IP Contact Center</p>		
	<p><b>9</b>     <b>Занятие № 9. Услуги сетей IP-телефонии</b>  1. Классификация провайдеров услуг IP-телефонии.  2. Принципы тарификации.  3. Биллинг в VoIP сетях.</p>		
	<p><b>10</b>    <b>Занятие № 10. Управление сетями IP-телефонии</b>  1. Особенности системы управления сетями IP-телефонии.  2. Модель управления мультисервисными сетями.</p>		

	<b>11</b>	<b>Занятие № 11. Информационная безопасность в сетях IP-телефонии.</b> 1. Типы угроз в сетях IP-телефонии 2. Особенности системы безопасности в IP-телефонии. 3. Обеспечение безопасности на базе протокола OSP. 4. Обеспечение безопасности IP-телефонии на базе VPN		
	<b>Лабораторные работы</b>		6	
	<b>1.1</b>	<b>Занятие № 12.</b> Трассировка абонентской и межстанционной сигнализации		
	<b>1.2</b>	<b>Занятие № 13.</b> Тестирование кодеков		
	<b>1.3</b>	<b>Занятие № 14.</b> Исследование параметров качества обслуживания		
<b>Самостоятельная работа обучающихся:</b> Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к лабораторным работам с использованием методических пособий и рекомендаций преподавателя. Тематика внеаудиторной самостоятельной работы: Построение ГТС, состав оборудования ЦСК, классификация систем сигнализации, модели транспортных сетей SDH, ATM, OTN, алгоритмы кодирования кодеков.		14		
<b>Тема 3.2.</b> <b>Администрирование сетей IP-телефонии 44 (18+26ч.ПЗ)+ 22 ч.СР</b>	<b>Содержание учебного материала</b>		18	2
	<b>1</b>	<b>Занятие № 15. Конфигурация сети H.323</b> 1. Описание H.323 и общие рекомендации. 2. Функциональные компоненты H.323. 3. Установка и поддержка соединения H.323. 4. Многопользовательские конференции. 5. Обеспечение отказоустойчивости		
	<b>2</b>	<b>Занятие № 16. Администрирование сети H.323</b> 1. Настройка H.323 шлюзов. 2. Настройка H.323 Gatekeeper 3. Мониторинг и устранение неисправностей		
	<b>3</b>	<b>Занятие № 17. Конфигурация сети SIP</b> 1. Технология SIP и связанные с ней стандарты 2. Функциональные компоненты SIP. 3. Сообщения SIP. 4. Адресация SIP. 5. Модель установления соединения 6. Планирование отказоустойчивости.		

4	<b>Занятие № 18. Администрирование сети SIP</b> 1. Настройка оконечных терминалов. 2. Настройка прокси – сервера. 3. Мониторинг и устранение неисправностей		
5	<b>Занятие № 19. Настройка шлюзов</b> 1. Классификация шлюзов, модель организации связи. 2. Команды протокола, структура команд, структура ответов на команды, 3. Описание сеансов связи. 4. Определение способов подключения шлюзов в окружении предприятия, провайдера услуг. 5. Мониторинг и устранение неисправностей		
6	<b>Занятие № 20. Группа Sigtran</b> 1. Система общеканальной сигнализации №7 в IP-сети. 2. Архитектура Sigtran. 3. Основные функциональные возможности SCTP. 4. Множественная адресация. Соединения для нескольких потоков. 5. Мониторинг и устранение неисправностей		
7	<b>Занятие № 21. Установка и инсталляция программного коммутатора</b> 1. Монтажные процедуры. 2. Процедуры инсталляции. 3. Управление аппаратными средствами и портами. 4. Создание аналоговых абонентов. 5. Внутростанционная маршрутизация.		
8	<b>Занятие № 22. Управление программным коммутатором</b> 1. Настройка маршрутизации. 2. Создание групп соединительных линий. 3. Подключение станций с TDM (абонентский доступ TDM). 4. Создание группы абонентов. 5. Настройка дополнительных абонентских услуг		
9	<b>Занятие № 23. Обслуживание программного коммутатора</b> 1. Управление обработкой неисправностей, конфигурацией, тарификацией, рабочими характеристиками и безопасностью. 2. Контроль и обработка аварийных сигналов для сетевых элементов. 3. Инструменты для отслеживания событий и устранения неисправностей. 4. Сигнальные трейсеры. Статистика		

	<b>Лабораторные работы</b>		26	
	2.4	<b>Занятие № 24.</b> Настройка аппаратных IP – телефонов		
	2.5	<b>Занятие № 25.</b> Настройка программных IP – телефонов, факсов		
	2.6	<b>Занятие № 26.</b> Настройка шлюзов		
	2.7	<b>Занятие № 27.</b> Установка, подключение и первоначальные настройки голосового маршрутизатора		
	2.8	<b>Занятие № 28.</b> Настройка таблицы пользователей в голосовом маршрутизаторе		
	2.9	<b>Занятие № 29.</b> Настройка групп в голосовом маршрутизаторе		
	2.10	<b>Занятие № 30.</b> Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе		
	2.11	<b>Занятие № 31.</b> Настройка голосовых сообщений в маршрутизаторе		
	2.12	<b>Занятие № 32.</b> Установка и начальное конфигурирование программного коммутатора.		
	2.13	<b>Занятие № 33.</b> Настройка групп пользователей в программном коммутаторе		
	2.14	<b>Занятие № 34.</b> Конфигурирование IVR в программном коммутаторе		
	2.15	<b>Занятие № 35.</b> Настройка голосовой почты в программном коммутаторе		
	2.16	<b>Занятие № 36.</b> Настройка связи между двумя программными коммутаторами		
	<b>Самостоятельная работа обучающихся:</b> Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Подготовка к лабораторным работам с использованием методических пособий и рекомендаций преподавателя. <b>Тематика внеаудиторной самостоятельной работы:</b> Сигнальные протоколы сети H.323, создание алгоритмов голосовых сообщений для групп пользователей, создание алгоритмов маршрутизации.		22	
<b>Тема3.3. Эксплуатация систем IP-телефонии</b>  <b>24 (8+16ч.ПЗ)+ 12 ч.СР</b>	<b>Содержание учебного материала</b>		8	2
	1	<b>Занятие № 37. Организация эксплуатации систем IP-телефонии.</b> 1. Техническое обслуживание. 2. Плановый текущий ремонт. 3. Плановый капитальный ремонт. 4. Внеплановый ремонт.		



	<b>2</b>	<b>Занятие № 38. Наблюдение за правильной работой оборудования</b> 1. Периодический осмотр и контроль за техническим состоянием оборудования. 2. Устранение обнаруженных дефектов. 3. Регулировка и настройка		
	<b>3</b>	<b>Занятие № 39. Средства мониторинга и анализа систем IP-телефонии</b> 1. Классификация средств мониторинга и анализа систем IP-телефонии		
	<b>4</b>	<b>Занятие № 40. Восстановление работы сети после аварии</b> 1. Схемы послеаварийного восстановления работоспособности сети. 2. Способы резервного копирования данных. 3. Принципы работы хранилищ данных;		
	<b>Лабораторные работы</b>		16	
	<b>3.17</b>	<b>Занятие № 41. Мониторинг и анализ соединений H.323</b>		
	<b>3.18</b>	<b>Занятие № 42. Мониторинг и анализ соединений SIP</b>		
	<b>3.19</b>	<b>Занятие № 43. Мониторинг и анализ протокола MGCP</b>		
	<b>3.20</b>	<b>Занятие № 44. Мониторинг вызовов в программном коммутаторе</b>		
	<b>3.21</b>	<b>Занятие № 45. Создание резервных копий баз данных</b>		
	<b>3.22</b>	<b>Занятие № 46. Диагностика и поиск неисправностей в системах IP-телефонии</b>		
	<b>3.23</b>	<b>Занятие № 47. Устранение неисправностей в системах IP- телефонии</b>		
	<b>3.24</b>	<b>Занятие № 48. Восстановление работы сети после аварии</b>		

	<p><b>Самостоятельная работа при изучении Раздела 3 ПМ</b>          Работа с конспектами, учебной и специальной литературой (по параграфам, главам учебных пособий, указанным преподавателем).          Подготовка к лабораторным занятиям с использованием методических рекомендаций преподавателя, оформление лабораторных работ и подготовка их к защите</p> <p><b>Тематика домашних заданий</b>          Основы VoIP. Передача речи по IP-сетям. История технологии VoIP. Достоинства технологии VoIP. Проблемы, возникающие при использовании среды IP для передачи речи. Методы уменьшения объёмов передаваемого трафика. Кодирование информации. Протоколы RTP/RTCP.          Сети и сценарии IP-телефонии Основные сценарии IP-телефонии. Базовые архитектуры построения сетей IP- телефонии. Основные услуги, реализуемые с использованием технологии VoIP.          Сеть IP-телефонии согласно рекомендации H.323 Архитектура сети H.323 и назначение её элементов. Конференции в H.323. Структура стека протоколов H.323. Протоколы RAS, H.225 и H.245. Базовые сценарии установления соединения в сети, построенной согласно H.323.</p>																				
<p><b>Производственная практика (по профилю специальности)</b></p>	<table border="1"> <tr> <td data-bbox="517 823 600 855">1</td> <td data-bbox="600 823 1664 855">Ознакомление со структурой предприятия</td> </tr> <tr> <td data-bbox="517 855 600 887">2</td> <td data-bbox="600 855 1664 887">Вводный инструктаж по технике безопасности и охране труда</td> </tr> <tr> <td data-bbox="517 887 600 919">3</td> <td data-bbox="600 887 1664 919">Ознакомление с отделами и службами предприятия</td> </tr> <tr> <td data-bbox="517 919 600 1046">4</td> <td data-bbox="600 919 1664 1046">Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: профилактические работы в объектах сетевой инфраструктуры</td> </tr> <tr> <td data-bbox="517 1046 600 1118">5</td> <td data-bbox="600 1046 1664 1118">Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: Структура системы управления</td> </tr> <tr> <td data-bbox="517 1118 600 1190">6</td> <td data-bbox="600 1118 1664 1190">Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: архитектура системы управления</td> </tr> <tr> <td data-bbox="517 1190 600 1262">7</td> <td data-bbox="600 1190 1664 1262">Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: правила системы управления</td> </tr> <tr> <td data-bbox="517 1262 600 1334">8</td> <td data-bbox="600 1262 1664 1334">Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с протоколами</td> </tr> <tr> <td data-bbox="517 1334 600 1406">9</td> <td data-bbox="600 1334 1664 1406">Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с протоколами</td> </tr> </table>	1	Ознакомление со структурой предприятия	2	Вводный инструктаж по технике безопасности и охране труда	3	Ознакомление с отделами и службами предприятия	4	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: профилактические работы в объектах сетевой инфраструктуры	5	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: Структура системы управления	6	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: архитектура системы управления	7	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: правила системы управления	8	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с протоколами	9	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с протоколами	<p>144</p>	
1	Ознакомление со структурой предприятия																				
2	Вводный инструктаж по технике безопасности и охране труда																				
3	Ознакомление с отделами и службами предприятия																				
4	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: профилактические работы в объектах сетевой инфраструктуры																				
5	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: Структура системы управления																				
6	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: архитектура системы управления																				
7	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: правила системы управления																				
8	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с протоколами																				
9	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с протоколами																				

<b>10</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с ПО для восстановления
<b>11</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: контроль восстановления системы
<b>12</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: анализ результатов восстановления системы
<b>13</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с сервером
<b>14</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: чтение кодов
<b>15</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа над ошибками
<b>16</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: удаленное администрирование сервера с рабочих станций
<b>17</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: программы удаленного доступа
<b>18</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: планирования восстановления работоспособности
<b>19</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: определение точек восстановления
<b>20</b>	Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: мониторинг сети после восстановления
<b>21</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: мониторинг СКС
<b>22</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: работа с кабельным сканером
<b>23</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: работа с кабельным тестером
<b>24</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: работа с БД

<b>25</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: создание БД на сервере
<b>26</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: создание таблиц
<b>27</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: импорт данных
<b>28</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: хранение данных
<b>29</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: редактирование данных
<b>30</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: создание плана восстановления сети
<b>31</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: обеспечение базовых механизмов защиты сети
<b>32</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: разработка моделей систем защиты информации в сети
<b>33</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: защита информации в СКС
<b>34</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: программная защита информации
<b>35</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: анализ входящего трафика
<b>36</b>	Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: анализ исходящего трафика
<b>37</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: установка межсетевых экранов на предприятии
<b>38</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: установка на рабочие станции антивирусных программ на предприятии
<b>39</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: установка и настройка ОС на предприятии

<b>40</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: тестирование сетевого оборудования на предприятии		
<b>41</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: устранение неполадок сети на предприятии		
<b>42</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: ремонт сетевого оборудования		
<b>43</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: использование активного сетевого оборудования		
<b>44</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: использование пассивного сетевого оборудования		
<b>45</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: заполнение технической документации		
<b>46</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: Работа по созданию, редактированию, удалению пользователей в DOMAIN		
<b>47</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: построение физической карты локальной сети		
<b>48</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: мониторинг сети с помощью специализированного ПО		
<b>49</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: анализ работы сети с помощью программных и аппаратных средств		
<b>50</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: контроль доступа		
<b>51</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: сохранение целостности данных		
<b>52</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: журналирование		

<b>53</b>	Организация бесперебойной работы системы по резервному копированию и восстановлению информации: работа со встроенными сканерами диагностики и управления		
<b>54</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: контроль утечки конфиденциальной информации		
<b>55</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: определение уязвимостей КС		
<b>56</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: определение угроз утечки конфиденциальной информации		
<b>57</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка IPSec		
<b>58</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка VPN		
<b>59</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: программное обеспечение для работы с VPN		
<b>60</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: нормативно-правовая база VPN		
<b>61</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: определение паразитирующей нагрузки		
<b>62</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: устранение паразитирующей нагрузки		
<b>63</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: определение программных закладок		
<b>64</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка защиты беспроводных сетей с помощью систем шифрования		
<b>65</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: установка системы обнаружения вторжений		

	<b>66</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка системы обнаружения атак		
	<b>67</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: анализ сети на инсайдеров		
	<b>68</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: установка DLP		
	<b>69</b>	Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка DLP		
	<b>70</b>	Составление отчета по ходу выполнения работ		
	<b>71</b>	Заполнение дневника по практике		
	<b>72</b>	Сдача рабочего места		
<b>Всего</b>			<b>750</b>	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

## **4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

### **4.1. Требования к материально-техническому обеспечению**

Реализация профессионального модуля предполагает наличие лаборатории эксплуатации объектов сетевой инфраструктуры, лаборатории программно-аппаратной защиты объектов сетевой инфраструктуры, лаборатории Информационно-коммуникационных сетей связи, а также полигона технического контроля и диагностики сетевой инфраструктуры.

#### **Оборудование лаборатории эксплуатации объектов сетевой инфраструктуры**

Оборудование лаборатории и рабочих мест мастерской:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- печатные/электронные демонстрационные пособия.

Технические средства обучения:

компьютеры с лицензионным программным обеспечением  
проектор, экран

Для выполнения лабораторных и практических работ:

оборудование: объединенных сетей, сетей доступа (ADSL, Wi Fi), межсетевые экраны, операционные системы WINDOWS, LINUX,

Коммутаторы, маршрутизаторы, учрежденческая телефонная станция CORAL2, модемы

#### **Оборудование лаборатории программно-аппаратной защиты объектов сетевой инфраструктуры:**

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- печатные/электронные демонстрационные пособия.

**Технические средства обучения:**

- компьютеры, лицензионное программное обеспечение;
- мультимедийный проектор;
- экран.

Для выполнения лабораторных и практических работ:

оборудование: объединенных сетей, сетей доступа (ADSL, Wi Fi), межсетевые экраны, операционные системы WINDOWS, LINUX, антивирусные программы, коммутаторы, маршрутизаторы, учрежденческая телефонная станция CORAL2, модемы и др..

- программное обеспечение.

#### **Оборудование лаборатории Информационно-коммуникационных сетей связи**

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- печатные/электронные демонстрационные пособия.

Технические средства обучения:

- компьютер, лицензионное программное обеспечение;
- мультимедийный проектор;

Демонстрационные материалы (блоки, узлы, элементы, образцы кабелей, стойки с кроссами), инструменты и материалы

#### **Оборудование полигона «технического контроля и диагностики сетевой инфраструктуры»**

- автоматизированные рабочие места на 25-30 обучающихся;
- автоматизированное рабочее место преподавателя;
- комплект учебно-методической документации;
- Проектор, компьютеры, лицензионное программное обеспечение:



- Сервер лаборатории
- серверная стойка 42 U;
- комплект сетевого оборудования (сетевые адаптеры, повторители, сетевые коммутаторы, концентраторы, мосты, маршрутизаторы, мосты-маршрутизаторы, шлюзы);
- инструмент для работы с витой парой, тестеры кабельные
- кабель витая пара.

техническое оснащение рабочих мест полигона:

оборудование: объединенных сетей, сетей доступа (ETTH, ADSL, Wi Fi), межсетевые экраны, операционные системы WINDOWS, LINUX, коммутаторы, маршрутизаторы  
программное оборудование.

## 4.2. Информационное обеспечение обучения

### Основные источники

1. Кенин, А. Практическое руководство системного администратора/А.Кенин. – СПб.: БХВ-Петербург, 2013.
2. Кенин, А.М. Самоучитель системного администратора/А.Кенин. - СПб.: БХВ-Петербург, 2012.
3. Кузин, А.В. Компьютерные сети: учебное пособие для студ. учрежд. СПО/А.В.Кузин. - М.: Форум: ИНФРА-М, 2017.
4. Логинов, М.Д. Техническое обслуживание средств вычислительной техники/М.Д.Логинов. - М.: Бином. Лаборатория знаний, 2013.
5. Максимов, Н.В. Компьютерные сети: учебное пособие/Н.В.Максимов, И.И.Попов. - М.: Форум, 2017.
6. Назаров, А.В. Эксплуатация объектов сетевой инфраструктуры: учебник для студ. учрежд. СПО / А.В. Назаров, А.Н. Енгальчев, В.П. Мельников. – М.: КУРС; ИНФРА-М, 2017.
7. Таненбаум, Э. Компьютерные сети/Э.Таненбаум, Д.Уэзеролл. - СПб.: Питер, 2014.
8. Чекмарев, Ю.В. Локальные вычислительные сети: учебное пособие/ Ю.В. Чекмарев. - Саратов: Профобразование, 2017.
9. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для СПО /А.В.Васильков, И.А.Васильков. - М.: Форум, 2017.
10. Зверева, В.П. Участие в планировании и организации работ по обеспечению защиты информации: учебник для студ. учрежд. СПО/ В.П. Зверева, А.В. Назаров. — М.: КУРС: ИНФРА-М, 2017.
11. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - М.: Форум: ИНФРА-М, 2015.
12. Партыка, Т.Л. Информационная безопасность: учебное пособие для студ. учрежд. СПО /Т.Л.Партыка, И.И.Попов. - М.: Форум: ИНФРА-М, 2017.
13. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие для вузов/П.Б.Хорев. - М.: Форум: Инфра-М, 2015.
14. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО/В.Ф.Шаньгин. - М.: ФОРУМ: ИНФРА-М, 2017.
15. IP-телефония в компьютерных сетях: учебное пособие/ И.В.Баскаков, А.В.Пролетарский, С.А.Мельников. - М.: БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
16. Гольдштейн, Б.С. IP-телефония / Б.С.Гольдштейн, А.В.Пинчук, А.Л.Суховицкий. - СПб. БХВ-Петербург, 2014.

17. Гольдштейн Б. С. Call-центры и компьютерная телефония/Б.С.Гольдштейн, В.А.Фрейнкман. - СПб.: БХВ-Петербург, 2014.
18. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие/ Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017.
19. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А. Бузов. - М.: Горячая линия-Телеком, 2014.
20. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для СПО /А.В. Васильков, И.А.Васильков. - М.: ФОРУМ, 2017.
21. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. - М.: ФОРУМ: ИНФРА-М, 2017.
22. Гольдштейн, Б.С. Сети связи/Б.С. Гольдштейн, Н.А. Соколов, Г.Г.Яновский. – М.: БХВ-Петербург, 2014.
23. Атцик, А.А. Протокол MEGACO/H.248 /А.А.Атцик, А.Б.Гольдштейн, Б.С. Гольдштейн. – СПб.: БХВ-Петербург, 2014.
24. Гольдштейн, Б. С. Softswitch/ Б.С..Гольдштейн, А.Б.Гольдштейн. - СПб.: БХВ-Петербург, 2014.
25. Гольдштейн, Б. С. Сигнализация в сетях связи. Том 1/Б.С.Гольдштейн. - СПб. : БХВ-Петербург, 2014

#### **Дополнительные источники:**

1. Богомазова, Г.Н. Модернизация программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования: учебник/Г.Н.Богомазова. - М.: Академия, 2015.
2. Богомазова, Г.Н. Установка и обслуживание программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования: учебник/Г.Н.Богомазова. - М.: Академия, 2015.
3. Васин, Н. Н. Построение сетей на базе коммутаторов и маршрутизаторов/Н.Н.Васин. - М.: Интернет-университет информационных технологий, 2016.
4. Есина, А. П. Модернизация аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования: учебник для студ. учреждений СПО /А.П.Есина, З.А.Гаврилова. – М.: Академия, 2016.
5. Сенкевич, Г. Искусство восстановления данных/Г.Сенкевич. - СПб.: БХВ-Петербург, 2011.
6. Сперанский, Д.В. Моделирование, тестирование и диагностика цифровых устройств/ Д.В.Сперанский, Ю.А.Скобцов, В.Ю.Скобцов. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
7. Построение коммутируемых компьютерных сетей /Е.А.Смирнова [и др.].- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
8. Чащина, Е.Л. Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники: учебник для студ. учреждений СПО/Е.Л.Чащина. – М.: Академия, 2016.
9. Чащина, Е.Л. Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники: практикум: учебное пособие для студ. учреждений СПО/Е.Л.Чащина. – М.: Академия, 2016.

10. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие/ А.А.Афанасьев, Л.Т.Веденьев, А.А.Воронцов. - М.: Горячая линия - Телеком, 2012.
11. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие/ Е.К.Баранова, А.В.Бабаш. - 3-е изд., перераб. и доп. - М.: РИОР: ИНФРА-М, 2017.
12. Глинская, Е.В Информационная безопасность конструкций ЭВМ и систем: учебное пособие/Е.В.Глинская, Н.В.Чичварин. - М.: ИНФРА-М, 2016.
13. Грибунин, В.Г. Цифровая стеганография/ В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. - М.: СОЛОН-ПРЕСС, 2017.
14. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - М.: Форум: ИНФРА-М, 2017.
15. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками/П.Н.Девянин. - М.: Горячая линия-Телеком, 2012.
16. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие / А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2016.
17. Жук, А. П. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015.
18. Мартемьянов, Ю.Ф. Операционные системы. Концепции построения и обеспечения безопасности: учебное пособие для вузов/ Ю.Ф.Мартемьянов, Ал.В.Яковлев, Ан.В. Яковлев.- М.: Горячая линия-Телеком, 2011.
19. Методы и средства обеспечения программно-аппаратной защиты информации: научно-техническое издание/ А.И. Астайкин [и др.]. - Саратов: Российский федеральный ядерный центр – ВНИИЭФ, 2015.
20. Молдовян, А.А. Протоколы аутентификации с нулевым разглашением секрета /А.А.Молдовян, Д.Н.Молдовян, А.Б.Левина. - СПб.: Университет ИТМО, 2016.
21. Петренко, С.А. Политики безопасности компании при работе в Интернет/ С.А. Петренко, В.А. Курбатов. - Саратов: Профобразование, 2017.
22. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты/ А.А. Петров. - Саратов: Профобразование, 2017.
23. Романьков, В.А. Введение в криптографию: курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. — М.: Форум: ИНФРА-М, 2017.
24. Рябко, Б. Я. Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. – М.: Горячая линия–Телеком, 2012.
25. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства/В.Ф.Шаньгин. – Саратов: Профобразование, 2017.
26. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов/О. И.Шелухин, Д. Ж. Сакалема, А. С. Филинова.- М.: Горячая линия-Телеком, 2013.
27. Гольдштейн, Б. С. Системы коммутации: учебник для вузов/Б.С.Гольдштейн. - СПб. : БХВ-Петербург, 2014.
28. Гольдштейн, Б. С. Протокол SIP: справочник /Б.С.Гольдштейн, А.А.Зарубин, В.В.Саморезов. - СПб.: БХВ-Петербург, 2014.

#### **Интернет-ресурсы:**

1. СІТ-Forum: Центр информационных технологий: материалы сайта [Электронный ресурс]. - Режим доступа: <http://citforum.ru/>, свободный.
2. Библиотека учебных курсов Microsoft [Электронный ресурс]. - Режим доступа: <http://msdn.microsoft.com/ru-ru/gg638594>, свободный.
3. Интернет-Университет информационных технологий. Библиотека учебных

- курсов [Электронный ресурс]. - Режим доступа: <https://www.intuit.ru/studies/courses>, свободный.
4. Сайт компании Cisco [Электронный ресурс]. - Режим доступа: <http://www.cisco.ru/>, свободный.
  5. Сайт компании D-Link [Электронный ресурс]. - Режим доступа: <http://www.dlink.ru/>, свободный.
  6. SecurityLab. Защита информации и информационная безопасность [Электронный ресурс]: информационный портал/ООО "Positive Technologies". - Режим доступа: <http://www.securitylab.ru>, свободный.
  7. Атцик, А.А. IP-коммуникации в NGN [Электронный ресурс]: учебное пособие / А. А. Атцик, А. Б. Гольдштейн, В. В. Саморезов. - СПб. : СПбГУТ, 2007. — Режим доступа: [http://libr.itut.ru/Jirbis2\\_spbgut/index.php?option=com\\_irbis&view=irbis&Itemid=308](http://libr.itut.ru/Jirbis2_spbgut/index.php?option=com_irbis&view=irbis&Itemid=308), свободный.
  8. Гольдштейн, А.Б. IP-телефония [Электронный ресурс]: методические рекомендации к лабораторным работам/ А. Б. Гольдштейн, В. В. Саморезов. - СПб.: СПбГУТ, 2003. - Режим доступа: [http://libr.itut.ru/Jirbis2\\_spbgut/index.php?option=com\\_irbis&view=irbis&Itemid=308](http://libr.itut.ru/Jirbis2_spbgut/index.php?option=com_irbis&view=irbis&Itemid=308), свободный.
  9. Гольдштейн, Б.С. Протоколы IP-телефонии: RTP, RTSP [Электронный ресурс] : учебное пособие / Б. С. Гольдштейн, В. Ю. Гойхман, Ю. В. Столповская". - СПб. : СПбГУТ, 2014. — Режим доступа: [http://libr.itut.ru/Jirbis2\\_spbgut/index.php?option=com\\_irbis&view=irbis&Itemid=308](http://libr.itut.ru/Jirbis2_spbgut/index.php?option=com_irbis&view=irbis&Itemid=308), свободный.
  10. Некоторые аспекты технологий IP-телефонии [Электронный ресурс]. — Режим доступа: <http://www.ixbt.com/comm/ip-aspects.html>, свободный.
  11. Сайт IP-телефония на базе Asterick [Электронный ресурс]. - Режим доступа: <http://www.voxlink.ru/>, свободный.

#### **4.3. Общие требования к организации образовательного процесса**

Программа профессионального модуля обеспечивается учебно-методической документацией по всем разделам междисциплинарного курса.

Внеаудиторная работа сопровождается методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение.

Реализация программы профессионального модуля обеспечивается доступом каждого обучающегося к базам данных и библиотечным фондам, формируемым по полному перечню разделов модуля. Во время самостоятельной подготовки обучающиеся обеспечиваются доступом к сети Интернет.

Материально-техническая база, перечисленная в п. 4.1, обеспечивает проведение всех видов практических занятий, практики. Материально-техническая база должна соответствовать действующим санитарным и противопожарным нормам.

## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**Контроль и оценка** результатов освоения междисциплинарных курсов осуществляется преподавателем в процессе проведения занятий, проверке домашних заданий, контрольных работ, тестирования, а также оценки выполнения обучающимися самостоятельных работ, индивидуальных заданий, проектов, исследований. Промежуточная аттестация по междисциплинарным курсам проводится в форме дифференцированных зачётов.

**Контроль и оценка** результатов освоения профессиональных компетенций осуществляется при проведении экзаменационной комиссией экзамена квалификационного с использованием контрольно-оценочных средств (КОС) позволяющих оценить освоенные компетенции.

Основными показателям результатов подготовки являются освоение профессиональных компетенций:

<b>Результаты (освоенные профессиональные компетенции)</b>	<b>Основные показатели оценки результата</b>	<b>Формы и методы контроля и оценки</b>
ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей	<ul style="list-style-type: none"> <li>– точность и скорость настройки сети;</li> <li>– качество рекомендаций по повышению работоспособности сети;</li> <li>– выбор технологического оборудования для настройки сети;</li> <li>– расчет времени для настройки сети;</li> <li>– точность и грамотность оформления технологической документации.</li> </ul>	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы <ul style="list-style-type: none"> <li>- на практических занятиях,</li> <li>-при решении ситуационных задач,</li> <li>-при выполнении определенных видов работ</li> </ul> производственной практики, -зачет по разделу практики
ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях	<ul style="list-style-type: none"> <li>– точность и скорость настройки сети;</li> <li>– качество анализа свойств сети, исходя из ее служебного назначения;</li> <li>– качество рекомендаций по повышению технологичности сети;</li> <li>– точность и грамотность оформления технологической документации.</li> </ul>	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы <ul style="list-style-type: none"> <li>- на практических занятиях,</li> <li>-при выполнении определенных видов работ</li> </ul> производственной практики,

		-зачет по разделу практики
ПК 3.3. Осуществлять эксплуатацию сетевых конфигураций	<ul style="list-style-type: none"> <li>– точность и скорость настройки сети;</li> <li>– качество анализа и рациональность выбора сетевых конфигураций;</li> <li>– выбор способов настройки и технологически грамотное назначение технологической базы</li> </ul>	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при выполнении определенных видов работ производственной практики, - зачет по разделу практики
ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации	– выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, - зачет по разделу практики
ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования	– выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, - зачет по разделу практики
ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять	– выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов	Экспертная оценка результатов деятельности обучающихся в процессе освоения

устаревшее оборудование и программные средства сетевой инфраструктуры.		образовательной программы - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики Междисциплинарный экзамен
--	--	---

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

<b>Результаты (освоенные общие компетенции)</b>	<b>Основные показатели оценки результата</b>	<b>Формы и методы контроля и оценки</b>
ОК 1 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	1) Формулировка области и объектов профессиональной деятельности техника по компьютерным сетям в соответствии с ФГОС по специальности 09.02.02 Компьютерные сети	<i>оценка на экзамене по модулю</i>
	2) участие в профессиональных конкурсах, конференциях, проектах, выставках, фестивалях, олимпиадах	<i>- оценка профессионального портфолио студента на экзамене по модулю</i>
ОК 2 Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	1) четкое выполнение должностных обязанностей в рамках конкретного проекта	<i>- интерпретация результатов наблюдения на производственной практике;</i>
	2) дана адекватная оценка эффективности и качества выбранных методов решения профессиональных задач	<i>- оценка анализа эффективности методов решения профессиональных задач на производственной практике</i>
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	-верность принятия решения в смоделированной нестандартной ситуации по разработке и адаптации ПО с оценкой возможных рисков при их реализации;	<i>Накопительная оценка за решения смоделированных нестандартных ситуации на учебной практике</i>
ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных	- отобранная на основе анализа и оценки информация позволяет ставить и решать профессиональные задачи и	<i>Накопительная оценка за представленную информацию на учебной практике</i>

задач, профессионального и личностного развития.	задачи профессионального и личностного развития	
ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.	- для разработки и адаптации ПО использованы современные информационно-коммуникационные технологии	<i>интерпретация результата наблюдения за деятельностью на производственной практике</i>
ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.	- эффективность взаимодействия с коллегами, клиентами при разработке технического задания проекта	<i>интерпретация результата наблюдения за деятельностью студента на производственной практике</i>
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий	при обеспечении проектной деятельности: - верно поставлены цели и осуществлена мотивация подчиненных, - эффективно организована работа с подчиненными, - верно выбраны методы контроля за качеством проведения проектных операций;	<i>интерпретация результата наблюдения за деятельностью студента на производственной практике</i>
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	1) верно определены задачи профессионального и личностного развития; 2) план самообразования обоснован задачами профессионального и личностного развития и включает мероприятия по повышению квалификации;	<i>оценка плана самообразования на учебной практике</i>
ОК 9. Быть готовым к смене технологий в профессиональной деятельности.	- проектная деятельность организована с использованием новых отраслевых технологий	<i>интерпретация результата наблюдения за деятельностью студента на производственной практике</i>



## КОНКРЕТИЗАЦИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

<b>ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей</b>	
<i><b>Иметь практический опыт:</b></i>	<i><b>Виды работ на практике:</b></i>
<ul style="list-style-type: none"> <li>– поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры;</li> </ul>	<p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: контроль утечки конфиденциальной информации</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: определение уязвимостей КС</p> <p>Поддержка пользователей сети, настройка аппаратного и программно обеспечения сетевой инфраструктуры: определение угроз утечки конфиденциальной информации</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка IPSec</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка VPN</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: программное обеспечение для работы с VPN</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: нормативно-правовая база VPN</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: определение паразитирующей нагрузки</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: устранение паразитирующей нагрузки</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: определение программных закладок</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка защиты беспроводных сетей с помощью систем шифрования</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения</p>

	<p>сетевой инфраструктуры: установка системы обнаружения вторжений</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка системы обнаружения атак</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: анализ сети на инсайдеров</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: установка DLP</p> <p>Поддержка пользователей сети, настройка аппаратного и программного обеспечения сетевой инфраструктуры: настройка DLP</p>
<b>Уметь:</b>	<b>Тематика лабораторных/практических работ:</b>
<ul style="list-style-type: none"> <li>– выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;</li> <li>– устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;</li> </ul>	<ul style="list-style-type: none"> <li>– Поддержка пользователей в сети</li> <li>– Создание пользователей в домене (создание пароля, создание групп и распределение пользователей по группам)</li> <li>– Настройка прав доступа</li> <li>– Оформление технической документации, правила оформления документов</li> <li>– Настройка аппаратного и программного обеспечения сети.</li> <li>– Настройка сетевой карты (имя компьютера, рабочая группа, введение компьютера в домен)</li> <li>– Выполнение мониторинга и анализа работы локальной сети с помощью программных средств</li> <li>– Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы, коммутационное оборудование)</li> </ul>
<b>Знать:</b>	<b>Перечень тем, включенных в МДК:</b>
<ul style="list-style-type: none"> <li>– архитектуру и функции систем управления сетями, стандарты систем управления;</li> <li>– задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;</li> <li>– средства мониторинга и анализа локальных сетей;</li> </ul>	<b>Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры. Профилактические работы</b>
<b>Самостоятельная работа</b>	<b>Самостоятельная работа обучающихся</b>

	<p>преподавателя Подготовка к лабораторно-практическим работам с использованием методических рекомендаций; оформление лабораторно-практических работ, отчетов и подготовка к их защите.</p> <p><b>Примерная тематика внеаудиторной работы</b></p> <ol style="list-style-type: none"> <li>1. Технические регламенты, виды документов для технических осмотров, методы и принципы проверки различного оборудования, методы резервирования, программы для резервирования информации, BackUp.</li> <li>2. Маршрутизация в Windows Server.</li> <li>3. Управление общими свойствами IP-маршрутизации.</li> <li>4. Основные сведения о NAT, различие между NAT и ICS.</li> <li>5. Удалённый доступ по телефонной линии, авторизация подключений удалённого доступа</li> <li>6. Поиск неисправностей по принципу локализации неисправностей конкретного оборудования.</li> <li>7. Изучить и понять принцип работы новых контрольно-измерительных аппаратов</li> </ol>
<p><b>ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях</b></p>	
<p><b><i>Иметь практический опыт:</i></b></p>	<p><b><i>Виды работ на практике:</i></b></p>
<p>– обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;</p>	<p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: профилактические работы в объектах сетевой инфраструктуры</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: Структура системы управления</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: архитектура системы управления</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: правила системы управления</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с протоколами</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа с протоколами</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети</p>

	<p>после сбоя: работа с ПО для восстановления</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети</p> <p>после сбоя: контроль восстановления системы</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети</p> <p>после сбоя: анализ результатов восстановления системы</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети</p> <p>после сбоя: работа с сервером</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети</p> <p>после сбоя: чтение кодов</p>
<b>Уметь:</b>	<b>Тематика лабораторных/практических работ:</b>
<ul style="list-style-type: none"> <li>– использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры;</li> <li>– тестировать кабели и коммуникационные устройства</li> </ul>	<ul style="list-style-type: none"> <li>– Работа контрольно-измерительной аппаратуры.</li> <li>– Замена расходных материалов.</li> <li>– Мелкий ремонт периферийного оборудования</li> <li>– Программная диагностика неисправностей.</li> <li>– Аппаратная диагностика неисправностей</li> <li>– Поиск неисправностей технических средств.</li> <li>– Выполнение действий по устранению неисправностей.</li> </ul>
<b>Знать:</b>	<b>Перечень тем, включенных в МДК:</b>
<ul style="list-style-type: none"> <li>– классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;</li> </ul>	<b>Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры. Профилактические работы</b>
<b>Самостоятельная работа</b>	<p><b>Самостоятельная работа обучающихся преподавателя</b> Подготовка к лабораторно-практическим работам с использованием методических рекомендаций; оформление лабораторно-практических работ, отчетов и подготовка к их защите.</p> <p><b>Примерная тематика внеаудиторной работы</b></p> <ol style="list-style-type: none"> <li>1. Физическая, логическая инфраструктуры.</li> <li>2. Сетевые подключения, протоколы, адресация, система имён.</li> <li>3. Автоматическое назначение частных IP-адресов.</li> <li>4. Маршрутизация и инфраструктура сети Windows Server</li> </ol>

	<p>5. Установка сетевых компонентов Windows, установка Active Directory в сети Windows.</p> <p>6. Разбиение на подсети, механизм разбиения на подсети, определение емкости подсети</p>
<b>ПК 3.3. Эксплуатировать сетевые конфигурации</b>	
<b><i>Иметь практический опыт:</i></b>	<b><i>Виды работ на практике:</i></b>
<p>– удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;</p>	<p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: мониторинг СКС</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: работа с кабельным сканером</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: работа с кабельным тестером</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: работа с БД</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: создание БД на сервере</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: создание таблиц</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: импорт данных</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: хранение данных</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: редактирование данных</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: создание плана восстановления сети</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: обеспечение базовых механизмов защиты сети</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: разработка моделей систем защиты информации в сети</p>

<b>Уметь:</b>	<b>Тематика лабораторных/практических работ:</b>
<ul style="list-style-type: none"> <li>– наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;</li> </ul>	<ul style="list-style-type: none"> <li>– Анализ сетевого трафика средствами сетевого монитора</li> <li>– Основные сведения о сетевом мониторе</li> <li>– Анализ рисков информационной безопасности</li> <li>– Обеспечение информационной безопасности в ведущих зарубежных странах</li> <li>– Изучение нормативно-правовой базы ИБ</li> <li>– Построение концепции информационной безопасности предприятия</li> <li>– Аудит информационной безопасности предприятия</li> <li>– Разработка положений о защите персональных данных работников предприятий</li> <li>– Разработка политики безопасности предприятия</li> <li>– Методы защиты информации. Шифр простой перестановки</li> <li>– Методы защиты информации. Шифр Цезаря</li> <li>– Резервное копирование информации</li> <li>– Основные признаки присутствия на компьютере вредоносных программ</li> <li>– Одноразовые блокноты</li> <li>– Сеть Фейстеля</li> <li>– Шифрование с открытым ключом и электронная цифровая подпись на GPG. Метод шифрования с открытым ключом RSA</li> <li>– Оценка защищенности информации по акустическому каналу</li> <li>– Оценка защищенности информации по электромагнитному каналу</li> <li>– Виды и конфигурирования VPN-туннелей</li> <li>– Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации</li> <li>– Исследование защищенности беспроводных сетей передачи данных</li> <li>– Программные средства анализа сетей с коммутацией пакетов. Анализ сетевого трафика с помощью программы</li> </ul>

	<p>«Wireshark»</p> <ul style="list-style-type: none"> <li>– Процедура аутентификации пользователя на основе пароля</li> <li>– Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA</li> <li>– Алгоритмы предупреждения и обнаружения вирусных угроз</li> <li>– Организация инженерно-технической защиты информации</li> <li>– Трассировка абонентской и межстанционной сигнализации</li> <li>– Тестирование кодеков</li> <li>– Исследование параметров качества обслуживания</li> <li>– Настройка аппаратных IP – телефонов</li> <li>– Настройка программных IP – телефонов, факсов</li> <li>– Настройка шлюзов</li> <li>– Установка, подключение и первоначальные настройки голосового маршрутизатора</li> <li>– Настройка таблицы пользователей в голосовом маршрутизаторе</li> <li>– Настройка групп в голосовом маршрутизаторе</li> <li>– Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе</li> <li>– Настройка голосовых сообщений в маршрутизаторе</li> <li>– Установка и начальное конфигурирование программного коммутатора.</li> <li>– Настройка групп пользователей в программном коммутаторе</li> <li>– Конфигурирование IVR в программном коммутаторе</li> <li>– Настройка голосовой почты в программном коммутаторе</li> <li>– Настройка связи между двумя программными коммутаторами</li> <li>– Мониторинг и анализ соединений H.323</li> <li>– Мониторинг и анализ соединений SIP</li> <li>– Мониторинг и анализ протокола MGCP</li> <li>– Мониторинг вызовов в программном коммутаторе</li> <li>– Создание резервных копий баз данных</li> <li>– Диагностика и поиск неисправностей в системах IP- телефонии</li> <li>– Устранение неисправностей в системах</li> </ul>
--	--

	<p>IP- телефонии</p> <p>– Восстановление работы сети после аварии</p>
<b>Знать:</b>	<b>Перечень тем, включенных в МДК:</b>
<p>– расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;</p>	<p>Тема 1.2. Управление сетями</p> <p>Тема 2.1. Основы информационной безопасности</p> <p>Тема 2.2. Правовое обеспечение информационной безопасности</p> <p>Тема 2.3. Организационное обеспечение информационной безопасности</p> <p>Тема 2.4. Программно-аппаратные средства защиты информации</p> <p>Тема 5. Защита компьютерных сетей</p> <p>Тема 3. 1. Организация, принципы построения и функционирования сетей IP-телефонии</p> <p>Тема 3.2. Администрирование сетей IP-телефонии</p> <p>Тема 3. Эксплуатация систем IP-телефонии</p>
<b>Самостоятельная работа</b>	<p><b>Самостоятельная работа обучающихся</b></p> <p>Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите</p> <p><b>Тематика домашних заданий</b></p> <ol style="list-style-type: none"> <li>1. Составление доклада о Стандарте шифрования ГОСТ 28147-89</li> <li>2. Подготовка реферата по теме «Абсолютный шифр».</li> <li>3. Схема «Простая замена».</li> <li>4. Схема «Простая замена с ключом».</li> <li>5. Схема «Система Цезаря с ключом».</li> <li>6. Схема «Символьное кодирование».</li> <li>7. Подготовка реферата по теме «Основные процедуры цифровой подписи».</li> <li>8. Подготовка реферата по теме «Комбинированная криптосистема».</li> <li>9. Схема симметричное шифрование.</li> <li>10. Выполнение реферата по теме «Криптология».</li> <li>11. Подготовка презентаций по теме «Криптоанализ».</li> <li>12. Оформление в виде конспекта основных положений криптографии.</li> <li>13. Разработка схемы Механизма арбитраж.</li> <li>14. Изучение структуры Симметричной системы шифрования.</li> </ol>



	<ol style="list-style-type: none"> <li>15. Составление схемы сервера приложений.</li> <li>16. Оформление в виде конспекта основных положений процесса генерации ключей.</li> <li>17. Подготовка схемы Абонентское шифрование.</li> <li>18. Разработка схемы Пакетное шифрование.</li> <li>19. Разработка схемы Аутентификация данных</li> <li>20. Оформление в виде конспекта основных положений представления алфавита в двоичном коде .</li> <li>21. Подготовка схемы функционирования электронных платежных систем.</li> <li>22. Оформление в виде конспекта основ кодирования.</li> <li>23. Разработка схемы Однонаправленных хеш-функций.</li> <li>24. Разработка схемы шифрования с открытым ключом.</li> <li>25. Оформление в виде конспекта материала по Шифрованию методами замены.</li> <li>26. Оформление в виде конспекта материала об Абонентском шифровании.</li> <li>27. Разработка схемы Матричной перестановки.</li> <li>28. Оформление в виде конспекта материала о криптоанализе.</li> <li>29. Подготовка к практическому занятию «Кодирование».</li> <li>30. Разработка схемы Частотного анализа.</li> <li>31. Разработка схемы криптоанализа.</li> <li>32. Построение ГТС, состав оборудования ЦСК, классификация систем сигнализации, модели транспортных сетей SDH, ATM, OTN, алгоритмы кодирования кодеков.</li> <li>33. Основы VoIP. Передача речи по IP-сетям. История технологии VoIP. Достоинства технологии VoIP. Проблемы, возникающие при использовании среды IP для передачи речи. Методы уменьшения объёмов передаваемого трафика. Кодирование информации.</li> </ol>
--	--

	<p>Протоколы RTP/RTCP.</p> <p>34. Сети и сценарии IP-телефонии Основные сценарии IP-телефонии. Базовые архитектуры построения сетей IP- телефонии. Основные услуги, реализуемые с использованием технологии VoIP.</p> <p>35. Сеть IP-телефонии согласно рекомендации H.323 Архитектура сети H.323 и назначение её элементов. Конференции в H.323. Структура стека протоколов H.323. Протоколы RAS, H.225 и H.245. Базовые сценарии установления соединения в сети, построенной согласно H.323.</p>
<p align="center"><b>ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации</b></p>	
<p><b><i>Иметь практический опыт:</i></b></p>	<p><b><i>Виды работ на практике:</i></b></p>
<p>– обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;</p>	<p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: работа над ошибками</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: удаленное администрирование сервера с рабочих станций</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: программы удаленного доступа</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: планирования восстановления работоспособности</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: определение точек восстановления</p> <p>Обслуживание сетевой инфраструктуры, восстановление работоспособности сети после сбоя: мониторинг сети после восстановления</p>
<p><b><i>Уметь:</i></b></p>	<p><b><i>Тематика лабораторных/практических работ:</i></b></p>
<p>– правильно оформлять техническую документацию;</p>	<p>– Запись данных средствами сетевого монитора.</p> <p>– Устранение неполадок с помощью Ping и PathPing.</p> <p>– Диагностика сети и Netdiag</p> <p>– Удалённое администрирование</p> <p>– Восстановление работоспособности</p>

	<p>сетевой инфраструктуры.</p> <ul style="list-style-type: none"> <li>– Авторизация подключений удалённого доступа</li> <li>– Использование консоли. Производительность.</li> <li>– Мониторинг сетевого трафика с помощью утилиты Netstat</li> </ul>
<b>Знать:</b>	<b>Перечень тем, включенных в МДК:</b>
<ul style="list-style-type: none"> <li>– методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;</li> <li>– основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем (ИС), требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;</li> </ul>	<p><b>Тема 1.2. Управление сетями</b></p>
<b>Самостоятельная работа</b>	<p><b>Самостоятельная работа обучающихся</b> Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите</p> <p><b>Примерная тематика внеаудиторной работы</b></p> <ol style="list-style-type: none"> <li>1. Устройство пакета, передаваемого по сети.</li> <li>2. Использование бесклассовой междоменной маршрутизации.</li> <li>3. Маски подсети переменной длины.</li> <li>4. Проверка существующего IP-адреса, ручная настройка адреса.</li> <li>5. DNS, NetBIOS. DNS в сетях Windows Server</li> <li>6. Механизм работы DNS-запросов.</li> </ol>
<p><b>ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования</b></p>	

<b><i>Иметь практический опыт:</i></b>	<b><i>Виды работ на практике:</i></b>
<p>– организации бесперебойной работы системы по резервному копированию и восстановлению информации;</p>	<p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: установка межсетевого экрана на предприятии</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: установка на рабочие станции антивирусных программ на предприятии</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: установка и настройка ОС на предприятии</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: тестирование сетевого оборудования на предприятии</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: устранение неполадок сети на предприятии</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: ремонт сетевого оборудования</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: использование активного сетевого оборудования</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: использование пассивного сетевого оборудования</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: заполнение технической документации</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: Работа по созданию, редактированию, удалению пользователей в DOMAIN</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: построение физической карты локальной сети</p> <p>Организация бесперебойной работы</p>

	<p>системы по резервному копированию и восстановлению информации: мониторинг сети с помощью специализированного ПО</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: анализ работы сети с помощью программных и аппаратных средств</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: контроль доступа</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: сохранение целостности данных</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: журналирование</p> <p>Организация бесперебойной работы системы по резервному копированию и восстановлению информации: работа со встроенными сканерами диагностики и управления</p>
<b>Уметь:</b>	<b>Тематика лабораторных/практических работ:</b>
<ul style="list-style-type: none"> <li>– осуществлять диагностику и поиск неисправностей технических средств;</li> <li>– выполнять действия по устранению неисправностей в части, касающейся полномочий техника;</li> </ul>	<ul style="list-style-type: none"> <li>– Тестирование кабелей.</li> <li>– Тестирование коммутационного оборудования</li> <li>– Операции по резервному копированию данных.</li> <li>– Операции по восстановлению данных</li> <li>– Организация бесперебойной работы системы резервного копирования.</li> <li>– Восстановление информации</li> <li>– Восстановление работоспособности сети после сбоя.</li> </ul>
<b>Знать:</b>	<b>Перечень тем, включенных в МДК:</b>
<ul style="list-style-type: none"> <li>– правила эксплуатации технических средств сетевой инфраструктуры;</li> </ul>	<b>Тема 1.2. Управление сетями</b>
<b>Самостоятельная работа</b>	<p><b>Самостоятельная работа обучающихся</b></p> <p>Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите</p> <p><b>Примерная тематика внеаудиторной работы</b></p> <p>7. Основные сведения о политиках</p>

	<p>удалённого доступа.</p> <p>8. Устранение неполадок при подключениях удалённого доступа.</p> <p>9. Реализация процедур безопасного администрирования сети.</p> <p>10. Оснастка</p> <p>11. Шаблоны безопасности.</p> <p>12. Схемы обжимки витой пары.</p>
<p><b>ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.</b></p>	
<b><i>Иметь практический опыт:</i></b>	<b><i>Виды работ на практике:</i></b>
<p>– удаленного администрирования и восстановления работоспособности сетевой инфраструктуры</p>	<p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: защита информации в СКС</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: программная защита информации. Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: анализ входящего трафика</p> <p>Удаленное администрирование и восстановление работоспособности сетевой инфраструктуры: анализ исходящего трафика</p>
<b><i>Уметь:</i></b>	<b><i>Тематика лабораторных/практических работ:</i></b>
<p>– выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;</p>	<p>– Разработка плана восстановления</p> <p>– Использование схемы послеаварийного восстановления сети.</p> <p>– Возврат к нормальному функционированию системы</p>
<b><i>Знать:</i></b>	<b><i>Перечень тем, включенных в МДК:</i></b>
<p>– основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем</p>	<p><b>Тема 1.2. Управление сетями</b></p>
<b><i>Самостоятельная работа</i></b>	<p><b>Самостоятельная работа обучающихся</b></p> <p>Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите</p> <p><b>Примерная тематика внеаудиторной работы</b></p> <p>1. Настройка параметров DNS-сервера. Средства устранения неполадок DNS</p>

	<ol style="list-style-type: none"><li>2. Изучение утилиты Acronis, изучение безопасной зоны Acronis.</li><li>3. Создание контрольной точки восстановления с помощью Acronis.</li><li>4. Создание базы данных на примере учебной группы.</li><li>5. Разработка плана восстановления работоспособности сети на примере одной взятой организации (колледжа, офиса)</li></ol>
--	---

**Информационные ресурсы, используемые при выполнении самостоятельной работы**

\*рекомендуется пользоваться Интернет-ресурсами при самостоятельной работе по всем разделам дисциплины

**Раздел 1. Эксплуатация объектов сетевой инфраструктуры**

	Рекомендуемые учебные издания
Занятие № 1	[9] с. 17-19, 55-56
Занятие № 2	[10] с. 115-116
Занятие № 3	[2] с. 127-129
Занятие № 4	[10] с. 368-371
Занятие № 5	[9] с. 17-19, 55-56; [10] с. 115-116
Занятие № 6	[3] с. 313-314; [4] с. 23-24
Занятие № 7	[8] с. 176-182
Занятие № 8	[8] с. 176-177
Занятие № 9	[8] с. 177-178
Занятие № 10	[8] с. 178-179
Занятие № 11	[8] с. 179-180
Занятие № 12	[8] с. 180-181
Занятие № 13	[8] с. 181-182
Занятие № 14	[10] с. 368-369
Занятие № 15	[10] с. 370-371
Занятие № 16	[12] с. 36-59
Занятие № 17	[12] с. 36-59
Занятие № 18	[2] с. 91-98
Занятие № 19	[3] с. 87-92
Занятие № 20	[8] с. 262-265
Занятие № 21	[5] с. 395-401
Занятие № 22	[8] с. 265-272
Занятие № 23	[12] с. 125-126
Занятие № 24	[5] с. 395-401
Занятие № 25	[5] с. 395-401
Занятие № 26	[8] с. 176-182
Занятие № 27	[8] с. 176-182
Занятие № 28	[8] с. 176-182
Занятие № 29	[8] с. 176-182
Занятие № 30	[10] с. 305-325
Занятие № 31	[10] с. 305-325
Занятие № 32	[10] с. 305-325
Занятие № 33	[10] с. 305-325
Занятие № 34	[3] с. 353-354; [5] с. 39-40, 416-419
Занятие № 35	[9] с. 353-354
Занятие № 36	[10] с. 345-347
Занятие № 37	[12] с. 201-202
Занятие № 38	[3] с. 329-330
Занятие № 39	[3] с. 330-331
Занятие № 40	[3] с. 332-333
Занятие № 41	[9] с. 329-333
Занятие № 42	[6] с. 411-415



Занятие № 43	[6] с. 416-421
Занятие № 44	[2] с. 280-281
Занятие № 45	[2] с. 281-282
Занятие № 46	[4] с. 167-169
Занятие № 47	[4] с. 170-171
Занятие № 48	[8] с. 20-21
Занятие № 49	[8] с. 21-22
Занятие № 50	[8] с. 23-24
Занятие № 51	[8] с. 24-26
Занятие № 52	[8] с. 26-28
Занятие № 53	[8] с. 29-32
Занятие № 54	[3] с. 329-333
Занятие № 55	[3] с. 329-333
Занятие № 56	[3] с. 329-333
Занятие № 57	[2] с. 140-141
Занятие № 58	[2] с. 141-142
Занятие № 59	[3] с. 159-160
Занятие № 60	[3] с. 160-164
Занятие № 61	[9] с. 159-160
Занятие № 62	[9] с. 160-162
Занятие № 63	[9] с. 162-164
Занятие № 64	[2] с. 280-282
Занятие № 65	[2] с. 280-282
Занятие № 66	[2] с. 280-282
Занятие № 67	[3] с. 164-169
Занятие № 68	[3] с. 170-175
Занятие № 69	[3] с. 176-180
Занятие № 70	[3] с. 181-185

### **МДК.03.02. Безопасность функционирования информационных систем**

	Рекомендуемые учебные издания
Занятие № 1	[14], с.6-19; [18], с.5-64
Занятие № 2	[14], с. 34-37, 44-48; [21], с. 21-35, 53-56
Занятие № 3	[14], с.15-22, 30-31
Занятие № 4	[14], с.12-13, 31-33; [15], с.334-344
Занятие № 5	[21], с. 21-35
Занятие № 6	[19], с.10-29
Занятие № 7	[14], с.15-19
Занятие № 8	[14], с.15-19
Занятие № 9	[17], с. 13-22, 94-102
Занятие № 10	[14], с.26-30[20], с. 76-97
Занятие № 11	[14], с.15-19
Занятие № 12	[17], с.11-13, 51-64; [16], с. 116-156
Занятие № 13	[20], с. 61-75
Занятие № 14	[20], с. 9-25; [14], с. 44-48; [16], с.244-249, 334-350
Занятие № 15	[17], с.66-78
Занятие № 16	[16], с.244-249
Занятие № 17	[16], с. 94-109
Занятие № 18	[20], с. 61-73; [21], с. 62-86

Занятие № 19	[19], с. 365-403
Занятие № 20	[20], с. 334-343
Занятие № 21	[20], с. 344-353
Занятие № 22	[20], с. 121-141; [21], с. 86-94
Занятие № 23	[20], с. 353-357
Занятие № 24	[20], с. 367-377; [21], с. 492-510
Занятие № 25	[21], с. 86-90
Занятие № 26	[21], с. 86-90
Занятие № 27	[21], с.527-530
Занятие № 28	[21], с.527-530
Занятие № 29	[21], с. 94-110
Занятие № 30	[21], с. 111-123
Занятие № 31	[21], с. 111-123
Занятие № 32	[15], с. 257-275
Занятие № 33	[15], с. 257-275
Занятие № 34	[18], с. 96-158, [20], с. 97-121
Занятие № 35	[20], с. 142-170
Занятие № 36	[20], с. 333-353
Занятие № 37	[21], с. 250-270
Занятие № 38	[21], с. 271-288
Занятие № 39	[21], с. 492-507
Занятие № 40	[21], с. 441-479
Занятие № 41	[21], с. 407-440
Занятие № 42	[15], с. 122-246
Занятие № 43	[15], с.512-534
Занятие № 44	[16], с. 253-278
Занятие № 45	[20], с. 142-170
Занятие № 46	[20], с.217-238
Занятие № 47	[20], с. 179-192
Занятие № 48	[15], с. 248-277

### **МДК.03.03. Эксплуатация систем IP-телефонии.**

<b>№ п.п.</b>	<b>Рекомендуемые учебные издания</b>
Занятие № 1	[22], с.39-48, 53-65
Занятие № 2	[25], с.69-78
Занятие № 3	[25], с.26-37
Занятие № 4	[22], с.12-16, [23], с.69-78
Занятие № 5	[22], с.52-59, [23], с.81-92
Занятие № 6	[22], с.59-61, [25], с.341-345
Занятие № 7	[22], с.94-107, [23], с.287-291, [25], с.346-353
Занятие № 8	[24], с.25-35
Занятие № 9	[25], с.323-332
Занятие № 10	[22], с.140-148
Занятие № 11	[22], с.112-129
Занятие № 12	[22], с.112-129
Занятие № 13	[16], с.86-88, [24],с.44-46
Занятие № 14	[16], с.283-286
Занятие № 15	[22], с.61-78, [23], с.153-191
Занятие № 16	[24], с.59-75

Занятие № 17	[22], с.80-85, [23], с.193-220
Занятие № 18	[24], с.47-52
Занятие № 19	[22], с.90-92, [23], с.229-27
Занятие № 20	[25], с.303-308, [24], с.163-196
Занятие № 21	[6], с. 60-89
Занятие № 22	[6], с. 40-60
Занятие № 23	[24], с.312-314
Занятие № 24	[23], с.17-20
Занятие № 25	[23], с.21-27
Занятие № 26	[23], с.10-15
Занятие № 27	[23], с.23-40
Занятие № 28	[24], с.40-59
Занятие № 29	[24], с.60-63
Занятие № 30	[24], с.64-75
Занятие № 31	[16], с.229-230
Занятие № 32	[16], с.231-243
Занятие № 33	[16], с.244-251
Занятие № 34	[16], с.251-256
Занятие № 35	[16], с.257-271
Занятие № 36	[16], с.271-290
Занятие № 37	[24], с.412-417
Занятие № 38	[24], с.785-787
Занятие № 39	[24], с.787-789
Занятие № 40	[6], с.145-159
Занятие № 41	[17], с.331-335
Занятие № 42	[17], с.247-263
Занятие № 43	[16], с.35-45
Занятие № 44	[16], с.307-315
Занятие № 45	[6], с.12-136
Занятие № 46	[6], с.161-180
Занятие № 47	[6], с.181-260
Занятие № 48	[6], с.140-159