ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт – Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»
Санкт-Петербургский колледж телекоммуникаций

УТВЕРЖДАЮ
ПЕРВЫЙ ПРОРЕКТОР-
ПРОРЕКТОР ПО УЧЕБНОЙ РАБОТЕ

_____ Г.М. МАШКОВ
“_ ” ____ _____ 2017 г.
Регистрационный номер № _____/ _____

РАБОЧАЯ ПРОГРАММА

ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

(наименование модуля)

программа подготовки специалистов среднего звена

09.02.02 Компьютерные сети
(код и наименование специальности)

квалификация Техник по компьютерным сетям

Санкт- Петербург
2017

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» 27 апреля 2017г., протокол №4.

Составитель:
Преподаватель высшей категории _____ Н.В.Кривоносова
(подпись)

СОГЛАСОВАНО
Главный специалист НТБ УИОР _____ Р.Х. Ахтреева
(подпись)

ОБСУЖДЕНО
на заседании цикловой комиссии № 4 (компьютерных сетей и программно-аппаратных средств)

15 марта 2017 г., протокол № 7
Председатель цикловой (предметной) комиссии:
_____ К.В. Лебедева
(подпись)

ОДОБРЕНО
Методическим советом Санкт-Петербургского колледжа телекоммуникации
«29» марта 2017 г. Протокол № 4

И.о.зам. директора по УР колледжа СПб ГУТ
_____ О.В. Колбанёва
(подпись)

СОГЛАСОВАНО
И.о.директора колледжа СПб ГУТ
_____ Т.Н. Сиротская
(подпись)

СОГЛАСОВАНО
Начальник учебно-методического управления
_____В.И. Аверченков
(подпись)

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. Эксплуатация объектов сетевой инфраструктуры

1.1. Область применения программы

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

1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей;
2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях;
3. Эксплуатировать сетевые конфигурации;
4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации;
5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования;
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 ОПОП СПО по специальности 09.02.02 «Компьютерные сети» с квалификацией «Техник».

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

С целью овладения указанным видом профессиональной 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. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – 750 часов, в том числе:
максимальной учебной нагрузки обучающегося – 584 часа, включая:
обязательной аудиторной учебной нагрузки обучающегося – 498 часов,
в том числе:
самостоятельной работы обучающегося – 166 часов;
учебной и производственной практики – 108 и 144 часа.

Наименование разделов профессионального модуля (междисциплинарных курсов):
МДК.03.01. Эксплуатация объектов сетевой инфраструктуры;
МДК.03.02. Безопасность функционирования информационных систем;
МДК.03.03. Эксплуатация систем IP-телефонии.

Виды промежуточной аттестации:
- дифференциальный зачет по междисциплинарному курсу;
- экзамен квалификационный по профессиональному модулю.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности *Сопровождение, настройка и администрирование системного и сетевого программного обеспечения, эксплуатация и обслуживание серверного и сетевого оборудования, диагностика и мониторинг работоспособности программно-технических средств, обеспечение целостности резервирования информации и информационной безопасности объектов сетевой инфраструктуры*, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
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.
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), 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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

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	246	210	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	144	48	-	48	-		-
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	144	48		48		36	-
	Производственная практика (по профилю специальности), часов	144							144
	Всего:	**750**	**498**	**166**	**-**	**166**		**108**	**144**

3.2. Тематический план и содержание профессионального модуля
«Программное обеспечение компьютерных сетей»

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 и обслуживание технических и программно-аппаратных средств компьютерных сетей	**Содержание**		70	
	1.	**Физические аспекты эксплуатации.** Физическое вмешательство в инфраструктуру сети; активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.		*2*
	2.	**Логические (информационные) аспекты эксплуатации.** Несанкционированное ПО (в том числе сетевое); паразитная нагрузка.		*2*
	3.	**Расширяемость сети. Масштабируемость сети.** Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб); наращивание длины сегментов сети; замена существующей аппаратуры (на более мощную). Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.		*2*
	4.	**Техническая и проектная документация.** Паспорт технических устройств; руководство по эксплуатации; Физическая карта всей сети; логическая схема компьютерной сети;		*2*
	5.	**Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры** Комплекс организационно-технических мероприятий; выявление и своевременная замена элементов инфраструктуры.		*2*
	6.	**Проверка объектов сетевой инфраструктуры и профилактические работы** Проверка физических компонентов; проверка документации и требований; проверка списка совместимого оборудования.		*2*
	7.	**Проведение регулярного резервирования** Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения.		*2*

8.	**Анализаторы протоколов** Программные или аппаратно-программные системы, функции мониторинга, анализ трафика в сетях.	*2*
9.	**Оборудование для диагностики и сертификации кабельных систем** Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	*2*
10.	**Экспертные системы** Выявление причин аномальной работы сетей; возможные способы приведения сети в работоспособное состояние.	*2*
11	**Встроенные системы диагностики и управления. Сетевые мониторы** Средняя интенсивность общего трафика сети, средняя интенсивность потока пакетов с определенным типом ошибки. Программно-аппаратный модуль, установленный в коммуникационное оборудование, программный модуль, встроенный в операционные системы.	*2*
12	**Резервное копирование данных**	*2*
13	**Хранилищ данных** Принципы работы хранилищ данных. Принципы построения. Основные компоненты хранилища данных	*2*
14	**Технологии управления информацией. OLAP-технология**	*2*
15	**Понятие баз данных.** Основные понятия, принцип работы. СУБД	*2*
16	Принципы планирования восстановления работоспособности сети при аварийной ситуации	*2*
17	Допущения при разработке схемы послеаварийного восстановления. Основные требования к политике организации схемы послеаварийного восстановления	*2*
18	Организация работ по восстановлению функционирования системы	*2*
19	**План восстановления системы** Порядок уведомления о чрезвычайных событиях. Активация. Возврат к нормальному функционированию системы.	*2*
20	Принципы локализации неисправностей	*2*
21	Контрольно-измерительная аппаратура	*2*
22	Сервисные платы и комплексы	*2*
23	Программные средства диагностики	*2*
24	Номенклатура и особенности работы тест-программ	*2*

25	Диагностика неисправностей средств сетевых коммуникаций		*2*
26	Контроль функционирования аппаратно-программных комплексов.		*2*
27	Действия при не работающей сети, при медленной сети,		*2*
28	Действия при не стабильно работающей сети.		*2*
29	**Архитектура системы управления. Структура системы управления.** Архитектура в концепции TMN; централизованное управление; децентрализованное управление.		*2*
30	**Уровни управления** Многоуровневая архитектура управления TMN: бизнесом; услугами; сетью; элементами сети; уровень элементов сети.		*2*
31	**Области управления.** Области управления ошибками; конфигурацией; доступом; производительностью; безопасностью.		*2*
32	**Протоколы управления.** SNMP; CMIP; TMN; LNMP; ANMP.		*2*
33	**Управление отказами.** Выявление, определение и устранение последствий сбоев и отказов в работе сети.		*2*
34	**Учет работы сети. Управление конфигурацией.** Регистрация, управление используемыми ресурсами и устройствами; конфигурирование компонентов сети, сетевые адреса и идентификаторы, управление параметрами сетевых операционных систем.		*2*
35	**Управление производительностью, безопасностью сети.** Статистика работы сети в реальном времени, минимизации заторов и узких мест, выявления складывающихся тенденций и планирования ресурсов для будущих нужд; Контроль доступа, сохранение целостности данных и журналирование.		*2*
Лабораторные работы		70	
1.	Поддержка пользователей сети.		
2.	Создание пользователей в domain, редактирование пользователей в domain, создание пароля пользователем в domain, создание групп и распределение пользователей по группам в domain.		
3.	Настройка прав доступа.		
4.	Оформление технической документации, правила оформления документов.		
5.	Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в		

	domain.		
6.	Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.		
7.	Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы, коммутационное оборудование)		
8.	Вкладка. Сеть утилиты. Диспетчер задач		
9.	Использование консоли. Производительность		
10	Мониторинг сетевого трафика с помощью утилиты Netstat		
11	Тестирование кабелей		
12	Тестирование коммутационного оборудования		
13	Операции по резервному копированию данных;		
14	Операции по восстановлению данных.		
15	Организации по бесперебойной работе системы по резервному копированию		
16	Восстановление информации		
17	Восстановление работоспособности сети после сбоя		
18	Разработка плана восстановления		
19	Использовать схему после аварийного восстановления сети.		
20	Возврат к нормальному функционированию системы.		
21	Работа контрольно-измерительной аппаратуры		
22	Замена расходных материалов		
23	Мелкий ремонт периферийного оборудования		
24	Программная диагностика неисправностей		
25	Аппаратная диагностика неисправностей		
26	Поиск неисправностей технических средств		
27	Выполнение действий по устранению неисправностей		
28	Установка программного обеспечения		
29	Анализ сетевого трафика средствами Сетевого монитора		
30	Основные сведения о сетевом мониторе		
31	Запись данных средствами Сетевого монитора		
32	Устранение неполадок с помощью Ping и PathPing		
33	Диагностика сети и Netdiag		
34	Удаленное администрирование;		
35	Восстановление работоспособности сетевой инфраструктуры. Авторизация		

		подключений удаленного доступа		
Самостоятельная работа при изучении раздела ПМ 1.				
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. **Примерная тематика домашних заданий** Физическая инфраструктура; Логическая инфраструктура; Сетевые подключения, протоколы, адресация, система имен. Автоматическое назначение частных IP-адресов; Маршрутизация и инфраструктура сети Windows Server 2003; Установка сетевых компонентов Windows; Установка Active Directory в сети Windows; Разбиение на подсети; Механизм разбиения на подсети; Определение емкости подсети; Технические регламенты, виды документов для технических осмотров, методы и принципы проверки различного оборудования, методы резервирования, программы для резервирования информации, BackUp. Маршрутизация в Windows Server 2003; Управление общими свойствами IP-маршрутизации; Основные сведения о NAT; Различие между NAT и ICS; Удаленный доступ по телефонной линии; Авторизация подключений удаленного доступа Основные сведения о политиках удаленного доступа Устранение неполадок при подключениях удаленного доступа Реализация процедур безопасного администрирования сети Оснастка Шаблоны безопасности Схемы обжимки витой пары; Устройство «пакета», передаваемого по сети. Использование бесклассовой междоменной маршрутизации; Маски подсети переменной длины; Проверка существующего IP-адреса; Ручная настройка адреса; DNS; NetBIOS; DNS в сетях Windows Server 2003; Механизм работы DNS-запросов; Настройка параметров DNS-сервера;			70	

Средства устранения неполадок DNS; Изучение утилиты Acronis, изучение безопасной зоны Acronis,				
Учебная практика УП.ПМ.03.01	**Содержание**		**36**	
	1.	Настройка прав доступа.		
	2.	Оформление технической документации, правила оформления документов.		
	3.	Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.		
	4.	Программная диагностика неисправностей		
	5.	Программная диагностика неисправностей		
	6.	Программная диагностика неисправностей		
	7.	Аппаратная диагностика неисправностей		
	8.	Аппаратная диагностика неисправностей		
	9.	Аппаратная диагностика неисправностей		
	10.	Поиск неисправностей технических средств		
	11.	Поиск неисправностей технических средств		
	12.	Поиск неисправностей технических средств		
	13.	Выполнение действий по устранению неисправностей		
	14.	Выполнение действий по устранению неисправностей		

	15.	Выполнение действий по устранению неисправностей		
	16.	Изучение утилиты Acronis		
	17.	Изучение утилиты Acronis		
	18.	Изучение утилиты Acronis		
Раздел 2. Безопасность функционирования информационных систем			**180**	
МДК 03.02. Безопасность функционирования информационных систем			**144**	
Тема 2.1 Основы информационной безопасности	**Содержание**		16	
	1	**Понятие национальной безопасности.** Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.		*2*
	2	**Информационная безопасность в системе национальной безопасности Российской Федерации.** Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере.		*2*
	3	**Государственная информационная политика.** Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.		*2*
	4	**Информация - наиболее ценный ресурс современного общества.** Понятие «информационный ресурс». Классы информационных ресурсов.		*2*
	5	**Проблемы информационной войны.** Информационное оружие и его классификация. Информационная война.		*2*
	6	**Проблемы информационной безопасности в сфере государственного и муниципального управления.** Информационные процессы в сфере государственного и муниципального управления. Виды информации и информационных ресурсов в сфере ГМУ. Состояние и перспективы информатизации сферы ГМУ.		*2*
	7	**Информационные системы.** Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах.		*2*
	8	**Методы и модели оценки уязвимости информации.** Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита»		*2*
	Лабораторные работы		12	

	1	Установка программы Ethereal и подготовка к захвату.		
	2	Пользовательский интерфейс программы Ethereal. Фильтр отображения пакетов. Поиск кадров.		
	3	Выделение ключевых кадров. Сохранение данных захвата. Печать информации. Просмотр кадра в отдельном окне.		
	4	Анализ протоколов Ethernet и ARP.		
	5	Анализ протоколов IP и ICMP.		
	6	Анализ протокола TCP		
Тема 2.2. Проблемы информационной безопасности	**Содержание**		8	*2*
	1	**Основные понятия и анализ угроз информационной безопасности.** Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.		*2*
	2	**Проблемы информационной безопасности сетей.** Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей.		*2*
	3	**Политика безопасности.** Основные понятия политики безопасности. Структура политики безопасности организации.		*2*
	4	**Стандарты информационной безопасности.** Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий		*2*
	Лабораторные работы		10	
	1	Система анализа рисков проверки политики информационной безопасности предприятия.		
	2	Анализ угроз сетевой безопасности.		
	3	Этапы сетевой атаки. Исследование сетевой топологии.		
	4	Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы		
	5	Реализации атак. Выявление атаки на протокол SMB.		
Тема 2.3. Технологии защиты данных	**Содержание**		6	
	1	**Принципы криптографической защиты информации.** Основные понятия криптографической защиты информации. Симметричные		*2*

		криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования. Электронная цифровая подпись и функция хэширования.		
	2	**Криптографические алгоритмы.** Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы.		*2*
	3	**Технологии аутентификации.** Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.		*2*
	Лабораторные работы		4	
	1	Изучение стандарта криптографической защиты AES (Advanced Encryption Standart).		
	2	Изучение отечественных стандартов хэш-функции и цифровой подписи.		
Тема 2.4. Технологии защиты межсетевого обмена данными	**Содержание**		18	
	1	**Обеспечение безопасности операционных систем.** Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС.		*2*
	2	**Технологии межсетевых экранов.** Функции межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ.		*2*
	3	**Основы технологии виртуальных защищенных сетей VPN.** Концепция построения виртуальных защищенных сетей VPN. VPN-решения для построения защищенных сетей. Достоинства применения технологий VPN.		*2*
	4	**Защита на канальном и сеансовом уровнях.** Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне. Защита беспроводных сетей.		*2*
	5	**Защита на сетевом уровне - протокол IPSEC.** Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол управления криптоключами IKE. Особенности реализации средств IPSec.		*2*
	6	**Инфраструктура защиты на прикладном уровне.** Управление идентификацией и доступом. Организация защищенного удаленного доступа. Управление доступом по схеме однократного входа с авторизацией Single		*2*

		Sign-On. Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.	22	
	7	**Анализ защищенности и обнаружение атак.** Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак.		*2*
	8	**Защита от вирусов. Методы управления средствами сетевой безопасности.** Компьютерные вирусы и проблемы антивирусной защиты. Антивирусные программы и комплексы.		*2*
	9	Построение системы антивирусной защиты корпоративной сети. Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности.		*2*
	Лабораторные работы			
	1	Компоненты межсетевого экрана. Политика межсетевого экранирования		
	2	Архитектура МЭ. Пример реализации политики МЭ.		
	3	Применение МЭ на основе двудомного узла. Применение МЭ на основе фильтрующего маршрутизатора. Применение МЭ на основе экранирующего узла		
	4	Применение технологии трансляции сетевых адресов.		
	5	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.		
	6	Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне		
	7	Организация VPN средствами СЗИ VipNet. Использование протокола IPSec для защиты сетей. Защита на транспортном уровне		
	8	Организация VPN средствами протокола SSL в Windows Server		
	9	Сигнатурный анализ и обнаружение аномалий		
	10	Обнаружение в реальном времени и отложенный анализ. Локальные и сетевые системы обнаружения атак		
	11	Распределенные системы обнаружения атак. Система обнаружения атак Snort.		

Самостоятельная работа при изучении раздела ПМ 2. 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 **Примерная тематика домашних заданий** 1. Оформление в виде конспекта основных руководящих документов об автоматизированных системах. 2. Разработка схемы классификации автоматизированных систем. 3. Изучение концепции автоматизированной системы. 4. Составление схемы подсистема защиты от несанкционированного доступа. 5. Оформление в виде конспекта основных признаков несанкционированного доступа к информации. 6. Разработка схемы Парольной аутентификации. 7. Оформление в виде конспекта основных положений общеметодологических принципов формирования теории защиты. 8. Составление перечня задач теории защиты. 9. Принципы построения защиты в сетях 10. Оформление в виде конспекта вопросов, касающихся понятия стратегии защиты информации и особенностей стратегических решений. 9. Подготовка перечня требований к сервисам безопасности. 11. Составление схемы основных составляющих политики безопасности. 12. Оформление в виде конспекта основных положений Механизма аутентификации. 13. Разработка структуры процессов технологии управления подсистемой защиты ОС. 10. Понятие системного анализа: микроскопическое представление системы, иерархическое представление системы. 14. Разработка классификации моделей защиты. 15. Оформление в виде конспекта основных требований к Средствам и методам выявления компьютерных вирусов. 16. Подготовка архитектурной модели Управления доступом. 17. Оформление в виде конспекта основных положений Аутентификации в доменах Windows. 18. Составление перечня стадий Сетевых атак. 19. Определение типовой модели системы автоматизированного проектирования защиты информации. 20. Разработка модели защиты информации. 21. Оформление в виде конспекта основных положений аппаратных средств защиты информации. 22. Оформление в виде конспекта основных видов контроля безопасности. 23. Подготовка плана Аудита. Оформление в виде конспекта основных положений математической защиты информации. 24. Составление перечня методов кодирования информации. 25. Разработка алгоритма хеширования. 26. Подготовка перечня антивирусных программ. 27. Оформление в виде конспекта основных положений инженерно-технической защиты информации.	48	

28. Разработка схемы защиты операционной системы. 29. Оформление в виде конспекта основных видов потенциально опасных программ **Тематика домашних заданий** 1. Составление доклада о критериях защиты информации. 2. Подготовка реферата по теме «Линейная структура защиты информации». 3. Схема «Классы защиты автоматизированных систем». 4. Схема «Нормативно-правовое регулирование защиты информации». 5. Подготовка презентаций по теме «Несанкционированный доступ к информации». 6. Подготовка доклада «Модель защиты Кларка-Вилсона». 7. Схема «Источник несанкционированного доступа к информации». 8. Составление доклада «Модель защиты Балла-Ла Падулы». 9. Подготовка презентаций «Защита операционной системы Windows».			
Учебная практика **УП.ПМ.03.02**	1.	Использование активного оборудования сети.	36
	2.	Использование пассивного оборудования сети.	
	3.	Устранение паразитирующей нагрузки в сети.	
	4.	Заполнение технической документации.	
	5.	Построение физической карты локальной сети.	
	6.	Работа по созданию, редактированию, удалению пользователей в DOMAIN.	
	7.	Регламенты технических осмотров.	
	8.	Профилактические работы в объектах сетевой инфраструктуры.	
	9.	Мониторинг и анализ сети с помощью программных и аппаратных средств	
	10.	Структура системы управления, архитектура системы управления.	
	11.	Управление областями сети: ошибками, конфигурацией, доступом, производительностью, безопасностью.	
	12.	Работа с протоколами SNMP; CMIP; TMN; LNMP; ANMP.	
	13.	Отслеживание работы сети.	
	14.	Работа с сервером, чтение голов, работа над ошибками	
	15.	Работа с сервером.	
	16.	Удаленное администрирование рабочих станций с сервера	
	17.	Контроль доступа, сохранение целостности данных и журналирование.	
	18.	Удаленное администрирование сервера с рабочих станций, программы для удаленного доступа.	
Раздел 3. Эксплуатация систем IP-телефонии			**180**
МДК.03.03. Эксплуатация систем IP-телефонии			**144**

Тема 3.1. Организация, принципы построения и функционирования сетей IP-телефонии	**Содержание**		22	
	1	**Организация телефонной сети общего пользования** TDM-телефония, основные понятия. Формирование сетей ТФОП. Состав оборудования ТФОП. Включение абонентских и соединительных линий в ЦСК. Виды доступов.		*2*
	2	Сигнализация в телефонных сетях. Абонентская, внутристанционная и межстанционная сигнализации.		*2*
	3	Технологии мультиплексирования. Общие принципы построения транспортных сетей на базе PDH, SHD и WDM.		*2*
	4	**Передача речи по IP-сети**. Причины появления IP-телефонии. Особенности IP-телефонии. Принципы пакетной передачи. Виды соединений, взаимодействие с компьютерной сетью. Особенности передачи речевой информации по IP-сетям. Взаимодействие протоколов VoIP.		*2*
	5	**Принципы кодирования речи** Цифровые процессы обработки сигналов для речевых кодеков, основные алгоритмы кодирования речи, используемые в IP-телефонии. Кодеки, стандартизированные ITU-T: G.711, G.723.1, G.726, G.728, G.729. Алгоритмы кодирования ETSI, передача сигналов DTMF		*2*
	6	**Качество передачи речевой информации по IP-сети** Задержка и меры по уменьшению ее влияния. Явление джиттера, меры уменьшения его влияния. Эхо, устройства ограничения его влияния.		*2*
	7	**Внедрение и улучшение качества обслуживания в сетях VoIP** Механизмы обеспечения качества обслуживания в IP сетях. Механизмы QoS. Классификация трафика. Границы доверия. Управление перегрузками. Формирование трафика (Traffic Shaping). Сжатие. Фрагментация и перемешивание данных		*2*
	8	**Построение сетей IP-телефонии** Классификация сетей IP-телефонии: по способу связи оконечных устройств, по масштабу. Сети на основе Softswitch. Типовые схемы построения корпоративных сетей IP-телефонии: IP-Centrex, IP-PBX, Cisco CallManager, архитектура AVVID IPCC - IP Contact Center		*2*
	9	**Услуги сетей IP-телефонии** Классификация провайдеров услуг IP-телефонии. Принципы тарификации. Биллинг		*2*

		в VoIP сетях.		
	10	**Управление сетями IP-телефонии**		*2*
	11	**Информационная безопасность в сетях IP-телефонии.** Типы угроз в сетях IP-телефонии Методы криптографической защиты информации. Технологии аутентификации. Особенности системы безопасности в IP-телефонии. Обеспечение безопасности на базе протокола OSP. Обеспечение безопасности IP-телефонии на базе VPN		*2*
	Лабораторные работы		6	
	1	Трассировка абонентской и межстанционной сигнализации		
	2	Тестирование кодеков		
	3	Исследование параметров качества обслуживания		
Тема 3.2. Администрирование сетей IP-телефонии	**Содержание**		26	
	1	**Настройка H.323** Описание H.323 и общие рекомендации. Функциональные компоненты H.323. Установка и поддержка соединения H.323. Соединения без использования GateKeeper. Соединения с использованием GateKeeper. Соединения с использованием нескольких GateKeeper Многопользовательские конференции. Обеспечение отказоустойчивости		*2*
	2	Настройка H.323 шлюзов. Настройка H.323 Gatekeeper Мониторинг и устранение неисправностей		*2*
	3	**Настройка SIP** Описание и общие рекомендации. Технология SIP и связанные с ней стандарты Функциональные компоненты SIP. Сообщения SIP. Адресация SIP. Модель установления соединения Планирование отказоустойчивости.		*2*
	4	Настройка SIP на маршрутизаторах . Мониторинг и устранение неисправностей.		*2*
	5	**Настройка шлюзов** Классификация шлюзов, модель организации связи. Команды протокола, структура команд, структура ответов на команды, Описание сеансов связи. Установление, изменение и разрушение соединений. Рекомендации по выбору нужного шлюза Определение способов подключения шлюзов в окружении предприятия, провайдера услуг. Мониторинг и устранение неисправностей Мониторинг и устранение неисправностей.		*2*
	6	**Группа Sigtran**		*2*

	Система общеканальной сигнализации №7 в IP-сети. Архитектура Sigtran. Транспортный протокол с управлением потоками. Основные функциональные возможности SCTP. Множественная адресация. Соединения для нескольких потоков. Мониторинг и устранение неисправностей		
7	**Установка и инсталляция программного коммутатора** Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутристанционная маршрутизация.		*2*
8	**Управление программным коммутатором** Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM). Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP-абоненты. Группы абонентов. Дополнительные абонентские услуги		*2*
9	**Обслуживание программного коммутатора** Управление обработкой неисправностей, конфигурацией, тарификацией, рабочими характеристиками и безопасностью. Контроль и обработка аварийных сигналов для сетевых элементов. Инструменты для отслеживания событий и устранения неисправностей. Сигнальные трейсеры. Статистика.		*2*
10	**Организация эксплуатации систем IP-телефонии.** Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.		*2*
11	Наблюдение за правильной работой оборудования, периодический осмотр и контроль за техническим состоянием оборудования, устранение обнаруженных дефектов, регулировка и настройка.		*2*
12	**Средства мониторинга и анализа систем IP-телефонии**		*2*
13	**Восстановление работы сети после аварии** схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;		*2*
Лабораторные работы		42	
1	Настройка аппаратных IP – телефонов		
2	Настройка программных IP – телефонов, факсов		
3	Настройка шлюзов		
4	Установка, подключение и первоначальные настройки голосового маршрутизатора		
5	Настройка таблицы пользователей в голосовом маршрутизаторе		

	6	Настройка групп в голосовом маршрутизаторе	
	7	Настройка таблицы маршрутизации вызовов в голосовом маршрутизатое	
	8	Настройка голосовых сообщений в маршрутизаторе	
	9	Установка и начальное конфигурирование программного коммутатора	
	10	Настройка групп пользователей в программном коммутаторе	
	11	Конфигурирование IVR в программном коммутаторе	
	12	Настройка голосовой почты в программном коммутаторе	
	13	Настройка связи между двумя программными коммутаторами	
	14	Мониторинг и анализ соединений H.323	
	15	Мониторинг и анализ соединений SIP	
	16	Мониторинг и анализ протокола MGCP	
	17	Мониторинг вызовов в программном коммутаторе	
	18	Создание резервных копий баз данных	
	19	Диагностика и поиск неисправностей в системах IP- телефонии	
	20	Устранение неисправностей в системах IP- телефонии	
	21	Восстановление работы сети после аварии	
Самостоятельная работа при изучении Раздела 3 ПМ 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 **Примерная тематика домашних заданий** 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. Основы протокола SIP и SIP-T Архитектура сети SIP и назначение её элементов. Адресация в сети SIP. Сообщения протокола SIP. Базовые сценарии установления соединения в сети, согласно протоколу SIP. Взаимодействие SIP с сетями ТфОП, рекомендация SIP-T. Возможности протокола SIP. Архитектура распределённого шлюза. Протоколы управления шлюзом MGCP, MEGACO/H.248. Принцип декомпозиции шлюза. Назначение элементов распределённого шлюза. Эволюция протоколов управления медиашлюзами. Протокол		48	

MGCP: модель соединения, команды протокола. Протокол MEGACO/H.248: особенности протокола, модель соединения, команды протокола, структура сообщений. Базовые сценарии установления соединения в сети с использованием протокола MEGACO/H.248. Протокол BICC Принципы, положенные в основу протокола BICC. Протокол BICC в контексте сетей IP-телефонии и NGN. Архитектура сети согласно BICC. Узлы обслуживания протокола BICC. Структура протокола BICC. Сигнальная транспортная служба. BICC Capability Set 1. BICC Capability Set 2. Сценарии обслуживания вызова с использованием BICC. Рабочая группа SIGTRAN Передача сигнализации ОКС 7 по IP сети. Архитектура SIGTRAN. Семейство протоколов SIGTRAN: M2UA, M2PA, M3UA, SUA, IUA, V5UA. Протокол передачи с управлением потоками SCTP. Технология MPLS Обеспечение качества в сетях IP-телефонии. Архитектура сети MPLS. Основные понятия технологии MPLS. Передача трафика по сети MPLS. Протокол LDP. Traffic Engineering в MPLS. Основы построения NGN Термин NGN. Причины эволюции сетей связи. Тенденции развития сетей связи. Особенности перехода к NGN в России. Услуги NGN. Назначение основных элементов IMS. Протоколы IMS. Концепция предоставления услуг в IMS. Проект TISPAN.			
Организация мультисервисного доступа. Эволюция сетей доступа при переходе к NGN. Современное оборудование мультисервисного абонентского доступа. Мультисервисные абонентские концентраторы. IAD. Примеры организации сети доступа. Softswitch: оборудование и архитектура. Терминология Softswitch. История развития технологии Softswitch. Стандартизующие организации. Эталонная архитектура Softswitch. Функциональные возможности Softswitch. Softswitch 4 и 5 классов. Граничные контроллеры сессий SBC. История и причины появления SBC. Функции SBC. Возможные архитектуры построения SBC. Взаимосвязь Softswitch и SBC. Архитектура NGN 3GPP. IMS Организации 3GPP и 3GPP2 и мобильные сети 3G. Принципы IMS. Архитектура IMS.			
УП.ПМ.03.03	**Содержание**		36
	1	Архитектура сети Интернет	
	2	Использование модели уровней	
	3	Примеры протоколов и сервисов прикладного уровня	
	4	Протокол управления передачей TCP – надёжная коммуникация	
	5	Протокол дейтаграмм пользователя UDP – коммуникация с малой нагрузкой	
	6	IPv4	
	7	Маршрутизация – как обрабатываются наши пакеты	
	8	Процесс маршрутизации: как узнаются маршруты	
	9	Адресация IPv4	
	10	Вычисление адресов	

	11	Канальный уровень – Доступ к среде передачи	
	12	Адресация при доступе к среде и формирование кадров	
	13	Физический уровень – коммуникация сигналов	
	14	Ethernet – коммуникации через локальную сеть	
	15	Кадр Ethernet	
	16	Хабы и свитчи	
	17	Протокол разрешения адресов ARP	
	18	Настройка устройств Cisco – Основы IOS	
ПП.ПМ.03	1	Анализ трафика сети	144
	2	Анализ трафика сети	
	3	Анализ трафика сети	
	4	Работа с кабельными сканерами и тестерами	
	5	Работа с кабельными сканерами и тестерами	
	6	Работа с кабельными сканерами и тестерами	
	7	Работа со встроенными сканерами диагностики и управления.	
	8	Работа со встроенными сканерами диагностики и управления.	
	9	Работа со встроенными сканерами диагностики и управления.	
	10	Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных таблиц	
	11	Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных таблиц	
	12	Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных таблиц	
	13	Восстановление сети после сбоя.	
	14	Восстановление сети после сбоя.	
	15	Восстановление сети после сбоя.	
	16	Создание плана восстановления сети	
	17	Создание плана восстановления сети	
	18	Создание плана восстановления сети	
	19	Использование в работе контрольно	
	20	Использование в работе контрольно	
	21	Использование в работе контрольно	
	22	Разработка функциональных схем элементов автоматизированной системы защиты	

		информации		
	23	Разработка функциональных схем элементов автоматизированной системы защиты информации		
	24	Разработка функциональных схем элементов автоматизированной системы защиты информации		
	25	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование		
	26	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование		
	27	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование		
	28	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование		
	29	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование		
	30	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации		
	31	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации		
	32	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации		
	33	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации		
	34	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации		
	35	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации		
	36	Разработка политик безопасности и внедрение их в операционные системы		
	37	Разработка политик безопасности и внедрение их в операционные системы		
	38	Разработка политик безопасности и внедрение их в операционные системы		
	39	Разработка политик безопасности и внедрение их в операционные системы		
	40	Разработка политик безопасности и внедрение их в операционные системы		
	41	Разработка политик безопасности и внедрение их в операционные системы		
	42	Настройка IPSec и VPN. Настройка межсетевых экранов		

	43	Настройка IPSec и VPN. Настройка межсетевых экранов	
	44	Настройка IPSec и VPN. Настройка межсетевых экранов	
	45	Настройка IPSec и VPN. Настройка межсетевых экранов	
	46	Настройка IPSec и VPN. Настройка межсетевых экранов	
	47	Настройка IPSec и VPN. Настройка межсетевых экранов	
	48	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	49	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	50	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	51	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	52	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	53	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	54	Настройка защиты беспроводных сетей с помощью систем шифрования	
	55	Настройка защиты беспроводных сетей с помощью систем шифрования	
	56	Настройка защиты беспроводных сетей с помощью систем шифрования	
	57	Настройка защиты беспроводных сетей с помощью систем шифрования	
	58	Настройка защиты беспроводных сетей с помощью систем шифрования	
	59	Настройка защиты беспроводных сетей с помощью систем шифрования	
	60	Архивация и восстановление ключей в Windows Server (PKI).	
	61	Архивация и восстановление ключей в Windows Server (PKI).	
	62	Архивация и восстановление ключей в Windows Server (PKI).	
	63	Архивация и восстановление ключей в Windows Server (PKI).	
	64	Архивация и восстановление ключей в Windows Server (PKI).	
	65	Архивация и восстановление ключей в Windows Server (PKI).	
	66	Установка и настройка системы обнаружения атак Snort.	
	67	Установка и настройка системы обнаружения атак Snort.	
	68	Установка и настройка системы обнаружения атак Snort.	
	69	Установка и настройка системы обнаружения атак Snort.	

	70	Установка и настройка системы обнаружения атак Snort.		
	71	Установка и настройка системы обнаружения атак Snort.		
	72	Установка и настройка системы обнаружения атак Snort.		
		Всего	750	

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 лабораторий **эксплуатации объектов сетевой инфраструктуры** и **программно-аппаратной защиты объектов сетевой инфраструктуры, а** также полигона **технического контроля и диагностики сетевой инфраструктуры.**

Лаборатория эксплуатации объектов сетевой инфраструктуры

Оборудование лаборатории и рабочих мест мастерской:

- Оборудование лаборатории и рабочих мест лаборатории: 12 компьютеров ученика и 1 компьютер учителя;
- Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ-45, тестеры для кабеля);
- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности.

Оборудование и технологическое оснащение рабочих мест:

- Компьютер ученика (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО – CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)
- Компьютер учителя (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО – CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР).
- Сервер в лаборатории (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; Жесткий диск объемом не менее 1Тб; программное обеспечение:Windows Server 2003 или Windows Server 2008; лицензионные антивирусные программы; лицензионные программы восстановления данных.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением
- интерактивная доска
- проектор

Лаборатория программно-аппаратной защиты объектов сетевой инфраструктуры:

Оборудование мастерской и рабочих мест мастерской:

- Оборудование лаборатории и рабочих мест лаборатории: 12 компьютеров ученика и 1 компьютер учителя;
- Типовое активное оборудование: сетевые маршрутизаторы, сетевые коммутаторы, сетевые хранилища, сетевые модули и трансиверы, шасси и блоки питания, шлюзы VPN, принт-серверы, IP – камеры, медиа-конвертеры, сетевые адаптеры и карты, сетевые контроллеры, оборудование xDSL, аналоговые модемы, коммутационные панели, беспроводные маршрутизаторы, беспроводные принт-серверы, точки доступа WiFi, WiFi – адаптеры, Bluetooth – адаптеры, KVM-коммутаторы, KVM-адаптеры, VoIP маршрутизаторы, VoIP-адаптеры;
- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности.

Оборудование и технологическое оснащение рабочих мест:

- Компьютер ученика (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб;

программное обеспечение: лицензионное ПО – CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)

- Компьютер учителя (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО – CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)
- Сервер в лаборатории (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; Жесткий диск объемом не менее 1Тб; программное обеспечение:Windows Server 2003 или Windows Server 2008; лицензионные антивирусные программы; лицензионные программы восстановления данных.

Перечень программного обеспечения:

1. MS Windows 7
2. MS Office 2007
3. MS Windows 2003/2008
4. Ethereal, разработчик – Gerald Combs (C) 1998-2005, источник – http://www.ethereal.com, версия 0.10.11.
5. InterNetView, разработчик – Evgene Ilchenko, источник – http://www.tsu.ru /~evgene/info/inv, версия 2.0.
6. Netcat, разработчик – Weld Pond <weld@l0pht.com>, источник – http://www. l0pht.com, версия 1.10.
7. Nmap, разработчик – Copyright 2005 Insecure.Com, источник – http://www.insecure.com, версия 3.95.
8. Snort, разработчик – Martin Roesch & The Snort Team. Copyright 1998–2005 Sourcefire Inc., et al., источник – http://www.snort.org, версия 2.4.3.
9. VipNet Office, разработчик – ОАО Инфотекс, Москва, Россия, источник – http://www.infotecs.ru, версия 2.89 (Windows).
10. VMware Workstation, разработчик – VMware Inc, источник – http://www. vmware.com, версия 4.0.0.
11. WinPCap, источник – http://winpcap.polito.it.
12. AdRem Netcrunch, источник – http://www.adremsoft.com/netcrunch/

Nessus, источник – http://www.nessus.org

4.2. Информационное обеспечение обучения

Основные источники:

1. Бройдо, В. Вычислительные системы, сети и телекоммуникации: учебник для вузов/В.Бройдо, О.Ильина. - СПб.: Питер, 2010.
2. Виснадул, Б.Д. Основы компьютерных сетей: учебное пособие для учрежд. СПО/ Б.Д.Виснадул, С.А.Лупин, С.В. Сидоров; под ред. Л.Г.Гагариной. - М.: ФОРУМ: Инфра-М, 2012.
3. Исаченко, О.В. Программное обеспечение компьютерных сетей: учебное пособие для студ. учрежд. СПО. - М.: ИНФРА-М, 2014.
4. Кузин, А.В. Компьютерные сети: учебное пособие для студ. учрежд. СПО. - М.: Форум: ИНФРА-М, 2014.
5. Максимов, Н.В. Компьютерные сети: учебное пособие/Н.В.Максимов, И.И.Попов. - М.: ФОРУМ, 2013.
6. Назаров, А.В. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений СПО.- М.: Академия, 2014.
7. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для

вузов/В.Г.Олифер, Н.А.Олифер. - СПб. : Питер, 2012.
8. Олифер, В. Г. Основы компьютерных сетей: учебное пособие /В.Г.Олифер, Н.А.Олифер. - СПб.: Питер, 2014.
9. Таненбаум, Э. Компьютерные сети/Э.Таненбаум, Д.Уэзеролл. - СПб.: Питер, 2014.
10. Техническая диагностика современных цифровых сетей связи. Основные принципы и технические средства измерений параметров передачи для сетей PDH, SDH, IP, Ethernet и ATM/И.И.Власов, Э.В.Новиков, М.М.Птичников, Д.В.Сладких; под ред. М.М.Птичникова. - М.: Горячая линия-Телеком, 2012.
11. Технологии разработки и создания компьютерных сетей на базе аппаратуры D-LINK: учебное пособие для вузов/ В. В.Баринов, А. В.Благодаров, Е. А.Богданова, А. Н.Пылькин, Д. М.Скуднев. - М.: Горячая линия-Телеком, 2012.
12. Чекмарев, Ю. В. Вычислительные системы, сети и телекоммуникации. - М.: ДМК- Пресс, 2013.
13. Башлы, П. Н. Информационная безопасность и защита информации: учебник/П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013.
14. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для СПО /А.В.Васильков, И.А.Васильков. - М.: ФОРУМ, 2013.
15. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО/ В.Я.Ищейнов, М.В.Мецатунян. - М.: Форум: ИНФРА-М, 2015.
16. Партыка, Т.Л. Информационная безопасность: учебное пособие для студ. учредж. СПО /Т.Л.Партыка, И.И.Попов. - М.: Форум, 2014.
17. Рябко, Б.Я. Основы современной криптографии и стеганографии / Б.Я.Рябко, А.Н.Фионов. - М.: Горячая линия-Телеком, 2013.
18. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие для вузов. - М.: Форум: Инфра-М, 2015.
19. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО/В.Ф.Шаньгин. - М.: ФОРУМ: ИНФРА-М, 2014.
20. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. - М.: ФОРУМ: ИНФРА-М, 2013.
21. Гольдштейн, Б.С. IP-телефония / Б.С.Гольдштейн, А.В.Пинчук, А.Л.Суховицкий. - СПб. БХВ-Петербург, 2014.
22. Гольдштейн Б. С. Call-центры и компьютерная телефония/Б.С.Гольдштейн, В.А.Фрейнкман. - СПб.: БХВ-Петербург, 2014.
23. Гольдштейн Б. С. Softswitch/ Б.С..Гольдштейн, А.Б.Гольдштейн. - СПб.: БХВ-Петербург, 2014.

Дополнительные источники:

1. Васин, Н. Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов. - М.: Интернет-университет информационных технологий: Бином. Лаборатория знаний, 2011.
2. Васин, Н. Н. Построение сетей на базе коммутаторов и маршрутизаторов. - М.: Интернет-университет информационных технологий, 2011.
3. Головин, Ю.А. Информационные сети: учебник для вузов/Ю.А.Головин, А.А.Суконщиков, С.А.Яковлев. - М.: Академия, 2011.
4. Гусева, А. И. Вычислительные системы, сети и телекоммуникации / А. И. Гусева, В. С.Киреев. - М.: Академия, 2014.
5. Жуков, В. Г. Беспроводные локальные сети стандартов IEEE 802.11 a/b/g: учебное пособие. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010.
6. Запечников, С. В.Основы построения виртуальных частных сетей: учебное пособие для вузов/С.В.Запечников, Н.Г.Милославская, А.И.Толстой. - 2-е изд., стереотип.- М.: Горячая линия -Телеком, 2011.
7. Иншаков, М.В. Технологии и средства реализации информационных процессов в вычислительных сетях: учебное пособие. - М.: Московский городской педагогический

университет, 2013.
8. Киселев, С.В. Основы сетевых технологий: учебник для образоват. учрежд., реализующих программы НПО. - М.: Академия, 2012.
9. Новожилов, Е.О. Компьютерные сети: учебное пособие для студентов учреждений СПО/ Е.О.Новожилов, О.П.Новожилов. - М.: Академия, 2011.
10. Поляк-Брагинский, А. Локальная сеть. Самое необходимое. – СПб.: БХВ-Петербург, 2011.
11. Поляк-Брагинский, А. Локальная сеть под Linux. - СПб.: БХВ-Петербург, 2010.
12. Смелянский, Р.Л. Компьютерные сети: учебное пособие для вузовВ 2 ч. -М.: Академия, 2011.
13. Смирнова, Е.А. и др. Построение коммутируемых компьютерных сетей.- М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2013.
14. Авдошин, С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности/ С.М.Авдошин, А.А.Савельева, В.А.Сердюк. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2010.
15. Агапов, А. В. Обработка и обеспечение безопасности электронных данных: учебное пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев и др.; под ред. Д. В. Денисова. - М.: МФПУ Синергия, 2012.
16. 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.
17. Баранова, Е. К. Основы информатики и защиты информации: учебное пособие . - М. : РИОР : ИНФРА-М, 2013.
18. Баранова, Е.К. Моделирование системы защиты информации: практикум: учебное пособие / Е.К.Баранова, А.В.Бабаш. - М.: РИОР: ИНФРА-М, 2015.
19. Бурняшов, Б.А. Меры защиты информации на уровне пользователя информационно-технологическими средствами: методические указания к самостоятельной работе студентов: учебно-методическое пособие. - Саратов: Вузовское образование, 2014.
20. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: ИНФРА-М, 2015.
21. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками.-М.: Горячая линия-Телеком, 2012.
22. 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.
23. Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP: учебное пособие. - Красноярск : Сиб. гос. аэрокосмич. Ун-т, 2012.
24. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности: учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012.
25. Малюк, А.А. Введение в информационную безопасность: учебное пособие/ А.А.Малюк, В.С.Горбатов, В.И.Королев. - М.: Горячая линия - Телеком, 2011.
26. 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.
27. Мельников, В.П. Информационная безопасность и защита информации: учебное пособие для вузов/В.П.Мельников, С.А.Клейменов, А.М.Петраков; под ред. С.А.Клейменова.-М.: Академия, 2011.
28. Мельников, В.П. Информационная безопасность: учебное пособие для студ. учрежд. СПО/В.П.Мельников, С.А.Клейменов, А.М.Петраков; под ред. С.А.Клейменова.-М.: Академия, 2010.
29. Мельников, Д.А. Информационная безопасность открытых систем. - М.: Флинта, 2014.
30. Петренко, С. А. Политики информационной безопасности /С.А.Петренко, В.А.Курбатов. - М: ДМК Пресс, 2010.

31. Платонов, В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. - М.: Академия, 2013.
32. Радько, Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа/Н.М.Радько, И.О.Скобелев; под ред. В.И.Борисова.-М.: РадиоСофт, 2010.
33. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие. – СПб.: Питер, 2010.
34. Рябко, Б. Я. Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. – М.: Горячая линия–Телеком, 2012
35. Скрипник, Д.А. Общие вопросы технической защиты информации. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2012.
36. Технические средства и методы защиты информации: учебное пособие для ВУЗов/А.П.Зайцев, А.А.Шелупанов, Р.В.Мещеряков и др.; под ред. А.П.Зайцева, А.А.Шелупанова. - М.: Горячая линия-Телеком, 2012.
37. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс, 2010.
38. 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.
39. 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), 2008.
40. Гольдштейн, Б. С. Протокол SIP: справочник /Б.С.Гольдштейн, А.А.Зарубин, В.В.Саморезов. - СПб.: БХВ-Петербург, 2014.
41. Гольдштейн, Б.С. Сигнализация в сетях связи. Том 1. - СПб.: БХВ-Петербург, 2014.

Интернет-ресурсы:

1. CIT-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: http://old.intuit.ru, 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. Небаев, И.А. Разработка единой компьютерной сети передачи данных на базе технологии Ethernet и протокола IP [Электронный ресурс]: учебное пособие к курсовому проектированию/Кафедра обработки и передачи данных СПбГУТ. - 2012. - Режим доступа: http://opds.sut.ru/wp-content/uploads/mu/kspd_project.pdf, свободный.
7. SecurityLab. Защита информации и информационная безопасность [Электронный ресурс]: информационный портал/ООО "Positive Technologies". - Режим доступа: http://www.securitylab.ru, свободный.
8. VoIPReview: информационный сайт [Электронный ресурс]. — Режим доступа: http://voipreview.ru/, свободный.
9. 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, свободный.
10. 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, свободный.
11. Гольдштейн, Б.С. Протоколы IP-телефонии: RTP, RTCP [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, свободный.
12. Некоторые аспекты технологий IP-телефонии [Электронный ресурс]. — Режим доступа: http://www.ixbt.com/comm/ip-aspects.html, 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.

Консультации предусматриваются в объеме 100 часов на учебную группу на каждый учебный год, в том числе в период реализации среднего (полного) общего образования для лиц, обучающихся на базе основного общего образования. Формы проведения консультаций: групповые, индивидуальные, письменные, устные.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): реализация программы профессионального модуля должна обеспечиваться педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемого модуля.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального модуля в рамках производственной практики, эти преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

Инженерно-педагогический состав: высшее образование, соответствующее профилю преподаваемого модуля.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения практических и лабораторных занятий, тестирования.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	***Формы и методы контроля и оценки***
Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей	– точность и скорость настройки сети; – качество рекомендаций по повышению работоспособности сети; – выбор технологического оборудования для настройки сети; – расчет времени для настройки сети; – точность и грамотность оформления технологической документации.	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
Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях	– точность и скорость настройки сети; – качество анализа свойств сети, исходя из ее служебного назначения; – качество рекомендаций по повышению технологичности сети; – точность и грамотность оформления технологической документации.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики
Осуществлять эксплуатацию сетевых конфигураций	– точность и скорость настройки сети; – качество анализа и рациональность выбора сетевых конфигураций; – выбор способов настройки и технологически грамотное назначение технологической базы	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических

		занятиях, -при выполнении определенных видов работ производственной практики, - зачет по разделу практики
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
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
Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	– 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 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.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	1) Формулировка области и объектов профессиональной деятельности техника-программиста по разработке и адаптации ПО в соответствии с ФГОС по специальности 230701 Прикладная информатика (по отраслям); 2) участие в профессиональных конкурсах, конференциях, проектах, выставках, фестивалях, олимпиадах	*оценка на экзамене по модулю* - *оценка профессио-нального портфолио студента на экзамене по модулю*
Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	1) четкое выполнение должностных обязанностей в рамках конкретного проекта 2) дана адекватная оценка эффективности и качества выбранных методов решения профессиональных задач	- *интерпретация результатов наблюдения на производственной практике;* - *оценка анализа эффективности методов решения профессиональных задач на производственной практике*
Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.	-верность принятия решения в смоделированной нестандартной ситуации по разработке и адаптации ПО с оценкой возможных рисков при их реализации;	*Накопительная оценка за решения смоделированных нестандартных ситуации на учебной практике*
Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.	- отобранная на основе анализа и оценки информация позволяет ставить и решать профессиональные задачи и задачи профессионального и личностного развития	*Накопительная оценка за представленную информацию на учебной практике*
Использовать информационно-	- для разработки и адаптации ПО использованы современ-ные	*интерпретация результата наблюдения за*

коммуника-ционные технологии для совершенствования профес-сиональной деятельности.	информационно-коммуникационные технологии	*деятельностью на производственной практике*
Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.	- эффективность взаимодействия с коллегами, клиентами при разработке технического задания проекта	*интерпретация результата наблюдения за деятельностью студента на производственной практике*
Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности 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;	*интерпретация результата наблюдения за деятельностью студента на производственной практике*
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;	*оценка плана самообразования на учебной практике*
Быть готовым к смене технологий в профессиональной деятельности.	- проектная деятельность организована с использованием новых отраслевых технологий	*интерпретация результата наблюдения за деятельностью студента на производственной практике*
Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).	-эффективность использова-ния полученных профессио-нальных знаний для исполнения воинской обязанности	*экспертная оценка на военных сборах*