ГБПОУ «СТАПМ им.Д.И. Козлова»

УТВЕРЖДАЮ:
Зам.директора по УР ГБПОУ
«СТАПМ им. Д.И.Козлова»
_____ Н.В. Кривчун
«26» 05 2016 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Профессиональные модули
программы подготовки специалистов среднего звена

по специальности 09.02.02 Компьютерные сети

2016

ОДОБРЕНО

Цикловой комиссией
Специальностей: 09.02.04
Информационные системы (по отраслям),
230115 Программирование в компьютерных системах,
27.02.04 Автоматические системы управления
Председатель
_____ Инжеватова Г.В.
« 26 » 05 2016 г.

Составители:
Инжеватова Г.В., преподавателЬ ГБПОУ «СТАПМ им. Д.И. Козлова».

Эксперты: Внутренняя экспертиза
Содержательная экспертиза: _____ Зам.директора по МР Губарь А.С.

Техническая экспертиза:_____ Ст.методист Ляпнева Н.М

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.02 Компьютерные сети (утв. приказом Министерства образования и науки РФ от 28 июля 2014 г. N 803).

Рабочая программа профессионального модуля разработана в соответствии с разъяснениями по формированию примерных программ учебных модулей начального профессионального и среднего профессионального образования на основе Федеральных государственных образовательных стандартов начального профессионального и среднего профессионального образования, утвержденными И.М. Реморенко, директором Департамента государственной политики и нормативно-правового регулирования в сфере образования Министерства образования и науки Российской Федерации от 27 августа 2009 года.

Содержание программы реализуется в процессе освоения студентами программы подготовки специалистов среднего звена по специальности 09.02.02 Компьютерные сети в соответствии с требованиями ФГОС СПО третьего поколения.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 Эксплуатация объектов сетевой инфраструктуры

1.1. Область применения рабочей программы

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

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

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

ПМ.3.3 Эксплуатировать сетевые конфигурации;

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

ПМ.3.5 Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования;

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

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области информатики и вычислительной техники при наличии среднего (полного) общего образования. Опыт работы не требуется.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального 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. Количество часов на освоение рабочей программы профессионального модуля:

максимальной учебной нагрузки обучающегося – 541 час, включая:
обязательной аудиторной учебной нагрузки обучающегося – 379 часов,
в том числе:
лабораторных и практических занятий – 136 часов,
самостоятельной работы обучающегося – 127 часов;
производственной практики (по профилю специальности) 162 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) **Разработка технологических процессов изготовления деталей машин**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК3. 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 в 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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Код 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
МДК 03.01 Эксплуатация объектов сетевой инфраструктуры ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6.		230	153	82		77			
МДК 03.02. Безопасность функционирования информационных систем ПК 3.1-3.2		149	99	54		50			
Производственная практика (по профилю специальности)		162							162
Всего:		541	252	136		127			162

3.2. Содержание обучения по профессиональному модулю (ПМ)

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 ПМ 3. Эксплуатация объектов сетевой инфраструктуры			**541**	
МДК 03.01 Эксплуатация объектов сетевой инфраструктуры			**230**	
Раздел 1. Эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей.			**25**	
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры	**Содержание**		10	
	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.		3
	4.	**Техническая и проектная документация.** Паспорт технических устройств; руководство по эксплуатации; Физическая карта всей сети; логическая схема компьютерной сети;		1
Самостоятельная работа обучающихся по разделу 1: Повторение пройденного материала; Примерная тематика внеаудиторной работы: 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;			15	

Раздел 2. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях.			**45**	
Тема 2.1 Профилактические работы	**Содержание**		8	2
	1.	**Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры** Комплекс организационно-технических мероприятий; выявление и своевременная замена элементов инфраструктуры.		
	2.	**Проверка объектов сетевой инфраструктуры и профилактические работы** Проверка физических компонентов; проверка документации и требований; проверка списка совместимого оборудования.		3
	3.	**Проведение регулярного резервирования** Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения.		2
	Практические занятия			
	1.	. Поддержка пользователей сети	22	
	1.	Создание пользователей в domain, редактирование пользователей в domain, создание пароля пользователем в domain, создание групп и распределение пользователей по группам в domain		
	2	Настройка прав доступа		
	3	Оформление технической документации, правила оформления документов.		
	4	Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain		
	5	Выполнение мониторинга и анализа работы локальной сети с помощью программных средств		
	6	Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы, коммутационное оборудование)		
Самостоятельная работа обучающихся по разделу 2: **Примерная тематика внеаудиторной самостоятельной работы:** Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. Технические регламенты, виды документов для технических осмотров, методы и принципы проверки различного			15	

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.				
Раздел 3. Эксплуатация сетевых конфигураций.			**61**	
Тема 3.1 Управление сетями	**Содержание**		20	2
	1.	**Архитектура системы управления. Структура системы управления.** Архитектура в концепции TMN; централизованное управление; децентрализованное управление.		
	2.	**Уровни управления** Многоуровневая архитектура управления TMN: бизнесом; услугами; сетью; элементами сети; уровень элементов сети.		2
	3.	**Области управления.** Области управления ошибками; конфигурацией; доступом; производительностью; безопасностью.		2
	4.	**Протоколы управления.** SNMP; CMIP; TMN; LNMP; ANMP.		2
	5.	**Управление отказами.** Выявление, определение и устранение последствий сбоев и отказов в работе сети.		2
	6.	**Учет работы сети. Управление конфигурацией.** Регистрация, управление используемыми ресурсами и устройствами; конфигурирование компонентов сети, сетевые адреса и идентификаторы, управление параметрами сетевых операционных систем.		3
	7.	**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.		3
	Лабораторные работы		10	
	1	Анализ сетевого трафика средствами Сетевого монитора		
	2	Основные сведения о сетевом мониторе		
	3	Запись данных средствами Сетевого монитора		
	4	Устранение неполадок с помощью Ping и PathPing		
	5	Диагностика сети и Netdiag		
	Практические занятия		6	

	1	Удаленное администрирование;		
	2	Восстановление работоспособности сетевой инфраструктуры.		
	3	Авторизация подключений удаленного доступа		
	Лабораторные работы		6	
	1	Вкладка. Сеть утилиты. Диспетчер задач		
	2	Использование консоли. Производительность		
	3	Мониторинг сетевого трафика с помощью утилиты Netstat		
	Практические занятия		4	
	1.	Тестирование кабелей		
	2	Тестирование коммутационного оборудования		
Самостоятельная работа обучающихся по разделу 3: Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Тематика внеаудиторной самостоятельной работы:** 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; Средства устранения неполадок DNS;			15	
1.				
Раздел 4. Схемы послеаварийного восстановления работоспособности компьютерной сети.			**41**	
Тема 4.1 Хранение информации	**Содержание**		10	3
	1.	**Резервное копирование данных**		
	2.	**Хранилищ данных** Принципы работы хранилищ данных. Принципы построения. Основные компоненты хранилища данных		2

	3.	**Технологии управления информацией. OLAP-технология**		2
	4.	**Понятие баз данных.** Основные понятия, принцип работы. СУБД		3
	Лабораторные работы		8	
	1.	Операции по резервному копированию данных;		
	2.	Операции по восстановлению данных.		
	Практические занятия			
	1.	Организации по бесперебойной работе системы по резервному копированию		
	2.	Восстановление информации		
Тема 4.2 Схема после аварийного восстановления	**Содержание**		10	
	1.	Принципы планирования восстановления работоспособности сети при аварийной ситуации		2
	2.	Допущения при разработке схемы послеаварийного восстановления. Основные требования к политике организации схемы послеаварийного восстановления		2
	3.	Организация работ по восстановлению функционирования системы		2
	4.	**План восстановления системы** Порядок уведомления о чрезвычайных событиях. Активация. Возврат к нормальному функционированию системы.		3
	Лабораторные работы		8	
	1.	Восстановление работоспособности сети после сбоя		
	2.	Разработка плана восстановления		
	Практические занятия			
	1.	Использовать схему после аварийного восстановления сети.		
	2.	Возврат к нормальному функционированию системы.		
Самостоятельная работа обучающихся по разделу 4: Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Повторение пройденного материала, Изучение утилиты Acronis, изучение безопасной зоны Acronis, Создание контрольной точки восстановления с помощью Acronis; Создание базы данных на примере учебной группы; Разработка плана восстановления работоспособности сети на примере одной взятой организации (колледжа, офиса)			15	
Раздел 5.	**Замена расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой**		**58**	

	инфраструктуры.			
Тема 5.1 Диагностика неисправностей технических средств и сетевой структуры	**Содержание**		23	
	1.	Принципы локализации неисправностей		3
	2.	Контрольно-измерительная аппаратура		3
	3.	Сервисные платы и комплексы		3
	4.	Программные средства диагностики		2
	5.	Номенклатура и особенности работы тест-программ		2
	6.	Диагностика неисправностей средств сетевых коммуникаций		3
	7.	Контроль функционирования аппаратно-программных комплексов.		2
	8.	Действия при не работающей сети, при медленной сети,		3
	9.	Действия при не стабильно работающей сети.		3
	Практические занятия		18	
	1.	Работа контрольно-измерительной аппаратуры		
	2.	Замена расходных материалов		
	3.	Мелкий ремонт периферийного оборудования		
	4.	Программная диагностика неисправностей		
	5.	Аппаратная диагностика неисправностей		
	6.	Поиск неисправностей технических средств		
	7.	Выполнение действий по устранению неисправностей		
	8.	Установка программного обеспечения		
Самостоятельная работа обучающихся по разделу 5: Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Поиск неисправностей по принципу локализации неисправностей конкретного оборудования; Изучить и понять принцип работы новых контрольно-измерительных аппаратов			17	
МДК 03.02. Безопасность функционирования информационных			**149**	

систем				
Введение	Информационная безопасность и технологии защиты информации		**2**	
Тема 1.1 Основы информационной безопасности	**Содержание**		10	**3**
	1.	**Понятие национальной безопасности.** Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.		
	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.		**3**
	4.	**Информация - наиболее ценный ресурс современного общества.** Понятие «информационный ресурс». Классы информационных ресурсов.		**3**
	5.	**Проблемы информационной войны.** Информационное оружие и его классификация. Информационная война.		**3**
	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.		**3**
	7.	**Информационные системы.** Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах.		**3**
	8.	**Методы и модели оценки уязвимости информации.** Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита»		**3**
Тема 1.2. Проблемы информационной безопасности.	**Содержание**		7	**3**
	1.	**Основные понятия и анализ угроз информационной безопасности.** Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.		

	2.	**Проблемы информационной безопасности сетей.** Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей.		**3**
	3.	**Политика безопасности.** Основные понятия политики безопасности. Структура политики безопасности организации.		**3**
	4.	**Стандарты информационной безопасности.** Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий		**3**
Тема 1.3. Технологии защиты данных.	**Содержание**		9	
	1	**Принципы криптографической защиты информации.** Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования. Электронная цифровая подпись и функция хэширования.		**2**
	2	**Криптографические алгоритмы.** Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы.		**3**
	3	**Технологии аутентификации.** Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.		**3**
	Практические работы		22	
	1	Криптографическое шифрование методом простой замены		
	2	Криптографическое шифрование методом многоалфавитной одноконтурной замены.		
	3	Криптографическое шифрование методом усложнённой перестановки по маршрутам.		
	4	Составление блок-схемы алгоритма идентификации и установки подлинности пользователя		
	5	Аутентификация пользователей		
Тема 1.4. Технологии	**Содержание**		12	

защиты межсетевого обмена данными.	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.		**3**
	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.		**3**
	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 Sign-On. Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.		**1**
	Практические занятия		22	
	1	Компоненты межсетевого экрана. Политика межсетевого экранирования		
	2	Задачи, решаемые VPN. Уровни защищенных каналов. Защита данных на канальном уровне		
	3.	Создание ключей PGP		
	4.	Передача открытого ключа PGP корреспондентам		
	5.	Работа с командной строкой. Сетевая активность		
	6.	Расчет ожидаемого времени раскрытия пароля, состоящего из определённого количества символов		
Тема 1.5. Технологии	**Содержание**		7	**1**

обнаружения вторжений.	1	**Анализ защищенности и обнаружение атак.** Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак.		
	2	**Защита от вирусов. Методы управления средствами сетевой безопасности.** Компьютерные вирусы и проблемы антивирусной защиты. Антивирусные программы и комплексы. Построение системы антивирусной защиты корпоративной сети. Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности.		**3**
	Практические занятия		10	
	1.	Настройка безопасности браузера Internet Explorer		
	2	Защита от несанкционированного доступа и сетевых хакерских атак		
	3	Обнаружение в реальном времени и отложенный анализ. Локальные и сетевые системы обнаружения атак		
	4	Установка антивирусного программного обеспечения		
Самостоятельная работа при изучении раздела ПМ 2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Службы каталогов. Подготовка индивидуального задания по теме «Аудит информационной безопасности компьютерных систем».			**50**	
Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Локальная сеть Ethernet, Шинная информационная система Profibus-DP. Сеть полевого уровня AS – interface.				
Производственная практика (по профилю специальности) итоговая по модулю. **Виды работ:** Составление структуры предприятия; Определение функций специалистов предприятия; Определение перспективы развития производства; Составление плана освоения новых технологий			**162**	

Ознакомление с проводимыми на ЛВС предприятия регламентные технические осмотры объектов сетевой инфраструктуры. Определение проведения на предприятии мониторинга и анализа работы локальной сети и регулярное резервирование Знакомство с архитектурой системы управления сетью предприятия. Структуры системы управления сетью. Использование удалённого администрирования в управлении сетью предприятия. Управление отказами. Выявление, определение и устранение последствий сбоев и отказов в работе сети. Используемые программные или аппаратно-программные системы в сетях предприятия Функции мониторинга, анализ трафика в сетях предприятия. Выявление причин аномальной работы сети предприятия. Приведения сети в работоспособное состояние. Локализации неисправностей сети. Контрольно-измерительная аппаратура предприятия. Применение хранилищ данных и резервного копирования данных на предприятии Применение и используемые методы криптографической защиты информации и электронной цифровой подписи. Применение и методы аутентификации, авторизации и администрирования действий пользователей в локальной сети. Управление подсистемой контроля входа в ЛВС предприятия. Использование виртуальных защищённых сетей VPN. Управление подсистемой управления доступом к БД предприятия. Технологии анализа защищённости и обнаружения атак.		
Всего	**541**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному 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 REMOTE ADMINISTRATOR 3.0.

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 2003, 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 –операционные системы Windows, UNIX, MS Office 2003, пакет САПР, VIRTUAL PC).
- 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. Dr Web Desktop Security Suite 6.0

Технические средства обучения:

Ontrack Easy Recovery 6.10.07, Restoration 3.2.13

- 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. Comodo Internet Security Rus 2015 (8.2.0.4703), источник – Free
5. Microsoft Security Essentials 4.7.205.0, источник – Free
6. Microsoft Network Monitor 3.4 источник – Free
7. TeamViewer 10.0.47484 источник – Free
8. FileZilla 3.14.1 источник – Free
9. Remote Administrator 3.0 Лицензионный сертификат Famatech от 26.03.2008г. – бессрочно
10. Ontrack EASYRecovery 6.10.07 источник – Free
11. Restoration 3.2.13 Netop School 6.2 Лицензионный сертификат от 22.10.2014г. - бессрочно
12. GNS3 1.3.11 источник – Free
13. LinuxLive USB Creator источник – Free
14. Oracle VirtualBox источник – Free
15. CPU-Z 1-71.0 источник – Free
16. WebSite X5 Evolution 11 источник – Free

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. О.Л. Голицына, Партыка Т.Л, И.И. Попов «Программное обеспечение» 3-е издание ФОРУМ 2010 год
2. Максимов Н.В., Попов И.И. «Компьютерные сети» учебное пособие для студентов учреждений профессионального образования ФОРУМ, 2010 год
3. В.Г. Олифер, Н.А. Олифер / Компьютерные сети. Принципы, технологии, протоколы.- 3 изд. СПБ: Изд. “Питер”, 2008г.
4. Осипенко, А. Л. Борьба с преступностью в глобальных компьютерных се-тях: Международный опыт [Текст]: Монография / А.Л. Осипенко. — М.: Норма, 2006. – 432 с.; 21 см. 3000 экз. – ISBN 5-89123-817-9
5. Партыка, Попов «Операционные системы, среды и оболочки» 2007 год
6. Т.Л. Партыка, И.И. Попов «Периферийные устройства вычислительной техники» 2-е издание М. Форум, 2009 год.
7. Скрембрей, Дж. Секреты хакеров. Безопасность Windows 2000 – готовые решения [Текст] : [пер. с англ.] / Джоел Скрембрей, Стюарт Мак-Клар. – М.: Вильямс, 2006. – 464 с. : ил. ; 24 см. – Перевод. изд.: Hacking Exposed. Windows 2000: Network security secrets & solutions / Joel Scrambray, Stuart McClure. – 3500 экз. – ISBN 5-8459-0300-9

8. Компьютерные сети. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки [Текст] : [пер. с англ.] – 2-е изд., испр. и доп. / Корпорация Майкорософт. – М. : Русская редакция, 2007. – 576 с. : ил. ; 24 см. + 1 электрон. опт. диск. – 3000 экз. – ISBN 5-7502-0101-5 (в пер.)

9. Уилсон, Э. Мониторинг и анализ сетей. Методы выявления неисправно-стей [Текст] : [пер. с англ.] / Эд Уилсон. – М.: ЛОРИ, 2006. – 350 с. : ил. ; 24 см. – Перевод. изд.: Network monitoring and analysys. A protocol ap-proach to troubleshooting / Ed Wilson. – 3200 экз. – ISBN 5-85582-163-3 (в пер.)

10. Рассел, Ч. Microsoft Windows 2000 Server. Справочник администратора [Текст] : [пер. с англ.] – 2-е изд., испр. / Ч. Рассел, Ш. Кроуфорд. – М.: ЭКОМ, 2006. – 1296 с. : ил. ; 25 см. + 1 электрон. опт. диск. – 3000 экз. – ISBN 5-7163-0084-7 (в пер.)

11. Чекмарев Ю. В. Ч37 Локальные вычислительные сети. Издание второе, исправленное и дополненное.– М.: ДМК Пресс, 2009. – 200 с. : ил. ISBN 978_5_94074_460_3

12. Фёдорова Г.Н. Информационные системы учебник, М., «Академия»,
13. 2013г. 2
14. Мельников В.П.Информационная безопасность, учебник, М., «Академия»,2009г.
7
15. Партыка Т.Л. Информационная безопасность, уч. пос., «Форум: Инфра-М», 2004г.

Дополнительные источники:

1. Корт, С. С. Теоретические основы защиты информации [Текст] : учеб. по-собие для вузов / С. С. Корт. – М.: Гелиос АРВ, 2005. – 240 с. : ил. ; 24 см. – 2000 экз. – ISBN 5-85438-010-2
2. Стивенс, У. Р. Протоколы TCP/IP. Практическое руководство [Текст] : [пер. с англ.] / У. Р. Стивенс. – СПб: БХВ-Петербург, 2005. – 672 с. : ил. ; 24 см. – 5000 экз. – ISBN 5-94157-300-6
3. Кульгин, М. Практика построения компьютерных сетей. Для профессио-налов [Текст] / М. Кульгин. – СПб.: Питер, 2007. – 320 с. : ил. ; 24 см. – 5000 экз. – ISBN 5-272-00351-9
4. Jones, A. Computer System Intrusion Detection: A Survey [Текст] / A. Jones, R. Sielken. – Department of Computer Science. University of Virginia, 2008. – 25 с. ; 30 см.
5. Treaster, M. A Survey of Distributed Intrusion Detection Approaches / M. Treaster. – National Center for Supercomputing Applications (NCSA). Univer-sity of Illinois, 2005. – 13 с. ; 30 см.
6. Kazienko, P. Intrusion Detection Systems (IDS). Part I, II [Электронный ре-сурс] / P. Kazienko, P. Dorosz. – http:/www.windowsecurity.com, 2004.
7. Справочная информация по локальным сетям [Электронный ресурс] http://lanhelper.ru/seti
8. Запечников, С.В. Основы построения виртуальных частных сетей [Текст]: Учеб. пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Тол-стой. — М.: Горячая линия–Телеком, 2005. — 249 с. ; 20 см. — 3000 экз. — ISBN 5-93517-139-2
9. Медведовский, И.Д. Атака на Internet [Текст] / И.Д. Медведовский, П.В.Семьянов, Д.Г.Леонов. – 2-е изд., перераб. и доп. – М.: ДМК, 1999. – 336 с.

10. Милославская, Н. Г. Интрасети: доступ в Internet, защита [Текст] : учеб. пособие для вузов / Н. Г. Милославская, А. И. Толстой. – М.: ЮНИТИ-ДАНА, 2005. – 527 с. : ил. ; 21 см. – 6000 экз. – ISBN 5-238-00134-7
11. Мандиа, К. Защита от вторжений. Расследование компьютерных преступ-лений [Текст] : [пер. с англ.] / К. Мандиа, К. Просис. – М.: ЛОРИ, 2005. – 476 с. : ил. ; 24 см. – Перевод. изд.: Incident response: investigating computer crime / Chris Prosise, Kevin Mandia. – 1500 экз. – ISBN 0-07-213182-9 (в пер.)
12. Лукацкий, А. В. Обнаружение атак [Текст] – 2-е изд., перераб. и доп. / А. В. Лукацкий. – СПб: БХВ-Петербург, 2005. – 608 с. : ил. ; 24 см. – 3000 экз. – ISBN 5-94157-246-8
13. Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Пер. с англ. - М. :Издательско-торговый дом «Русская Редакция», 2004. — 624 стр. : ил. ISBN 5-7502-0227-5
14. Бигелоу С. Сети: поиск неисправностей, поддержка и восстановление: Пер. с англ. – СПб.: БХВ-Петербург, 2005 – 1200 с.: ил. ISBN 5-94157-338-3

4.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках профессионального модуля «Эксплуатация объектов сетевой инфраструктуры» является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального.

При работе над курсовой работой (проектом) обучающимся оказываются консультации.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие высшего профессионального образования, соответствующего профилю модуля «Эксплуатация объектов сетевой инфраструктуры».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин.

Мастера: наличие 5–6 квалификационного разряда с обязательной стажировкой в профильных организациях не реже 1-го раза в 3 года. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

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 формирование 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**
ОК.01. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	-участие в работе научно-студенческих обществ, -выступления на научно-практических конференциях, -участие во внеурочной деятельности связанной с будущей профессией/специальностью (конкурсы профессионального мастерства, выставки и т.п.) - высокие показатели производственной деятельности	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: -на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.) - при выполнении и защите курсовой работы (проекта); - при выполнении работ на различных этапах производственной практики,
ОК.02. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач, оценка их эффективности и качества	
ОК.03. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	- анализ профессиональных ситуации; -решение стандартных и нестандартных профессиональных задач	
ОК.04. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	-эффективный поиск необходимой информации; -использование различных источников, включая электронные при изучении теоретического материала и прохождении различных этапов производственной практики	
ОК.05. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- использование в учебной и профессиональной деятельности различных видов программного обеспечения, в том числе специального, при оформлении и	

	презентации всех видов работ	
ОК.06. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	взаимодействие: - с обучающимися при проведении деловых игр, выполнении коллективных заданий (проектов), - с преподавателями, мастерами в ходе обучения, - с потребителями и коллегами в ходе производственной практики	
ОК.07. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполненных заданий.	- самоанализ и коррекция результатов собственной деятельности при выполнении коллективных заданий (проектов), -ответственность за результат выполнения заданий.	
ОК.08. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	- планирование и качественное выполнение заданий для самостоятельной работы при изучении теоретического материала и прохождении различных этапов производственной практики ; - определение этапов и содержания работы по реализации самообразования	
ОК.09. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	-адаптация к изменяющимся условиям профессиональной деятельности; -проявление профессиональной маневренности при прохождении различных этапов производственной практики	

ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ
В РАБОЧУЮ ПРОГРАММУ

№ изменения, дата внесения изменения; № страницы с изменением;	
БЫЛО	**СТАЛО**
Основание: **Подпись лица внесшего изменения**	