

Министерство транспорта Российской Федерации
ФГБОУ ВО «Российский университет транспорта (МИИТ)»
Институт прикладных технологий
МОСКОВСКИЙ КОЛЛЕДЖ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА


РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ
ИНФРАСТРУКТУРЫ

по специальности
09.02.02 Компьютерные сети

Москва 2017


СОГЛАСОВАНО

Первый заместитель начальника
дирекции информационно-
технологических систем и систем связи
ГУП Московский метрополитен


С.А. Пономаренко
_____ 2017г.

Разработана на основе Федерального
государственного образовательного
стандарта _____ среднего
профессионального образования по
специальности _____ 09.02.02
«Компьютерные сети» от 28 июля
2014 года №803

ОДОБРЕНА
Предметной (цикловой) комиссией
Протокол от 28 августа 2017 г. №1

Председатель

Т.А. Семенова

СОГЛАСОВАНО
и.о. зав. методическим кабинетом


Т.В. Сухарева



Составитель:

Тужилин С.М. – преподаватель МКЖТ ИПТ РУТ
(МИИТ)

Рецензенты:

Шарапова Л.В.

– зав. кафедрой Информационных
технологий и естественнонаучных
дисциплин АНО РОСНОУ

Поворотова Е.В. –

– преподаватель МКЖТ ИПТ РУТ (МИИТ)

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля

ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Специальности 09.02.02 Компьютерные сети

Программа профессионального модуля ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ предназначена для реализации государственных требований к уровню подготовки выпускников по специальности среднего профессионального образования 09.02.02 Компьютерные сети. Данный ПМ.03 может способствовать в части освоения основного вида профессиональной деятельности (ВПД): Эксплуатация объектов сетевой инфраструктуры и соответствующих профессиональных компетенций.

Программа профессионального модуля составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования и нормативно-правового регулирования в сфере образования Министерства образования и науки Российской Федерации.


Программа содержит следующие элементы: титульный лист, паспорт (указана область применения программы, место профессионального модуля в структуре основной образовательной программы, цели и задачи, объем учебной дисциплины и виды учебной работы); тематический план и содержание учебной дисциплины, условия реализации программы (требования к минимальному материально-техническому обеспечению, перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы); контроль и оценка результатов освоения учебной дисциплины.

Перечень компетенций (ОК и ПК) содержит все компетенции, указанные в ФГОС по специальности. Требования к практическому опыту, умениям и знаниям соответствуют перечисленным в ФГОС

Программа рассчитана на 820 часов, из которых 36% учебных занятий отводится на практические и лабораторные занятия. Самостоятельная работа составляет 30% учебного времени, спланированы ее тематика, виды и формы в каждом разделе.

Содержание программы направлено на достижение результатов, определяемых ФГОС по специальности 09.02.02 Компьютерные сети. Содержание отражает последовательность формирования знаний. В полной мере отражены виды работ, направленные на приобретение умений.

Программа может быть рекомендована для использования в образовательном процессе

Рецензент  Л.В.Шарапова

подпись, Ф.И.О.

Занимаемая должность: *зав.каф. Информационных технологий и естественно-научных дисциплин АНО ВО «РосНОУ»*

М.П.



РЕЦЕНЗИЯ

на рабочую программу профессионального модуля ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Специальности 09.02.02 Компьютерные сети

Программа профессионального модуля ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ предназначена для реализации государственных требований к уровню подготовки выпускников по специальности среднего профессионального образования 09.02.02 Компьютерные сети. Данный ПМ.03 может способствовать в части освоения основного вида профессиональной деятельности (ВПД): Эксплуатация объектов сетевой инфраструктуры и соответствующих профессиональных компетенций.

Программа профессионального модуля составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования и нормативно-правового регулирования в сфере образования Министерства образования и науки Российской Федерации.

Программа содержит следующие элементы: титульный лист, паспорт (указана область применения программы, место профессионального модуля в структуре основной образовательной программы, цели и задачи, объем учебной дисциплины и виды учебной работы); тематический план и содержание учебной дисциплины, условия реализации программы (требования к минимальному материально-техническому обеспечению, перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы); контроль и оценка результатов освоения учебной дисциплины.

Перечень компетенций (ОК и ПК) содержит все компетенции, указанные в ФГОС по специальности. Требования к практическому опыту, умениям и знаниям соответствуют перечисленным в ФГОС

Программа рассчитана на 820 часов, из которых 36% учебных занятий отводится на практические и лабораторные занятия. Самостоятельная работа составляет 30% учебного времени, спланированы ее тематика, виды и формы в каждом разделе.

Содержание программы направлено на достижение результатов, определяемых ФГОС по специальности 09.02.02 Компьютерные сети. Содержание отражает последовательность формирования знаний. В полной мере отражены виды работ, направленные на приобретение умений.

Программа может быть рекомендована для использования в образовательном процессе

Преподаватель МКЖТ ИПТ РУТ (МИИТ)



Е.В.Поворотова

СОДЕРЖАНИЕ

| | |
|---|----|
| 1.Паспорт рабочей программы профессионального модуля..... | 4 |
| 2.Результаты освоения профессионального модуля..... | 7 |
| 3.Структура и примерное содержание профессионального модуля..... | 9 |
| 4.Условия реализации программы профессионального модуля..... | 23 |
| 5. Контроль и оценка результатов освоения профессионального модуля..... | 28 |

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ Эксплуатация объектов сетевой инфраструктуры

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля (далее программа) – является частью основной профессиональной образовательной программы - программы подготовки специалистов среднего звена.

Программа разработана в соответствии с ФГОС по специальности СПО **09.02.02 Компьютерные сети** в части освоения основного вида профессиональной деятельности (ВПД): Эксплуатация объектов сетевой инфраструктуры и соответствующих профессиональных компетенций (ПК):

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

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

ПК 3.3 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.

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. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – **820** часов, в том числе:

максимальной учебной нагрузки обучающегося – **640** часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 433 часов,
в том числе:

практических занятий – 62 часа

лабораторных занятий – 58 часов

самостоятельной работы обучающегося – 207 часов;

курсовое проектирование (вариативная часть) - 30 часов;

производственной практики – 180 часов.

1.4 Использование часов вариативной части профессионального модуля:

| № | Профессиональные компетенции | Дополнительные знания, умения, практический опыт | № МДК | Количество часов | Обоснование включения в РП |
|---|------------------------------|--|---|------------------|--|
| | | | МДК 03.01. Эксплуатация объектов сетевой инфраструктуры | 31 | |
| | ПК 3.1- ПК 3.2 | 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 | МДК 03.02. Безопасность функционирования информационных систем (Курсовое проектирование) | 22 | Формирование навыков по составлению технической документации |
| | ПК.3.3- ПК.3.6 | Иметь практический опыт: Использования инструментальных средств для эксплуатации сетевых конфигураций Уметь: формализовать процессы технологической поддержки Знать: принципы эффективной организации работы подразделений технической поддержки пользователей | МДК 03.03 Автоматизированные информационные системы на железнодорожном транспорте | 135 | Формирование навыков эксплуатации сетевых конфигураций |

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) Эксплуатация 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 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. практические занятия, часов | в т. ч. лабораторные работы, 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 | 11 |
| ПК 3.1., ПК 3.2. ПК 3.3 ПК 3.4.ПК 3.5. ПК 3.6. | МДК 03.01 Эксплуатация объектов сетевой инфраструктуры | 275 | 178 | 34 | 26 | - | 97 | - | | |
| ПК 3.1-3.2 | МДК 03.02. Безопасность функционирования информационных систем | 230 | 164 | 28 | 12 | 30 | 66 | 30 | - | |
| ПК 3.3- ПК 3.6 | МДК 03.03. Автоматизированные информационные системы на железнодорожном транспорте | 135 | 44 | | 20 | | 44 | | - | - |
| | Производственная практика (по профилю специальности), часов | 180 | | | | | | | | 180 |
| | Всего: | 640 | 433 | 62 | 58 | 30 | 207 | | | 180 |

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.03. Эксплуатация объектов сетевой инфраструктуры | | 275 | |
| МДК 03.01 Эксплуатация объектов сетевой инфраструктуры | | 208 | |
| Введение | Объекты сетевой инфраструктуры и их эксплуатация | 2 | |
| Раздел 1. Эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей. | | 28 | |
| Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры | Содержание | 18 | |
| 1. | Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети; активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки. | | 2 |
| 2. | Структурированные кабельные системы, определение и назначение. Стандарты и категории. Типовые работы по монтажу. | | 3 |
| 3. | Кабель – канал, коммутационная панель, классификация коммутационных панелей. Кабели для СКС. Структурированное кабельное решение. Power over Ethernet (PoE). Преобразователь среды Fast Ethernet | | 1 |
| 4. | Логические (информационные) аспекты эксплуатации. Несанкционированное ПО (в том числе сетевое); паразитная нагрузка. | | 1 |
| 5. | 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. | | |
| | 6. | Сети отделов, кампусов и корпораций. Требования, предъявляемые к вычислительным сетям. | | |
| | 7. | Наращивание длины сегментов сети; замена существующей аппаратуры (на более мощную). Увеличение количества узлов сети; Увеличение протяженности связей между объектами сети. | | 1 |
| | 8. | Техническая и проектная документация. Паспорт технических устройств; руководство по эксплуатации; | | 1 |
| | 9. | Физическая карта всей сети; логическая схема компьютерной сети | | 1 |
| | Лабораторные работы | | 6 | |
| | 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. | | |
| | Практические занятия | | 4 | |
| | 1. | Оформление технической документации, правила оформления документов. | | |
| | 2. | Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain. | | |
| | 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; | | 12 | |

| | | | |
|---|--|-----------|---|
| Раздел 2. Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях. | | 30 | |
| Тема 2.1 Профилактические работы | Содержание | 10 | 2 |
| | 1. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры | | 3 |
| | 2. Комплекс организационно-технических мероприятий; выявление и своевременная замена элементов инфраструктуры. | | 2 |
| | 3. Проверка объектов сетевой инфраструктуры и профилактические работы Проверка физических компонентов; проверка документации и требований; проверка списка совместимого оборудования. | | 2 |
| | 4. Проведение регулярного резервирования Обслуживание физических компонентов. | | 2 |
| | 5. Контроль состояния аппаратного обеспечения; организация удаленного оповещения. | | 2 |
| | Лабораторные работы | 6 | |
| | 1. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств. | 14 | |
| | Практические занятия | | 1. Подсчет времени двойного оборота для заданной конфигурации коллизийного домена (4ч). |
| | 2. Выполнение монтажных работ с коаксиальным кабелем и витой парой (4ч). | | |
| 3. Выполнение монтажных работ с оптоволоконным кабелем (6ч). | | | |
| Самостоятельная работа обучающихся по разделу 1: 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 оборудования, методы резервирования, программы для резервирования информации, BackUp. Маршрутизация в Windows Server 2008; Управление общими свойствами IP-маршрутизации; Основные сведения о NAT; Различие между NAT и ICS; Удаленный доступ по телефонной линии; Авторизация подключений удаленного доступа. | 6 | | |

| | | | | |
|---|---|--|----|--|
| Раздел 3. Эксплуатация сетевых конфигураций. | | 54 | | |
| Тема 3.1 Управление сетями | Содержание | | 22 | |
| | 1. | Архитектура системы управления. Архитектура в концепции TMN; централизованное управление; децентрализованное управление. | 2 | |
| | 2. | Структура системы управления; Централизованное управление; децентрализованное управление. | 2 | |
| | 3. | Уровни управления Многоуровневая архитектура управления TMN: бизнесом; услугами; сетью; элементами сети; уровень элементов сети. | 2 | |
| | 4. | Области управления. Области управления ошибками; конфигурацией; доступом; производительностью; безопасностью. | 2 | |
| | 5. | Протоколы управления. SNMP; CMIP. | 2 | |
| | 6. | Протоколы управления. TMN; LNMP; ANMP. | 3 | |
| | 7. | Управление отказами. Выявление, определение и устранение последствий сбоев и отказов в работе сети. | 3 | |
| | 8. | Учет работы сети Регистрация, управление используемыми ресурсами и устройствами; | 2 | |
| | 9. | Управление конфигурацией Конфигурирование компонентов сети, сетевые адреса и идентификаторы. Управление параметрами сетевых операционных систем. | 2 | |
| | 10. | Управление производительностью, безопасностью сети. Статистика работы сети в реальном времени, минимизации заторов и узких мест, | 3 | |
| | 11. | Выявления складывающихся тенденций и планирования ресурсов для будущих нужд; Контроль доступа, сохранение целостности данных и журналирование. | 3 | |
| | Лабораторные работы | | 6 | |
| | 1 | Анализ сетевого трафика средствами Сетевого монитора | | |
| 2 | Основные сведения о сетевом мониторе Запись данных средствами Сетевого монитора | | | |
| 3 | Устранение неполадок с помощью Ping и PathPing Диагностика сети и Netdiag | | | |

| | | | | |
|--|--|---|---|--|
| | Практические занятия | 6 | | |
| 1 | Удаленное администрирование; | | | |
| 2 | Восстановление работоспособности сетевой инфраструктуры. | | | |
| 3 | Авторизация подключений удаленного доступа | | | |
| Тема 3.2 Средства мониторинга и анализа локальных сетей | Содержание | 12 | 2 | |
| | 1. | | | Анализаторы протоколов Программные или аппаратно-программные системы, функции мониторинга, анализ трафика в сетях. |
| | 2. | | | Оборудование для диагностики и сертификации кабельных систем Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры. |
| | 3. | | | Экспертные системы Выявление причин аномальной работы сетей; возможные способы приведения сети в работоспособное состояние. |
| | 4. | | | Встроенные системы диагностики и управления. Средняя интенсивность общего трафика сети, средняя интенсивность потока пакетов с определенным типом ошибки. |
| | 5. | | | Сетевые мониторы Программно-аппаратный модуль, установленный в коммуникационное оборудование, программный модуль, встроенный в операционные системы. |
| | 6. | | | Удаленное управление элементами сети. Программа — Telnet |
| | | Лабораторные работы | 4 | |
| | 1 | Вкладка. Сеть утилиты. Диспетчер задач | | |
| | 2 | Использование консоли. Производительность | | |
| | | 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. Примерная тематика внеаудиторной самостоятельной работы: Основные сведения о политиках удаленного доступа Устранение неполадок при подключениях удаленного доступа Реализация процедур безопасного администрирования сети | | 32 | | |

| | | | |
|---|---|-----------|---|
| <p>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;</p> | | | |
| Раздел 4. Схемы послеаварийного восстановления работоспособности компьютерной сети. | | 28 | |
| Тема 4.1 Хранение информации | Содержание | 6 | 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 действие OLAP. Реализации OLAP | | 2 |
| | | | 3 |
| | Лабораторные работы | 4 | |
| | 1. Операции по резервному копированию данных; | | |
| | 2. Операции по восстановлению данных. | | |
| | Практические занятия | 6 | |
| | 1. Организации по бесперебойной работе системы по резервному копированию | | |
| 2. Восстановление информации | | | |
| 3. Возврат к нормальному функционированию системы | | | |
| Тема 4.2 Схема после аварийного восстановления | Содержание | 12 | |
| | 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. Основные требования к политике организации схемы послеаварийного восстановления | | 2 |
| | 4. Организация работ по восстановлению функционирования системы | | 3 |
| | 5. План восстановления системы. Порядок уведомления о чрезвычайных событиях. | | 2 |
| | 6. Активация. Возврат к нормальному функционированию системы. | | 2 |
| 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: | | 24 | |

| | | | | |
|--|---|-----------|--|---|
| 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) | | | | |
| Раздел 5. | Замена расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры. | 36 | | |
| Тема 5.1. Диагностика неисправностей технических средств и сетевой структуры | Содержание | 36 | | |
| | 1. | | Принципы локализации неисправностей. Логический подход. | 3 |
| | 2. | | 6 этапов процедуры поиска и устранения неисправности | 3 |
| | 3. | | Этапы 1 – 3. Выявление признаков неисправности. Углубленный анализ признака неисправности. | 3 |
| | 4. | | Составление перечня возможных неисправных функций | 2 |
| | 5. | | Этапы 4 – 6. Локализация неисправной функции. Локализация неисправности в схеме. | 2 |
| | 6. | | Анализ отказов | 3 |
| | 7. | | Отыскание неисправностей в устройствах на ИС | 2 |
| | 8. | | Контрольно-измерительная аппаратура | 3 |
| | 9. | | Сервисные платы и комплексы | 3 |
| | 10. | | Номенклатура и особенности работы тест-программ. | 2 |
| | 11. | | Программные средства диагностики. | 2 |
| | 12. | | Диагностика неисправностей средств сетевых коммуникаций | 3 |
| | 13. | | Контроль функционирования аппаратно-программных комплексов. | 3 |
| | 14. | | Действия при не работающей сети, при медленной сети | 3 |
| | 15. | | Действия при не стабильно работающей сети. | 2 |
| | 16. | | Определение устаревшего оборудования и программных средств сетевой инфраструктуры | 2 |
| 17. | Программная и аппаратная совместимость при замене устаревшего оборудования новым. | 3 | | |
| Дифференцированный зачет | | 2 | | |
| 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, | | 23 | | |

| | | |
|---|--|--|
| <p>оформление лабораторно-практических работ, отчетов и подготовка к их защите.</p> <p>Примерная тематика внеаудиторной самостоятельной работы:</p> <p>Поиск неисправностей по принципу локализации неисправностей конкретного оборудования;</p> <p>Изучить и понять принцип работы новых контрольно-измерительных аппаратов</p> | | |
|---|--|--|

| 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 6. | Безопасность функционирования информационных систем | 230 | |
| МДК 03.02. Безопасность функционирования информационных систем | | 164 | |
| Введение | Информационная безопасность и технологии защиты информации | 2 | |
| Тема 1.1 Основы информационной безопасности | Содержание | 22 | 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. | | 3 |

| | | | |
|---|--|----|---|
| | Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита» | | |
| | Практические занятия | 8 | |
| | 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 1.2. Проблемы информационной безопасности. | Содержание | 12 | 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 |
| | Лабораторные работы | 6 | |
| | 1. Система анализа рисков проверки политики информационной безопасности предприятия. | | |
| | 2. Анализ угроз сетевой безопасности. | | |
| 3. Обеспечение информационной безопасности сетей. | | | |
| | Практические занятия | 6 | |
| | 1. Этапы сетевой атаки. Исследование сетевой топологии. | | |
| | 2. Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы | | |
| | 3. Реализации атак. Выявление атаки на протокол SMB. | | |

| | | | | |
|---|---|--|---|---|
| Тема 1.3. Технологии защиты данных. | Содержание | | 4 | 2 |
| | 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 | Криптографические алгоритмы. Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы. | | |
| | 3 | Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя. | | |
| | Лабораторные работы | | | |
| 1 | Изучение стандарта криптографической защиты AES (Advanced Encryption Standart). | -4 | | |
| 2 | Изучение отечественных стандартов хэш-функции и цифровой подписи. | | | |
| Раздел 2 | | | | |
| Тема 2.1 | | | | |
| Криптографическая защита информации | | | | |
| Тема 2.2. Технологии защиты межсетевого обмена данными. | | | | |
| Содержание | | 12+10 | | |
| 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. | | | 2 |

| | | | |
|---|--|---|-----|
| | Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол управления криптоключами IKE. Особенности реализации средств IPSec. | | |
| 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 | | 18-2 | |
| 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. | | |
| 8. | Организация VPN средствами СЗИ StrongNet. Защита на транспортном уровне | | |
| 9. | Организация VPN средствами протокола SSL в Windows Server | | |
| Тема 2.3. Технологии обнаружения вторжений. | Содержание | 4+12 | |
| | 1 | Анализ защищенности и обнаружение атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак. | 1 |
| | 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 | | 6-2 |
| 1. | Сигнатурный анализ и обнаружение аномалий | | |
| 2. | Обнаружение в реальном времени и отложенный анализ. Локальные и сетевые | | |

| | | | |
|---|---|------------|--|
| | системы обнаружения атак | | |
| 3. | Распределенные системы обнаружения атак. Система обнаружения атак Snort. | | |
| <p>Самостоятельная работа при изучении раздела</p> <p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).</p> <p>Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите.</p> <p>Примерная тематика внеаудиторной самостоятельной работы:</p> <p>Подготовка индивидуального задания по теме «Аудит информационной безопасности компьютерных систем». Выполнение домашнего задания и сдача разделов по курсовой работе в рамках дисциплины. Работы по сбору, сортировке и подготовке необходимого информационного материала, организации опытно-экспериментальной и исследовательской работы; анализа и обобщения, а также написание и оформление курсовой работы.</p> <p>Примерная тематика курсовых работ (проектов)</p> <ol style="list-style-type: none"> 1. Разработка политики информационной безопасности. 2. Защита информации при использовании электронной почты. 3. Организация защиты персональных данных в организации 4. Анализ безопасности средств удаленного доступа. 5. Анализ среды передачи данных в вычислительных сетях. 6. Анализ и оптимизация приемов администрирования локальной вычислительной сети и мер по устранению сбоев в работе сети применяемых в организации .5. Выработка и реализация сетевой политики, настройка телекоммуникационного оборудования локальной вычислительной сети рекламной компании. 7. Анализ требований заказчика и проектирование компьютерных сетей <p>Обязательная аудиторная учебная нагрузка по курсовой работе (проекту)</p> <ol style="list-style-type: none"> 1. Обеспечение внутренней безопасности сети. 2. Распределение прав доступа к внутренним ресурсам сети для разных групп пользователей. 3. Организация работы с ресурсами внешней сети (Интернет). 4. Распределение прав доступа пользователей к внешней сети. 5. Выбор средств обеспечения безопасности подключения к внешней сети. 6. Способы мониторинга устройств, пользователей. 7. Технологии поиска неисправностей. 8. Подбор соответствующего программного обеспечения. 9. Описание настроек рабочих станций и серверов. 10. Распределение сетевых адресов по хостам сети. | | 96 | |
| Раздел 7. Автоматизированные информационные системы на железнодорожном транспорте | | 135 | |
| МДК 03.03. Автоматизированные информационные системы на железнодорожном транспорте | | 91 | |
| Тема 3.1 АСУ ЖТ и перспективы развития | Роль информатизации в работе транспорта. Информация и информационные системы. Основные понятия в области информатизации. Автоматизированные информационные системы. Информационные технологии | 10 | |
| | Информационные системы ЖТ по реализации процессов, связанных: со сбором, | | |

| | | | |
|--|---|-----------|--|
| | хранением и классификацией больших объемов информации; с ведением информационных массивов сложной внутренней структуры и их подготовкой для последующей обработки; с логической обработкой данных при решении задач информационного характера; с выдачей информации, пригодной для непосредственного использования человеком. | | |
| | Функциональная структура ИСЖТ как совокупность четырех комплексов информационных технологий. Базовые функции информационных систем и основные внешние связи между ними. Интеграция автоматизированных комплексов и систем. | | |
| Тема 3.2 Информационно-управляющие системы ЖТ | Управление в информационной системе. Методология создания и экономическая оценка информационной системы железнодорожного транспорта. Системы статистического учета и отчетности, их функционирование. Принципы построения автоматизированной системы продажи и учета мест в поездах, а также управления пассажирскими перевозками («Экспресс»). Методы проектирования и внедрения. Структура системы и перспективы развития | 14 | |
| | Практические работы Анализ работы АСУ «Экспресс-3» Обеспечивающие и функциональные подсистемы. Решаемые задачи и перспективы развития программно-технического комплекса системы | 6 | |
| Тема 3.3 Автоматизированные системы оперативного управления перевозками | Автоматизированная система оперативного управления грузовыми перевозками (АСОУП), ее вычислительные и телекоммуникационные средства. Трехуровневая структура построения АСОУП. Требования к системам и методам внедрения. Перспективы развития системы АСОУП. СИРИУС - сетевая интегрированная Российская информационно-управляющая система. ГИД УРАЛ | 27 | |
| | Практические работы Анализ работы АСОУП Анализ функционирования сетевых подсистем ДИСПАРК Анализ системы ЕК АСУ ФР | 10 | |
| Тема 3.4 Электронный документооборот на ЖТ | Система фирменного транспортного обслуживания (СФТО). ЭТРАН – автоматизированная система централизованной подготовки и оформления перевозочных документов. Единый комплекс управления финансовой деятельностью ЕК АСУ ФР | 4 | |
| | Практические работы Анализ работы АС ЭТРАН | 4 | |
| Тема 3.5 Архитектурные решения на базе | Архитектура ИС. Функциональная структура ИС: технологические процессы на транспорте, представленные в виде трехуровневых, связанных между собой, бизнес- | 10 | |

| | | | |
|--|--|-------------------|--|
| <p>аппаратных платформ IBM</p> | <p>процессов сетевого, дорожного и линейного уровней управления. Архитектура баз данных: вычислительные и телекоммуникационные средства (техника и системное прикладное обеспечение); распределенная вычислительная среда, обеспечивающую создание единой территориально распределенной и безопасной вычислительной системы; основные системы обеспечения: безопасности, управления вычислительными ресурсами, конфигурации и архивации.</p> | | |
| <p>Самостоятельная работа при изучении раздела 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.</p> | | <p>44</p> | |
| <p>Производственная практика (по профилю специальности) ПП.03 Виды работ: Использование активного оборудования сети. Использование пассивного оборудования сети. Устранение паразитирующей нагрузки в сети. Заполнение технической документации. Построение физической карты локальной сети. Работа по созданию, редактированию, удалению пользователей в DOMAIN. Регламенты технических осмотров. Профилактические работы в объектах сетевой инфраструктуры. Мониторинг и анализ сети с помощью программных и аппаратных средств Структура системы управления, архитектура системы управления. Управление областями сети: ошибками, конфигурацией, доступом, производительностью, безопасностью. Работа с протоколами SNMP; CMIP; TMN; LNMP; ANMP. Отслеживание работы сети. Работа с сервером, чтение логов, работа над ошибками Работа с сервером. Контроль доступа, сохранение целостности данных и журналирование. Удаленное администрирование рабочих станций с сервера Удаленное администрирование сервера с рабочих станций, программы для удаленного доступа. Анализ трафика сети. Работа с кабельными сканерами и тестерами. Работа со встроенными сканерами диагностики и управления. Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных таблиц.</p> | | <p>180</p> | |

| | | |
|---|------------|--|
| <p>Восстановление сети после сбоя. Создание плана восстановления сети. Использование в работе контрольно-измерительной аппаратуры, сервисных плат, комплексов. Разработка функциональных схем элементов автоматизированной системы защиты информации. Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование. Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации. Разработка политик безопасности и внедрение их в операционные системы. Настройка IPSec и VPN. Настройка межсетевых экранов. Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств. Настройка защиты беспроводных сетей с помощью систем шифрования. Архивация и восстановление ключей в Windows Server (PKI). Установка и настройка системы обнаружения атак Snort.</p> | | |
| Всего | 640 | |

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».

Лаборатория оборудована рабочим местом преподавателя и рабочими места учеников 12 компьютеров:

- 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 «Эксплуатации объектов сетевой инфраструктуры».

Междисциплинарный курс МДК 03.01 «Эксплуатация сетевой инфраструктуры» реализуется в **Лаборатории «Эксплуатации объектов сетевой инфраструктуры».**

Минимально необходимое материально-техническое обеспечение включает в себя:

- Рабочие места по количеству обучающихся (стол, стулья аудиторные);
- Оборудованное рабочее место преподавателя (стол, кресло, персональный компьютер, локальная сеть с выходом в Internet
- Доска меловая
- Шкафы-стеллажи для размещения учебно-наглядных пособий и документации;
- Стенды
-

Компьютер 2x Intel CPU 1,8 GHz (15 шт.). Монитор ЭЛТ (15 шт.). Коммутатор -CISCO-1700.

Типовой набор инструментов наладки компьютерной сети, кабели различного типа, тестеры для кабеля

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 – Eugene 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/>
13. Nessus, источник – <http://www.nessus.org>

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Осипенко, А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт [Текст]: Монография / А.Л. Осипенко. — М.: Норма, 2006. — 432 с.; 21 см. 3000 экз. — ISBN 5-89123-817-9
2. 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
3. Компьютерные сети. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки [Текст] : [пер. с англ.] — 2-е изд., испр. и доп. / Корпорация Майкрософт. — М. : Русская редакция, 2007. — 576 с. : ил. ; 24 см. + 1 электрон. опт. диск. — 3000 экз. — ISBN 5-7502-0101-5 (в пер.)
4. Уилсон, Э. Мониторинг и анализ сетей. Методы выявления неисправностей [Текст] : [пер. с англ.] / Эд Уилсон. — М.: ЛОРИ, 2006. — 350 с. : ил. ; 24 см. — Перевод. изд.: Network monitoring and analysis. A protocol approach to troubleshooting / Ed Wilson. — 3200 экз. — ISBN 5-85582-163-3 (в пер.)
5. 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.)
6. 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

Дополнительные источники:

1. Корт, С. С. Теоретические основы защиты информации [Текст] : учеб. пособие 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 профессионалов [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). University of Illinois, 2005. – 13 с. ; 30 см.
6. Kazienko, P. Intrusion Detection Systems (IDS). Part I, II [Электронный ресурс] / 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. Толстой. — М.: Горячая линия–Телеком, 2005. — 249 с. ; 20 см. — 3000 экз. — ISBN 5-93517-139-2
9. Медведевский, И.Д. Атака на Internet [Текст] / И.Д. Медведевский, 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 преступлений [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. Бигелу 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 обучения.

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 |
|--|---|---|
| ПК 3.1 Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей | <ul style="list-style-type: none"> – 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. | <p>Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы</p> <ul style="list-style-type: none"> - на практических занятиях, - при решении ситуационных задач, - при выполнении определенных видов работ производственной практики, - зачет по разделу практики |
| ПК 3.2 Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях | <ul style="list-style-type: none"> – 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. | <p>Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы</p> <ul style="list-style-type: none"> - на практических занятиях, - при выполнении определенных видов работ производственной практики, - зачет по разделу практики |
| ПК 3.3 Осуществлять эксплуатацию сетевых конфигураций | <ul style="list-style-type: none"> – точность и скорость настройки сети; – качество анализа и рациональность выбора сетевых конфигураций; – выбор способов настройки и технологически грамотное назначение технологической базы | <p>Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы</p> <ul style="list-style-type: none"> - на практических занятиях, - при выполнении |

| | | |
|--|--|---|
| | | определенных видов работ производственной практики, - зачет по разделу практики |
| ПК 3.4 Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации | – выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов | Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, - при решении ситуационных задач, - при выполнении определенных видов работ производственной практики, - зачет по разделу практики |
| ПК 3.5 Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования | – выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов | Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, - зачет по разделу практики |
| ПК 3.6 Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять 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 Междисциплинарн ый экзамен |
|--|--|---|

Формы и методы контроля и оценки результатов обучения должны позволить проверить 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 |
|--|---|---|
| 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 индивидуальных проектов.) - при выполнении и защите курсовой работы (проекта); - при выполнении работ на различных этапах производственной практики по профилю специальности |
| 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 | |