МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СВЕРДЛОВСКОЙ ОБЛАСТИ КАМЫШЛОВСКИЙ ТЕХНИКУМ ПРОМЫШЛЕННОСТИ И ТРАНСПОРТА

СОГЛАСОВАНО:
руководителем рабочей группы
_____ / Потапова О.А
Пр. № 1 от «26» августа 2015 г.

УТВЕРЖДАЮ:
директор ГАПОУ СО «Камышловский техникум промышленности и транспорта»
_____ / Потапова З.А. /
М.П.
от «26» 08 2015 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

по программе подготовки квалифицированных рабочих (служащих)
09.01.02. Наладчик компьютерных сетей

Программа разработана:
Потаповой О.А. преподавателем
спецдисциплин 1 КК

Камышлов
2015

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по программе подготовки квалифицированных рабочих (служащих):

09.01.02. Наладчик компьютерных сетей

Содержание программы реализуется в процессе освоения студентами программы подготовки квалифицированных рабочих (служащих) с получением среднего общего образования, разработанной в соответствии с требованиями ФГОС СПО третьего поколения.

Организация-разработчик: ГАПОУ СО «Камышловский техникум промышленности и транспорта», юридический адрес: Свердловская область, г. Камышлов, ул. Энгельса,167.
тел. 8(34375) 2-45-32, e-mail: pl-16kam-v@mail.ru.

Разработчик (и):
Потапова Ольга Александровна преподаватель спецдисциплин 1 КК

Программа согласована с научно-методическим советом (НМС) ГАОУ СПО СО «Камышловский техникум промышленности и транспорта» и рекомендована к использованию в образовательном процессе.
Протокол НМС № _1_ от «_26__ » __августа_ 2015г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Область применения программы

Рабочая программа профессионального модуля – является частью программы подготовки квалифицированных рабочих (служащих) в соответствии с ФГОС СПО по профессии 09.01.02. Наладчик компьютерных сетей

Рабочая программа профессионального модуля может быть использована для подготовки Студентов по направлению подготовки 09.00.00 Информатика и вычислительная техника в части освоения основного вида профессиональной деятельности (ВПД):

- Обеспечение информационной безопасности компьютерных сетей и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Обеспечивать резервное копирование данных.

ПК 3.2. Осуществлять меры по защите компьютерных сетей от несанкционированного доступа.

ПК 3.3. Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.

ПК 3.4. Осуществлять мероприятия по защите персональных данных.

Программа профессионального модуля может быть использована при профессиональной подготовке и переподготовке квалифицированных рабочих (служащих) по профессии «Наладчик компьютерных сетей» для среднего (полного) общего , профессионального образования, с опытом работы на предприятиях отрасли связи, отделах и участках по обеспечению информационными технологиями предприятий разных форм собственности, электромонтеры связи и линейно-кабельных сооружений без учета стажа работы

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

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

иметь практический опыт:

обеспечения информационной безопасности компьютерных сетей, резервного копирования и восстановления данных; установки, настройки и эксплуатации антивирусных программ; противодействия возможным угрозам информационной безопасности

уметь:

обеспечивать резервное копирование данных; осуществлять меры по защите компьютерных сетей от несанкционированного доступа; применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами; осуществлять мероприятия по защите персональных данных; вести отчетную и техническую документацию;

знать:

виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них; аппаратные и программные средства резервного копирования данных; методы обеспечения защиты компьютерных сетей от несанкционированного доступа; специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами; состав мероприятий по защите персональных данных.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение студентами видом профессиональной деятельности обеспечение информационной безопасности компьютерных сетей, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1.	Обеспечивать резервное копирование данных
ПК 3.2.	Осуществлять меры по защите компьютерных сетей от несанкционированного доступа
ПК 3.3.	Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами
ПК 3.4.	Осуществлять мероприятия по защите персональных данных
ОК 1.	Понимать сущность и социальную значимость будущей профессии, проявлять к ней устойчивый интерес
ОК 2.	Организовывать собственную деятельность, исходя из цели и способов ее достижения, определенных руководителем
ОК 3.	Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы
ОК 4.	Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6.	Работать в команде, эффективно общаться с коллегами, руководством, клиентами
ОК 7.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

3. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Объем профессионального модуля и виды учебной работы

ПК	Наименования междисциплинарных курсов	Всего часов *(макс. учебная нагрузка и практики)*	Объем времени, отведенный на освоение междисциплинарного курса (курсов)				
			Обязательная аудиторная учебная нагрузка студента			Самостоятельная работа студента	
			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**
1	**МДК 03.01.** Информационная безопасность персональных компьютеров и компьютерных сетей	**82**	**55**	**25**	-	**27**	**-**
2	**Учебная практика**	**-**	**36**	**36**	**-**	**-**	**-**
3	**Производственная практика (по профилю специальности)**, часов *(если предусмотрена итоговая (концентрированная) практика)*	**-**	**468**	**468**	**-**	**-**	**-**
4	**Всего:**	**82**	**559**	**529**	**-**	**27**	**-**

3.2 Тематический план
профессионального модуля ПМ.03. Обеспечение информационной безопасности компьютерных сетей по программе подготовки квалифицированных рабочих (служащих)

09.01.02. Наладчик компьютерных сетей

3 курс , группа Н-355

(курс, группа)

МДК.03.01. Информационная безопасность персональных компьютеров и компьютерных сетей

Основания: ФГОС по ОПОП 09.01.02. Наладчик компьютерных сетей

№п\п	Наименование темы, раздела	Аудиторное количество часов	Из них часов на лабораторные, практические работы	Количество часов самостоятельной работы
Раздел 1. Информационная безопасность как часть инфраструктуры		**16**	**6**	
1.1	Сущность информационной безопасности	1		
1.2	Причины обострения проблемы обеспечения безопасности информационных технологий	1		
1.3	Классификация и виды средств информационной безопасности	2	*1*	
1.4	Виды мер и основные принципы информационной безопасности	2	*1*	
1.5	Правовые основы обеспечения информационной безопасности	2		
1.6	Сертификация и аттестация средств защиты информации. Электронная цифровая подпись	2	1	
1.7	Угрозы информационной безопасности и их краткая характеристика	2	1	
1.8	Настройка и администрирование сети. Возможные угрозы ее функционирования	2	1	
1.9	Возможные угрозы работы операционной системы и качественная характеристика путей их устранения	2	1	
Сам. работа	*Оформление сообщения по теме:* Причины обострения проблемы обеспечения безопасности информационных технологий			*2*
	Оформление электронной презентации по теме: Правовые основы обеспечения информационной безопасности **(**Сертификация средств защиты и аттестация объектов информатизации, Юридическая значимость ЭЦП)			*4*
Раздел 2. Резервное копирование и восстановление данных		**12**	**9**	
2.1	Сущность и основные понятия резервного копирования и восстановления данных	1		
2.2	Классификация аппаратных и программных средств резервного копирования и восстановления данных	1	1	
2.3	Способы использования размещения резервных копий внутри локальных сетей и на FTP- серверах	1	1	
2.4	Способы сохранения резервных копий на любое usb-носители, резервное копирование на дискеты ZIP,JAZ,MO	1	1	
2.5	Полное, дифференциальное, инкрементное резервное копирование данных. Отличия и возможности.	3	2	
2.6	Схемы ротации резервного копирования и восстановления данных, их использование в производстве	1		
2.7	Клонирование данных и запись образов системы. Теневое клонирование	1	1	
2.8	Резервное копирование и восстановление данных с использованием аппаратных средств.	1	1	
2.9	Виды RAID-массивов, технология их составления	1	1	
2.10	Технологии «облачного резервного копирования».	1	1	

Сам. работа	*Оформление электронной презентации по теме*: Классификация аппаратных и программных средств резервного копирования и восстановления данных			*4*
	Составление алгоритма смены рабочего набора носителей в процессе копирования (3 вида)			*4*
Раздел 3. Стандарты информационной безопасности		**5**		
3.1	Роль стандартов информационной безопасности	1		
3.2	Международные стандарты информационной безопасности	1		
3.2.1	Международный стандарт ISO 15408	1		
3.2.2	Стандарты для беспроводных сетей	1		
3.2.3	Стандарты информационной безопасности в Интернете	1		
Сам. работа	*Оформление электронной презентации по теме*: Международные стандарты информационной безопасности			*2*
	Оформление электронной презентации по теме: Международный стандарт ISO 15408			*2*
	Оформление электронной презентации по теме: Стандарты для беспроводных сетей			*2*
Раздел 4. Обеспечение безопасности операционных систем		**4**	**1**	
4.1	Проблемы обеспечения безопасности ОС	1		
4.2	Угрозы безопасности ОС, Понятие защищенной ОС	1		
4.3	Архитектура подсистемы защиты ОС	1		
4.3.1	Основные функции подсистемы защиты ОС : идентификация, аутентификация	1	1	
Сам. работа	*Ответить на контрольные вопросы по теме*: Угрозы безопасности ОС			*2*
	Оформить отчет и ответить на контрольные вопросы по лабораторной работе на тему: Основные функции подсистемы защиты ОС			*1*
Раздел 5. Анализ защищенности и обнаружение атак		**8**	**4**	
5.1	Технология анализа защищенности	1		
5.1.1	Средства анализа защищенности сетевых протоколов и сервисов	1		
5.1.2	Средства анализа защищенности ОС	1	1	
5.2	Технологии обнаружения атак	2		
5.2.1	Методы анализа сетевой информации	1	1	
5.2.2	Классификация систем обнаружения атак IDS	1	1	
5.2.3	Методы реагирования	1	1	
Сам. работа	*Оформление электронной презентации по теме*: Средства анализа защищенности сетевых протоколов и сервисов			*2*
	Ответить на контрольные вопросы по теме: Технологии обнаружения атак.			*1*
Раздел 6. Защита от вирусов		**4**	**2**	
6.1	Компьютерные вирусы и проблемы антивирусной защиты	2		
6.1.1	Виды компьютерных вирусов	1	1	
6.1.2	Основные каналы распространения вирусов и других вредоносных программ	1	1	
Раздел 7. Методы управления средствами сетевой безопасности		**6**	**3**	
7.1	Архитектура управления средствами сетевой безопасности	1		
7.1.1	Концепция глобального управления безопасностью	1		
7.1.2	Глобальная и локальная политики безопасности	1		
7.1.3	Функционирование системы управления средствами безопасности	1	1	
7.2	Аудит и мониторинг безопасности	2	2	
Сам. работа	*Ответить на контрольные вопросы по теме:* Методы управления средствами сетевой безопасности			*1*
	ИТОГО	**55**	**25**	**27**

Тематический план
УП.03. Учебная практика
3 курс, группа Н-355

Основание: ФГОС по ОПОП 09.01.02. Наладчик компьютерных сетей
Составитель: / _____/ Потапова Ольга Александровна

№ п.п.	Тематический план учебной практики	Количество часов
1	**Вводное занятие. Охрана труда и техника безопасности в мастерской. Настройка рабочих станций в работу**	**3**
1.1	Охрана труда и техника безопасности в радиомастерской. Правила ведения работ. Проведение Инструктажей на рабочем месте (вводный, первичный).	1
1.2	Настройка периферийных устройств и рабочих станций локальной сети лаборатории	2
2	**Выполнение резервного копирования данных**	**18**
2.1	Организация хранения резервных копий внутри локальной сети. Запись резервных данных на любое USB-совместимое устройство, резервное копирование с помощью специализированного программного обеспечения	6
2.2	Выполнение операций по резервному копированию данных, создание образов и в режиме реального времени	6
2.4	Использование криптографических методов защиты данных. Обеспечение безопасности flash носителей	6
3	**Осуществление мер защиты компьютерных сетей и данных**	**12**
3.1	Обеспечение доступа к ресурсам сети (диски, папки, файлы). Организация начала сеанса на рабочей станции, работа с учетными карточками пользователей, отслеживание журнала событий безопасности.	6
3.2	Применение специализированного программного обеспечения для организации защиты компьютерных сетей	6
4	**Дифференцированный зачет**	**3**
	Всего по модулю:	**36**

Тематический план
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

№п.п	Наименование темы	Кол-во часов
1	**Вводный инструктаж. Первичный инструктаж на рабочем месте. Знакомство с оборудованием предприятия**	**4**
2	**Выполнение работ по монтажу локальных компьютерных сетей**	**64**
2.1	*Монтаж несущих компонентов для кабеля*	8
2.2	*Прокладка кабеля*	8
2.3	*Разделка кабеля*	8
2.4	*Строительно-монтажные работы при монтаже ЛКС*	8
2.5	*Монтажные работы по прокладке локальной сети для офиса*	32
3.	**Работы по подключению оборудования к локальной сети**	**80**
3.1	*Сборка и запуск в работу рабочих станций*	16
3.2	*Настройка операционной системы под пользователя*	16
3.3	*Подключение сетевого оборудования и принтера к ЛКС*	16
3.4	*Настройка доступа к общим ресурсам сети*	16
3.5	*Подключение серверов*	16
4	**Выполнение работ по эксплуатации и обслуживанию сетевого оборудования**	**56**
4.1	*Выполнение различных регламентных работ. (внешний осмотр элементов сети, проверка надежности крепления и установок)*	16
4.2	*Выполнение различных регламентных работ (удаление пыли и загрязнений, проверка герметичности соединений, чистка разъемов, визуальная проверка механических повреждений и следов коррозии.)*	16
4.3	*Выполнение различных регламентных работ (Чистка пылесосом внутренних объемов аппаратуры, Тестирование элементов сети, регулировка параметров настроек сетевого оборудования)*	16
4.4	*Настройка оборудования абонента (ПК, роутер).*	8
5.	**Работы по настройке системы регистрации и авторизации пользователей сети**	**48**

5.1	*Создание базы данных пользователей сети*	32
5.2	*Настройка системы регистрации пользователей*	16
6.	**Выполнение работ по подключению к глобальным компьютерным сетям.**	**104**
6.1	*Настройка и подключение к сети Интернет с пользователей*	16
6.2	*Настройка параметров подключения к сети Интернет*	16
6.3	*Установка программного обеспечения для обеспечения производственного процесса*	16
6.4	*Установка программного обеспечения для поддержки работоспособности сетевого оборудования и рабочих станций*	16
6.5	*Настройка браузеров*	8
6.6	*Обслуживание электронных почтовых ящиков, сайтов*	16
6.7	*Настройка программного обеспечения серверов.*	16
7.	**Обеспечение информационной безопасности компьютерных сетей.**	**112**
7.1	*Настройка и выполнение резервного копирования данных*	16
7.2	*Установка программного обеспечения для защиты от вредоносного ПО*	16
7.3	*Проверка рабочих станций и серверов на наличие вирусов и вредоносного программного обеспечения*	32
7.4	*Проверка электронных почтовых ящиков на наличие вирусов*	16
7.5	*Настройка учетных записей и паролей пользователей*	16
7.6	*Подключение общих сетевых ресурсов (дисков, папок), настройка доступа к файлам*	16
	Итого	**468**

3.3 Содержание профессионального модуля

Тема 1. Информационная безопасность как часть инфраструктуры

Сущность информационной безопасности. Причины обострения проблемы обеспечения безопасности информационных технологий. Классификация и виды средств информационной безопасности. Виды мер и основные принципы информационной безопасности. Правовые основы обеспечения информационной безопасности. Сертификация и аттестация средств защиты информации. Электронная цифровая подпись Угрозы информационной безопасности и их краткая характеристика. Настройка и администрирование сети. Возможные угрозы ее функционирования. Возможные угрозы работы операционной системы и качественная характеристика путей их устранения

Лабораторные и практические работы:

1. Практическая работа «Виды средств информационной безопасности»
2. Практическая работа «Меры информационной безопасности в локальных сетях»
3. Лабораторная работа «Исследование механизмов создания электронной цифровой подписи»
4. Практическая работа «Угрозы информационной безопасности»
5. Лабораторная работа «Настройка параметров информационной безопасности в локальной сети»
6. Практическая работа «Изучение возможных информационных угроз операционной системы»

Самостоятельная работа

Оформление сообщения по теме: Причины обострения проблемы обеспечения безопасности информационных технологий

Оформление электронной презентации по теме: Правовые основы обеспечения информационной безопасности (Сертификация средств защиты и аттестация объектов информатизации, Юридическая значимость ЭЦП)

Тема 2. Резервное копирование и восстановление данных

Сущность и основные понятия резервного копирования и восстановления данных. Классификация аппаратных и программных средств резервного копирования и восстановления данных. Способы использования размещения резервных копий внутри

локальных сетей и на FTP- серверах. Способы сохранения резервных копий на любое usb-носители, резервное копирование на дискеты ZIP,JAZ,MO. Полное, дифференциальное, инкрементное резервное копирование данных. Отличия и возможности. Схемы ротации резервного копирования и восстановления данных, их использование в производстве. Клонирование данных и запись образов системы. Теневое клонирование. Резервное копирование и восстановление данных с использованием аппаратных средств. Виды RAID-массивов, технология их составления. Технологии «облачного резервного копирования».

Лабораторные и практические работы:

1. Практическая работа « Использование аппаратных и программных средств резервного копирования и восстановления данных»
2. Лабораторная работа «Размещение резервных копий в локальной сети и на FTP-сервере»
3. Лабораторная работа «Резервное копирование на съемные носители»
4. Лабораторная работа «Выполнение резервного копирования с использованием стандартного и специализированного программного обеспечения»
5. Лабораторная работа «Клонирование данных и запись образов системы»
6. Лабораторная работа «Резервное копирование и восстановление данных с использованием аппаратных средств»
7. Практическая работа «Виды RAID-массивов, технология их составления»
8. Практическая работа «Технологии «облачного резервного копирования».

Самостоятельная работа:

Оформление электронной презентации по теме: Классификация аппаратных и программных средств резервного копирования и восстановления данных

Составление алгоритма смены рабочего набора носителей в процессе копирования (3 вида)

Тема 3. Стандарты информационной безопасности

Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Международный стандарт ISO 15408. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернете.

Самостоятельная работа

Оформление электронной презентации по теме: Международные стандарты информационной безопасности

Оформление электронной презентации по теме: Международный стандарт ISO 15408

Оформление электронной презентации по теме: Стандарты для беспроводных сетей

Тема 4. Обеспечение безопасности операционных систем

Проблемы обеспечения безопасности ОС. Угрозы безопасности ОС, Понятие защищенной ОС. Архитектура подсистемы защиты ОС. Основные функции подсистемы защиты ОС : идентификация, аутентификация.

Практические работы:

1. Практическая работа «Основные функции подсистемы защиты ОС : идентификация, аутентификация»

Самостоятельная работа

Ответить на контрольные вопросы по теме: Угрозы безопасности ОС

Оформить отчет и ответить на контрольные вопросы по лабораторной работе на тему: Основные функции подсистемы защиты ОС

Тема 5. Анализ защищенности и обнаружение атак

Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности ОС. Технологии обнаружения атак. Методы

анализа сетевой информации. Классификация систем обнаружения атак IDS. Методы реагирования

Практические работы:

1. Практическая работа «Виды анализа защищенности операционной системы»
2. Практическая работа « Использование методов анализа сетевой информации для защиты информации»
3. Практическая работа «Виды систем обнаружения атак»
4. Практическая работа « Изучение методов реагирования при обнаружении атак»

Самостоятельная работа:

Оформление электронной презентации по теме: Средства анализа защищенности сетевых протоколов и сервисов

Ответить на контрольные вопросы по теме: Технологии обнаружения атак.

Тема 6. Защита от вирусов

Компьютерные вирусы и проблемы антивирусной защиты. Виды компьютерных вирусов. Основные каналы распространения вирусов и других вредоносных программ

Практические работы:

1. Практическая работа « Виды компьютерных вирусов»
2. Практическая работа «Способы распространения вирусов и других вредоносных программ»

Раздел 7. Методы управления средствами сетевой безопасности

Архитектура управления средствами сетевой безопасности. Концепция глобального управления безопасностью. Глобальная и локальная политики безопасности. Функционирование системы управления средствами безопасности. Аудит и мониторинг безопасности

Лабораторные и практические работы:

1. Лабораторная работа «Методы управления средствами безопасности ЛКС»
2. Лабораторная работа « Проверка состояния персонального компьютера на наличие вредоносного программного обеспечения»

Самостоятельная работа:

Ответить на контрольные вопросы по теме: Методы управления средствами сетевой безопасности

Учебная практика:

Тема 1. Вводное занятие. Охрана труда и техника безопасности в мастерской.

Охрана труда и техника безопасности в радиомастерской. Правила ведения работ. Проведение Инструктажей на рабочем месте (вводный, первичный). Настройка периферийных устройств и рабочих станций локальной сети лаборатории

Тема 2. Выполнение резервного копирования данных

Организация хранения резервных копий внутри локальной сети. Запись резервных данных на любое USB-совместимое устройство, резервное копирование с помощью специализированного программного обеспечения. Выполнение операций по резервному копированию данных, создание образов и в режиме реального времени. Использование криптографических методов защиты данных. Обеспечение безопасности flash носителей.

Тема 3. Осуществление мер защиты компьютерных сетей и данных

Обеспечение доступа к ресурсам сети (диски, папки, файлы). Организация начала сеанса на рабочей станции, работа с учетными карточками пользователей, отслеживание журнала событий безопасности. Применение специализированного программного обеспечения для организации защиты компьютерных сетей

Производственная практика:

1. **Вводный инструктаж. Первичный инструктаж на рабочем месте. Знакомство с оборудованием предприятия.**
2. **Обеспечение информационной безопасности компьютерных сетей.**

Настройка и выполнение резервного копирования данных. Установка программного обеспечения для защиты от вредоносного ПО. Проверка рабочих станций и серверов на наличие вирусов и вредоносного программного обеспечения. Проверка электронных почтовых ящиков на наличие вирусов. Настройка учетных записей и паролей пользователей. Подключение общих сетевых ресурсов (дисков, папок), настройка доступа к файлам.

3. Выполнение работ, связанных с обеспечением информационной безопасности и поддержанием целостности локальной компьютерной сети предприятия.

3.1.Выполнение работ по монтажу локальных компьютерных сетей

Монтаж несущих компонентов для кабеля. Прокладка кабеля. Разделка кабеля. Строительно-монтажные работы при монтаже ЛКС. Монтажные работы по прокладке локальной сети для офиса.

3.2.Работы по подключению оборудования к локальной сети

Сборка и запуск в работу рабочих станций. Настройка операционной системы под пользователя. Подключение сетевого оборудования и принтера к ЛКС. Настройка доступа к общим ресурсам сети. Подключение серверов.

3.3.Выполнение работ по эксплуатации и обслуживанию сетевого оборудования

Выполнение различных регламентных работ. (внешний осмотр элементов сети, проверка надежности крепления и установок). Выполнение различных регламентных работ (удаление пыли и загрязнений, проверка герметичности соединений, чистка разъемов, визуальная проверка механических повреждений и следов коррозии.). Выполнение различных регламентных работ (чистка пылесосом внутренних объемов аппаратуры, тестирование элементов сети, регулировка параметров настроек сетевого оборудования). Настройка оборудования абонента (ПК, роутер).

3.4.Работы по настройке системы регистрации и авторизации пользователей сети

Создание базы данных пользователей сети. Настройка системы регистрации пользователей.

3.5.Выполнение работ по подключению к глобальным компьютерным сетям.

Настройка и подключение к сети Интернет с пользователей. Настройка параметров подключения к сети Интернет. Установка программного обеспечения для обеспечения производственного процесса. Установка программного обеспечения для поддержки работоспособности сетевого оборудования и рабочих станций. Настройка браузеров. Обслуживание электронных почтовых ящиков, сайтов. Настройка программного обеспечения серверов.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие учебного кабинета спецдисциплин (кабинет №23) и лаборатории Монтажа и эксплуатации ЛКС.

Оборудование учебного кабинета и рабочих мест кабинета спецдисциплин (кабинет №23): кафедра преподавателя, стол ученический - 15 штук, стул ученический – 30 штук, доска маркерная

Технические средства обучения: персональный компьютер, мультимедийный проектор, аудиосистема

Оборудование лаборатории и рабочих мест лаборатории монтажа и эксплуатации ЛКС:

- стол ученический - 18 штук, стул ученический – 15 штук;
- стол письменный – 1 штука, стул мягкий – 1 штука;
- доска маркерная;
- Рабочее место мастера: персональный компьютер, монитор, мышь, клавиатура, мультимедийный проектор, аудиосистема;
- 15 рабочих мест: персональный компьютер, монитор, мышь, клавиатура;
- сетевое оборудование: коммутаторы, концентраторы, роутеры, принтеры;
- пакет прикладных программ Microsoft Office 2010: Word, Visio;
- операционные системы: Windows 7, Windows Server 2008, Unix;
- ознакомительные версии специализированного программного обеспечения: Acronis True Image, Handy Backup Server, DriveCrypt, BestCrypt, PGPdisk, Firewalls – брандмауэры, Proxy-servers.
- доступ к сети Интернет

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.
2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2014. - 416 с.
3. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.
4. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.
5. Основные положения информационной безопасности: Учебное пособие/ В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.

Дополнительные источники:

1. Компьютерные сети: Учебное пособие / А.В. Кузин. - 3-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; (Профессиональное образование).
2. Компьютерные сети: Учебное пособие для студ. учреждений СПО/ Н.В. Максимов, И.И. Попов. - 6-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2013. - 464 с. (Профессиональное образование).
3. Компьютерные сети, учебник/ Е.О.Новожилов., - М.: Академия , 2011г

4. Компьютерные сети: Учебное пособие по администрированию локальных и объединенных сетей/А.В.Велихов, К.С. Строчников ,Б.К.Леонтьев.- 2-е изд. 2004г. - 320 с.
5. Локальная сеть без проблем: учебное пособие / Д. Буравчик.- Издательство Лучшие Книги, 2005.- 224с.
6. Основы компьютерных сетей: Учебное пособие / Б.Д.Виснадул, С.А.Лупин, С.В. Сидоров.; Под ред. Л.Г.Гагариной - М.: ИД ФОРУМ: НИЦ Инфра-М, 2012. - 272 с.,(Профессиональное образование).
7. Широкополосные беспроводные сети передачи информации : Учебник/ Вишневский В.М.- Издательство Техносфера, 2005. -592с.

4.3. Общие требования к организации образовательного процесса

При реализации ФГОС предусматривается использование в образовательном процессе активных форм, проведения занятий с применением электронных образовательных ресурсов, анализа производственных ситуаций, групповых дискуссий в сочетании с внеаудиторной работой для формирования общих и профессиональных компетенций обучающихся.

Учебная практика проводятся образовательным учреждением при освоении обучающимися профессиональных компетенций в рамках профессиональных модулей и реализуется рассредоточено, чередуясь с теоретическими занятиями в рамках профессиональных модулей.

Консультации по выполнению самостоятельных работ проводятся в очной форме и с использованием дистанционных технологий.

Одновременно с началом обучения по профессиональному модулю рекомендуется начать изучение междисциплинарного курса:

МДК 03.01. Информационная безопасность персональных компьютеров и компьютерных сетей

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): среднее профессиональное или высшее профессиональное образование, соответствующее профилю преподаваемого модуля.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: мастера производственного обучения имеют на 1 – 2 разряда по профессии рабочего выше, чем предусмотрено образовательным стандартом для выпускников.

Преподаватели, отвечающие за освоение обучающимся профессионального цикла имеют опыт деятельности в организациях соответствующей профессиональной сферы, преподаватели и мастера производственного обучения проходят стажировку в профильных организациях 1 раз в 3 года

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. Обеспечивать резервное копирование данных	- Выполнение работ связанных с резервным копированием данных - Выполнение резервного копирования с использованием специализированного программного обеспечения - Выполнение резервного копирования с использованием аппаратного обеспечения	Текущий контроль в форме практических занятий и контрольных работ по темам МДК. Зачеты по учебной практике в виде выполнения практических работ направленных на освоение компетенции
ПК 3.2. Осуществлять меры по защите компьютерных сетей от несанкционированного доступа	- Выполнение работ по настройке контент – фильтрации; - Выполнение работ по настройке межсетевых экранов; - Выполнение работ по настройке учетных записей пользователей, настройке доступа, разграничению прав пользователей; - Выполнение работ по администрированию программного обеспечения, осуществляющего контент – фильтрацию - Выполнение работ по администрированию межсетевых экранов	Текущий контроль в форме практических занятий и контрольных работ по темам МДК. Зачеты по учебной практике в виде выполнения практических работ направленных на освоение компетенции
ПК 3.3. Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами	- Выполнение работ по установке антивирусного программного обеспечения; - Выполнение работ по настройке антивирусного программного обеспечения; - Выполнение работ по восстановлению и устранению последствий воздействия вредоносного программного обеспечения;	Текущий контроль в форме практических занятий темам МДК. Зачеты по учебной практике в виде выполнения практических работ направленных на освоение компетенции

ПК 3.4. Осуществлять мероприятия по защите персональных данных	- Выполнение работ по организации и планированию мероприятий по защите ИСПДн - Ведение отчетной документации по обеспечению защиты ИСПДн - Принятие мер по устранению неисправностей ЛКС, которые могут повлечь за собой, снижение уровня зашиты сети в целом	Зачеты по учебной практике в виде выполнения практических работ направленных на освоение компетенции Текущий контроль в форме практических занятий по темам МДК.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость будущей профессии, проявлять к ней устойчивый интерес	– Демонстрация интереса к будущей профессии – Участие в профессиональных конкурсах	Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 2. Организовывать собственную деятельность, исходя из цели и способов ее достижения, определенных руководителем	– Выбор и применение методов и способов решения профессиональных задач в процессе создания, обработки , публикации готовой продукции – Организация самостоятельных занятий при изучении профессионального модуля	Анализ результатов выполнения практических и квалификационных работы оценка при выполнении работ на учебной и производственной практике
ОК 3. Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы	– Демонстрация эффективности и качества выполнения профессиональных задач – Самоанализ и коррекция результатов собственной работы	оценка при выполнении работ на учебной практике
ОК 4. Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.	– Нахождение и использование информации для эффективного выполнения профессиональных задач	Анализ результатов выполнения практических и квалификационных работы
ОК 5. Использовать информационно-коммуникационные	– Демонстрация навыков использования информационно –	Анализ результатов выполнения практических и

технологии в профессиональной деятельности	коммуникационных технологий в профессиональной деятельности	квалификационных работы
ОК 6. Работать в команде, эффективно общаться с коллегами, руководством, клиентами	– Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения – Успешная работа в учебной бригаде при выполнении производственных заданий	Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 7. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).	– Демонстрация готовности к исполнению воинской обязанности – Активное участие в военно-патриотических мероприятиях	Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы