Частное образовательное учреждение
профессионального образования
«Московский областной гуманитарный открытый колледж»

ПРИНЯТА
Педагогическим советом
Протокол № 5 от «23» апреля 2021 г.

Председатель _____Т.С. Букина

УТВЕРЖДАЮ
Приказ № 14/04-21 от «23» апреля 2021 г.

Директор _____ Т. С. Букина

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

МДК.03.01 Информационная безопасность персональных компьютеров и компьютерных сетей

По направлению
230103.03 Наладчик компьютерных сетей

Серебряные пруды,2021г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Область применения программы

Рабочая программа профессионального модуля (далее программа ПМ) – является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО

230103.03 Наладчик компьютерных сетей

в части освоения основного вида профессиональной деятельности (ВПД):
обеспечение информационной безопасности компьютерных сетей.

и соответствующих профессиональных компетенций (ПК):

1. ПК 3.1. Обеспечивать резервное копирование данных.
2. ПК 3.2. Осуществлять меры по защите компьютерных сетей от несанкционированного доступа.
3. ПК 3.3. Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.
4. ПК 3.4. Осуществлять мероприятия по защите персональных данных

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

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – 822 часа, в том числе:

максимальной учебной нагрузки обучающегося – 192 часа, включая:

аудиторной учебной работы обучающегося – (обязательных учебных занятий) 128 часов;

внеаудиторной (самостоятельной) учебной работы обучающегося – 64 часа;

учебной практики – 18 часа

производственной практики – 612 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися 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 своей 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 СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Содержание обучения по профессиональному модулю (ПМ.03 Обеспечение информационной безопасности компьютерных сетей)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	**Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект)** *(если предусмотрены)*	**Объем часов**	**Уровень освоения**
1	**2**	**3**	**4**
Раздел 1. Информационная безопасность персональных компьютеров и компьютерных сетей		*	
МДК.03.01 Информационная безопасность персональных компьютеров и компьютерных сетей		*	
Раздел 1. Основные понятия, концепции и принципы информационной безопасности			
Тема 1.1. Основы информационной безопасности. Основные понятия и определения	**Содержание**	2	2
	1. Понятие информации Доступ к информации Информационные системы Обработка информации Защита информации Информационная безопасность		
Тема 1.2. Политика государства в области информационной безопасности	**Содержание**	2	2
	1. Стратегия национальной безопасности Доктрина информационной безопасности Законодательство в области защиты информации Государственная тайна Коммерческая тайна Персональные данные		
Тема 1.3. Идентификация, аутентификация и авторизация Модели информационной безопасности	**Содержание**	2	2
	1. Идентификация, аутентификация и авторизация Модели информационной безопасности Триада «конфиденциальность, доступность, целостность» Гексада Паркера и модель STRIDE		
Тема 1.4. Уязвимость, угроза, атака Ущерб и риск. Управление рисками Типы и примеры атак	**Содержание**	2	2
	1. Пассивные и активные атаки Отказ в обслуживании Внедрение вредоносных программ Кража личности, фишинг		
Тема 1.5. Иерархия средств защиты от информационных угроз	**Содержание**	2	2
	1. Средства безопасности законодательного уровня Административный уровень. Политика безопасности Средства безопасности процедурного уровня Средства безопасности технического уровня		
Тема 1.6. Принципы защиты	**Содержание**	2	2

информационной системы	1	Подход сверху вниз		

		Защита как процесс Эшелонированная защита Сбалансированная защита Компромиссы системы безопасности		
Тема 1.7. Шифрование	**Содержание**		2	2
	1.	Основные понятия и определения Симметричное шифрование. Проблема распределения ключей Метод Диффи-Хелмана передачи секретного ключа по незащищенному каналу Концепция асимметричного шифрования Алгоритм асимметричного шифрования RSA Хеш-функции. Односторонние функции шифрования. Проверка целостности		
Внеаудиторная (самостоятельная) учебная работа при изучении раздела 1				
Систематическая проработка конспектов занятий, учебной и специальной технической литературы с целью выполнения заданий преподавателя. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, подготовка к их защите. Реферат на тему: «Понятие информации», «Информационные системы», «Стратегия национальной безопасности», «Доктрина информационной безопасности», «Законодательство в области защиты информации», «Государственная тайна» «Коммерческая тайна»			*12*	
Раздел 2. Технологии аутентификации, авторизации и управления доступом				
Тема 2.1. Технологии аутентификации	**Содержание**		2	2
	1.	Факторы аутентификации человека Аутентификация на основе паролей Аутентификация на основе аппаратных аутентификаторов Аутентификация информации. Электронная подпись Аутентификация на основе цифровых сертификатов Аутентификация программных кодов		
	Практические занятия		2	
	1.	Факторы аутентификации человека Аутентификация на основе паролей Аутентификация на основе аппаратных аутентификаторов Аутентификация информации. Электронная подпись Аутентификация на основе цифровых сертификатов Аутентификация программных кодов		
Тема2.2. Технологии управления доступом и авторизации и	**Содержание**		2	2
	1	Формы представления ограничений доступа Дискреционный метод управления доступом Мандатный метод управления доступом Ролевое управление доступом		
Тема 2.3. Системы аутентификации и управления доступом операционных систем	**Содержание**		2	2
	1.	Аутентификации пользователей ОС Управление доступом в операционных системах		

		Концепция единого логического входа Система Kerberos		
Внеаудиторная (самостоятельная) учебная работа при изучении раздела 2				
Систематическая проработка конспектов занятий, учебной и специальной технической литературы с целью выполнения заданий преподавателя. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, подготовка к их защите. Реферат на тему: «Аутентификация субъектов доступа», «Разграничение доступа»			*10*	
Раздел 3. Технологии безопасности на основе фильтрации и мониторинга трафика				
Тема 3.1. Фильтрация	**Содержание**		2	2
	1.	Виды фильтрации Стандартные и дополнительные правила фильтрации маршрутизаторов		
Тема 3.2. Файерволы	**Содержание**		2	2
	1.	Функциональное назначение файервола Типы файерволов		
Тема 3. 3 Файерволы с функцией NAT	**Практические занятия**		2	
	1.	Традиционная технология NAT Базовая трансляция сетевых адресов Трансляция сетевых адресов и портов Типовые архитектуры сетей, защищаемых файерволами		
Тема 3.4. Мониторинг трафика. Анализаторы протоколов	**Практические занятия**		2	
	1.	Анализаторы протоколов Система мониторинга NetFlow Системы обнаружения вторжений		
Внеаудиторная (самостоятельная) учебная работа при изучении раздела 3				
Систематическая проработка конспектов занятий, учебной и специальной технической литературы с целью выполнения заданий преподавателя. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, подготовка к их защите.			*9*	
Раздел 4. Безопасность программного кода и сетевых служб				
Тема 4.1. Уязвимости программного кода и вредоносные программы	**Содержание**		2	2
	1.	Уязвимости, связанные с нарушением защиты оперативной памяти Уязвимости контроля вводимых данных Внедрение в компьютеры вредоносных программ Троянские программы Сетевые черви Вирусы Программные закладки Антивирусные программы Ботнет		
	Практические занятия		4	
	1.	Уязвимости, связанные с нарушением защиты оперативной памяти Уязвимости контроля вводимых данных		

		Внедрение в компьютеры вредоносных программ Троянские программы Сетевые черви Вирусы Программные закладки Антивирусные программы Ботнет		
Тема 4.2. Безопасность веб-сервиса	**Содержание**		4	2
	1.	Безопасность веб-браузера Приватность и куки Протокол HTTPS Безопасность средств создания динамических страниц		
	Практические занятия		2	
	1.	Безопасность веб-браузера Приватность и куки Протокол HTTPS Безопасность средств создания динамических страниц		
Тема 4.3. Безопасность электронной почты	**Содержание**		2	2
	1.	Угрозы приватности постового сервиса Аутентификация отправителя Шифрование содержимого письма Защита метаданных пользователя Спам Атаки почтовых приложений		
	Практические занятия		2	
	1.	Угрозы приватности постового сервиса Аутентификация отправителя Шифрование содержимого письма Защита метаданных пользователя Спам Атаки почтовых приложений		
Тема 4.4. Облачные сервисы и их безопасность	**Содержание**		2	2
	1.	Концепция облачных вычислений Определение облачных вычислений Модели сервисов облачных сервисов Облачные вычисления как источник угрозы Облачные сервисы как средство повышения сетевой безопасности		
Тема 4.5. Контрольная работа	**Практические занятия**		2	
	1.	Основы информационной безопасности. Основные понятия и определения Политика государства в области информационной безопасности "Идентификация, аутентификация и авторизация Модели информационной безопасности" Уязвимость, угроза, атака		

		Ущерб и риск. Управление рисками Типы и примеры атак Иерархия средств защиты от информационных угроз Принципы защиты информационной системы Шифрование Технологии аутентификации Технологии управления доступом и авторизации Системы аутентификации и управления доступом операционных систем Фильтрация Файерволы Файерволы с функцией NAT Мониторинг трафика. Анализаторы протоколов Уязвимости программного кода и вредоносные программы Безопасность веб-сервиса Безопасность электронной почты Облачные сервисы и их безопасность		
Внеаудиторная (самостоятельная) учебная работа при изучении раздела 4				
Систематическая проработка конспектов занятий, учебной и специальной технической литературы с целью выполнения заданий преподавателя. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, подготовка к их защите.			*9*	
Раздел 5. Настройка безопасности в Windows Server				
Тема 5.1. Обнаружение уязвимостей и использование инструментов Sysinternals	**Содержание**		2	2
	1.	Обзор возможностей обнаружения нарушений Использование инструментов Sysinternals для выявления нарушений		
Тема 5.2. Основные обнаружения нарушений и стратегии реагирования на инциденты	**Практические занятия**		2	
	1.	Выявление типов атак Применение стратегии реагирования на инциденты Изучение средств Sysinternals		
Тема 5.3. Защита учетных записей и привилегированный доступ	**Содержание**		2	2
	1.	Понимание работы прав пользователя Учетные записи компьютера и служб Защита учетных данных Понимание привилегированного доступа к рабочим станциям и серверам Развертывание решения для управления паролем локального администратора		
Тема 5.4. Права пользователя, параметры безопасности и групповые управляемые сервис аккаунты	**Практические занятия**		2	
	1.	Настройка параметров безопасности Настройка групп с ограниченным доступом Делегирование привилегий Создание и управление групповых управляемых сервис аккаунтов Настройка функций Охранника учетных данных (Credential Guard) Обнаружение проблемных учетных записей		

Тема 5.5. Настройка и развертывание решений управления паролем локального администратора (local administrator password - LAP)	**Практические занятия**		2	
	1.	Установка решений управления паролем локального администратора (LAP) Настройка решений LAP Развертывание решений LAP		
Тема 5.6. Ограничение прав администратора с помощью функции Just Enough Administration	**Содержание**		2	2
	1.	Понимание Just Enough Administration Настройка и развёртывание Just Enough Administration		
	Практические занятия		2	
	1.	Создание файла с перечнем возможностей Создание файла конфигурации сеанса Создание точки подсоединения Just Enough Administration Подключение к точке подсоединения Just Enough Administration Развертывание Just Enough Administration с помощью Desire State Configuration (DSC)		
Тема 5.7. Управление привилегированным доступом и администрирование леса	**Содержание**		2	2
	1.	Понимание расширенная административная среда безопасности леса Обзор MIM Реализация Just In Time (JIT) Administration и управление привилегированным доступом с помощью MIM		
Тема 5.8. Ограничение прав администратора с помощью управления привилегированным доступом	**Практические занятия**		2	
	1.	Использование многоуровневого подхода к безопасности Изучение MIM Настройка веб-портала MIM Настройка функции привилегированного доступа Запрос привилегированного доступа		
Тема 5.9. Противодействие вредоносным программам и угрозам	**Содержание**		2	2
	1.	Настройка и управление Защитником Windows Использование политик ограничения программного обеспечения (SRP) и AppLocker Настройка и использование Device Guard Использование и развертывание Enhanced Mitigation Experience Toolkit (EMET)		
Тема 5.10. Защита приложений с помощью AppLocker, защитника Windows, правил Device Guard и EMET	**Практические занятия**		2	
	1.	Настройка Защитника Windows Настройка AppLocker Настройка и развертывание Device Guard Развертывание и использование EMET		
Тема 5.11. Анализ активности с помощью расширенного аудита и журналов аналитики	**Содержание**		2	2
	1.	Обзор технологий аудита Понимание расширенный аудит Настройка аудита в Windows PowerShell и ведение журнала		
Тема 5.12. Настройка	**Практические занятия**		2	

шифрования и расширенный аудит	1.	Настройка аудита доступа к файловой системе Аудит входа в систему домена Управление конфигурацией расширенной политики аудита Протоколирование и аудит в Windows PowerShell		
Тема 5.13. Анализ активности с помощью Microsoft Advanced Threat Analytics и Operations Management Suite	**Содержание**		2	1
	1.	Обзор Advanced Threat Analytics Понимание OMS Использование Microsoft Advanced Threat Analytics и OMS Подготовка и развертывание Microsoft Advanced Threat Analytics Подготовка и развертывание OMS		
Тема 5.14. Защита виртуальной инфраструктуры	**Содержание**		2	1
	1.	Обзор защищённой фабрики виртуальных машин Понимание требований экранирования и поддержка шифрования ВМ Развертывание защищенной фабрики ВМ с доверенной проверкой администратора Развертывание экранированных ВМ		
Тема5.15. Защита данных с помощью шифрования	**Содержание**		2	2
	1.	Планирование и реализация шифрования Планирование и реализация BitLocker		
Тема 5.16. Настройка EFS и BitLocker	**Практические занятия**		2	
	1.	Шифрование и восстановление доступа к зашифрованным файлам Использование BitLocker для защиты данных		
Тема 5.17. Ограничение доступа к файлам и папкам	**Содержание**		2	2
	1.	Введение в Диспетчер ресурсов файлового сервера Реализация управления классификацией и задачи управления файлами Понимание динамического контроля доступа (DAC)		
Тема 5.18. Настройка квот и блокировки файлов	**Содержание**		2	2
	1.	Общие сведения о брандмауэре Windows Распределенные программные брандмауэры		
Тема 5.19. Использование брандмауэров для контроля сетевого трафика	**Содержание**		2	2
	1	Общие сведения о брандмауэре Windows Распределенные программные брандмауэры		
Тема 5.20. Брандмауэр Windows в режиме повышенной безопасности	**Практические занятия**		2	
	1.	Создание и тестирование правил входящих подключений Создание и тестирование правил исходящих подключений		
Тема5.21. Обеспечение безопасности сетевого трафика	**Содержание**		2	1
	1.	Угрозы безопасности сети и правила безопасного подключения Настройка дополнительных параметров DNS Анализ сетевого трафика с Microsoft Message Analyzer Обеспечение безопасности трафика SMB и анализа трафика SMB		
Тема 5.22. Правила безопасного подключения и обеспечение безопасности DNS	**Содержание**		2	1
	1.	Создание и тестирование правила безопасного подключения Настройка и тестирование DNSSEC		

Тема 5.23. Шифрование SMB и Microsoft Message Analyzer	**Содержание**		2	2
	1.	Использование Microsoft Message Analyzer Настройка и проверка шифрования SMB на общих папках		
Тема 5.24. Обновление Windows Server	**Содержание**		2	2
	1.	Обзор WSUS Развертывание обновлений с помощью WSUS		
Тема 5.25. Осуществление управления обновлениями	**Содержание**		2	2
	1.	Установка роли сервера WSUS Настройка параметров обновления Одобрение и развертывание обновления с помощью WSUS Развертывание обновлений для определений Защитника Windows с помощью WSUS		
Внеаудиторная (самостоятельная) учебная работа при изучении раздела 5				
Систематическая проработка конспектов занятий, учебной и специальной технической литературы с целью выполнения заданий преподавателя. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, подготовка к их защите.			*9*	
	Раздел 6. Резервное копирование и восстановление данных			
Тема 6.1. Резервное копирование и восстановление данных	**Содержание**		2	2
	1.	Сущность и основные понятия резервного копирования и восстановления данных Классификация аппаратных и программных средств резервного копирования и восстановления данных		
Тема 6.2. Способы сохранения резервного копирования	**Содержание**		2	2
	1.	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		
Тема 6.3. Виды резервного копирования	**Содержание**		2	2
	1.	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		
Тема 6.4. RAID	**Содержание**		2	2
	1.	Виды RAID-массивов, технология их составления		
Тема 6.5. Восстановление данных	**Содержание**		2	2
	1.	Резервное копирование и восстановление данных с использованием аппаратных средств.		
	Практические занятия		2	
	1.	Резервное копирование и восстановление данных с использованием аппаратных средств.		
Внеаудиторная (самостоятельная) учебная работа при изучении раздела 6			*9**	

Тематика домашних заданий Систематическая проработка конспектов занятий, учебной и специальной технической литературы с целью выполнения заданий преподавателя. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, подготовка к их защите.		
Учебная практика **Виды работ** Определение угроз Анализ рисков Построение модели защиты ПК и сети от вирусов Выбор метода защиты ПК от вирусов и от несанкционированного доступа. Установка безопасности Windows Установка и настройка антивирусного ПО Обновление антивирусного ПО. Отключение и удаление неиспользованных учетных записей. Установка паролей для всех учетных записей пользователей Защита сервера от вирусов. Диагностика заражения ПК вирусами. Контроль карантина. Восстановление зараженных файлов, папок. Установка и настройка межсетевого экрана Защита корпоративных сетей от вирусов и троянских программ. Установка и настройка аппаратных средств резервного копирования данных Установка и настройка программных средств резервного копирования данных Разработка и реализация стратегии резервного копирования. Резервное копирование данных. Архивирование данных Выбор архивных устройств и носителей Определение ограничений для резервного копирования. Теневые копии Обновление ПО для резервного копирования данных. Резервное копирование перед и после обновления системы. Создание ASR-копии Установка приемлемого окна резервного копирования данных. Установка расписания резервного копирования данных. Разработка политики хранения резервных копий. Тестирование восстановления из резервных копий. Архитектура безопасности данных. Классификация информационных систем персональных данных Защита информации от утечки по техническим каналам Защита информации от несанкционированного доступа Межсетевые экраны на границе контролируемой зоны ИСПДн Шифрование данных и файлов Непрерывное обеспечение безопасности данных. Организация и проведение мероприятий по защите персональных данных	18	

Создание системы защиты персональных данных Приведение процессов обработки и обеспечения безопасности персональных данных в соответствие требованиям законодательства Реализация политик шифрования данных в состоянии покоя Восстановление данных из резервной копии. Установка программ для проверки подлинности. Выбор методов проверки подлинности. Проверка подлинности. Авторизация пользователей Работа с программами восстановления данных. Безопасность ресурсов и контроль доступа Сканирование уязвимостей. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам Основные этапы допуска к ресурсам вычислительной системы Допуск к ресурсам сети Допуск к ресурсам сервера, базы данных Использование динамически изменяющегося пароля Взаимная проверка подлинности и другие случаи опознания. Применение различных способов разграничения доступа к компьютерным ресурсам Разграничение доступа по спискам Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Автоматическое шифрование логических дисков ПК. Борьба со спамом техническими средствами. Фильтрация почты. Сбор адресов электронной почты. Создание черных списков. Авторизация почтовых серверов Сортировка писем. Использование антивирусной защиты при заражении ПК. Настройка безопасности Windows Server		
Производственная практика **Виды работ** Настройка периферийных устройств и рабочих станций локальной сети Выполнение резервного копирования данных Использование криптографических методов защиты данных. Осуществление мер защиты компьютерных сетей и данных Обеспечение доступа к ресурсам сети (диски, папки, файлы). Применение специализированного программного обеспечения для организации защиты компьютерных сетей	612	
Всего	**822**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Материально-техническое обеспечение

Реализация программы модуля предполагает наличие учебных кабинетов информатики и информационных технологий;

Оборудование учебного кабинета и рабочих мест кабинета информатики и информационных технологий

- рабочие места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-методических материалов, методические рекомендации и разработки;
- образцы инструментов, приспособлений

Технические средства обучения: персональный компьютер с лицензионным программным обеспечением и мультимедиапроектор. Рабочие станции с выходом в интернет и сервер. Локальная сеть. Коммуникаторы. Сервер

Оборудование мастерской и рабочих мест мастерской:

Оборудование и технологическое оснащение рабочих мест:

- маршрутизатор
- коммутатор
- концентратор
- сервер

2.2. Информационное обеспечение обучения

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Обеспечение информационной безопасности компьютерных сетей/Богомазова Г. Н. – М. Издательский центр «Академия», 2017,

Дополнительные источники:

1. Windows Server 2012R2. Полное руководство. Том 1. Установка и конфигурирование сервера, сети , DNS, Active Directory и общего доступа к данным и принтерам/ М. Минаси/ М. : «И.Д. Вильямс», 2015
2. Windows Server 2012R2. Полное руководство. Том 2: дистанционное администрирование, установка среды с несколькими доменами, виртуализация, мониторинг и обслуживание сервера/М. Минаси/: Пер. с англ. - М. : «И.Д. Вильямс», 2015
3. Администрирование данных Windows Server 2012/ Платунова С.М./ Учебное пособие/ - СПб: НИУ ИТМО, 2016
4. Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, протоколы. 5-е изд. СПб: Издательство «Питер», 2017.

После каждого наименования печатного издания обязательно указываются издательство и год издания (в соответствии с ГОСТом). При составлении учитывается наличие результатов экспертизы учебных изданий в соответствии с порядком, установленным Минобрнауки России.

4.3. Организация образовательного процесса

Освоению программы модуля предшествует изучение общепрофессиональных дисциплин – основы информационных технологий, основы электротехники, основы электроники и цифровой схемотехники, охрана труда и техника безопасности в рамках которых,

учебными программами предусмотрены теоретические занятия для освоения знаний и практические занятия для закреплением полученных теоретических знаний.

Теоретические занятия проводятся парами по 2 урока по 45 минут, с 5 –минутным перерывом между уроками и 10-минутными перерывами между парами, по расписанию. Практические занятия могут проводится сгруппированными парами по 4 академических часа, в зависимости от вида запланированных работ.

МДК 01.01 завершается на шестом семестре дифференцированным зачетом.

Профессиональный модуль осваивается на 5-6 семестрах. На шестом семестре завершается **комплексным квалификационным экзаменом**. Также по мере освоения профессионального модуля предусмотрены комплексные следующие виды контроля:

Вид контроля	***Семестр***	***Разделы модуля***
Комплексный экзамен	***6***	МДК.02.01 Установка и настройка аппаратных и программных средств доступа в сеть Интернет
		МДК.03.01 Информационная безопасность персональных компьютеров и компьютерных сетей
Комплексный дифференцированный зачет	6	УП.01.01 Выполнение работ по монтажу, наладке, эксплуатации и обслуживанию локальных компьютерных сетей
		УП.02.01 Установка и настройка аппаратных и программных средств доступа в сеть Интернет
		УП.03.01 Обеспечение информационной безопасности компьютерных сетей
Комплексный квалификационный экзамен	6	ПМ.01 Выполнение работ по монтажу, наладке, эксплуатации и обслуживанию локальных компьютерных сетей
		ПМ.02 Обеспеченно информационной безопасности компьютерных сетей
		ПМ.03 Обеспечение информационной безопасности компьютерных сетей

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

Результаты (освоенные профессиональные и общие компетенции)	**Основные показатели оценки результата**
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
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
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;
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
ОК 1. Понимать сущность и социальную значимость будущей профессии, проявлять к ней устойчивый интерес	• Демонстрация интереса к будущей профессии • Участие в профессиональных конкурсах
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
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
ОК 4. Осуществлять поиск информации, необходимой для эффективного выполнения	• Демонстрация навыков использования информационно – коммуникационных технологий в профессиональной деятельности

профессиональных задач.	
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	• Демонстрация навыков использования информационно – коммуникационных технологий в профессиональной деятельности
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
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