

Министерство общего и профессионального образования Свердловской области  
государственное автономное профессиональное образовательное учреждение  
Свердловской области  
«Уральский радиотехнический колледж им. А.С. Попова»

УТВЕРЖДАЮ:  
Зам. директора  
\_\_\_\_\_ / С.Н. Меньшикова /  
«\_\_» \_\_\_\_\_ 2022 г.

**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**  
**ПМ.03 Обеспечение информационной безопасности компьютерных сетей**

для профессии среднего профессионального образования

09.01.02 Наладчик компьютерных сетей  
программы базовой подготовки

Екатеринбург  
2022

## **СОДЕРЖАНИЕ**

<b>1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>4</b>
<b>2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>6</b>
<b>3. СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>8</b>
<b>4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ</b>	<b>11</b>
<b>5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)</b>	<b>14</b>

# 1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) является частью основной профессиональной образовательной программы – образовательной программы среднего профессионального образования – программа подготовки квалифицированных рабочих, служащих по профессии (далее ППКРС).

Рабочая программа разработана в соответствии с ФГОС СПО утвержденный приказом Министерства образования и науки Российской Федерации от 02.08.2013 № 853 (в ред. от 13.07.2021), составлена по учебному плану 2022 года по профессии 09.01.02 «Наладчик компьютерных сетей» 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.

## 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:

В результате изучения профессионального модуля обучающийся 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. Количество часов на освоение программы профессионального модуля:**

всего – 504 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося – 120 часов;

самостоятельной работы обучающегося – 60 часов;

учебной практики -144 часов

производственной практики – 180 часов.

<b>Индекс</b>	<b>Наименование</b>	<b>Форма промежуточной аттестации, семестр</b>
МДК.03.01	Информационная безопасность персональных компьютеров и компьютерных сетей	дифференцированный зачет, 4 семестр
УП.03.01	Учебная практика по обеспечению информационной безопасности компьютерных сетей	дифференцированный зачет, 5 семестр
ПП.03.01	Производственная практика	дифференцированный зачет, 6 семестр
ПМ.03.ЭК	Экзамен (квалификационный)	5 семестр

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности по проектированию сетевой инфраструктуры, 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, 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.

Освоение профессионального модуля ПМ.03 «Обеспечение информационной безопасности компьютерных сетей» обеспечивает достижение обучающимися следующих **личностных результатов (ЛР):**

ЛР 3 Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих;

ЛР 4 Проявляющий и демонстрирующий уважение к людям труда, осознающий

ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»;

ЛР 10 Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой;

ЛР 14 Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм;

ЛР 15 Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;

ЛР 1 – Р Соблюдающий корпоративные стандарты и проявляющий корпоративную лояльность к организации-работодателю;

ЛР 1-К Уважающий лучшие традиции колледжа, стремящийся к сохранению положительной деловой репутации и приумножению позитивного имиджа образовательной организации.

### 3. СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Тематический план профессионального модуля

Коды ПК	Наименования разделов профессионального модуля *	Наименования разделов профессионального модуля	Всего часов (макс. учебная нагрузка и практики), в том числе по вариантиву	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					
				Обязательная аудиторная учебная нагрузка обучающегося				Самостоятельная работа обучающегося	
				Всего, часов	практические занятия, часов	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
ПК 3.1-ПК 3.4	МДК 03.01 Информационная безопасность персональных компьютеров и компьютерных сетей	Раздел 1. Обеспечение безопасности функционирования информационных систем	180	120	40			60	
ПК 3.1-ПК 3.4	УП 03.01 Учебная практика по обеспечению информационной безопасности компьютерных сетей		144						
ПК 3.1-ПК 3.4	Производственная практика (по профилю специальности), часов		180						
	<b>Всего:</b>		<b>504</b>	<b>120</b>	<b>40</b>		<b>-</b>	<b>60</b>	<b>-</b>

### 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
<b>Раздел 1 ПМ 03. Обеспечение безопасности функционирования информационных систем</b>			ОК 1-7, ПК 3.1-ПК 3.4, ЛР3, ЛР 4, ЛР 10, ЛР 14, ЛР 15, ЛР 1 – Р, ЛР 1-К
<b>МДК 03.01</b> Информационная безопасность персональных компьютеров и компьютерных сетей		<b>120</b>	
<b>Тема 2.1</b> Анализ и проектирование информационных систем	<p><b>Содержание</b></p> <p>1 Классификация информационных систем (ИС).</p> <p>2 Области применения и примеры реализации информационных систем.</p> <p>3 Требования, предъявляемые к информационным системам.</p>	16	
<b>Тема 2.2</b> Жизненный цикл ИС	<p><b>Содержание</b></p> <p>1 Общие сведения об управлении проектами. Классификация проектов.</p> <p>2 Основные фазы проектирования ИС.</p> <p>3 Процессы жизненного цикла ИС.</p> <p>4 Модели жизненного цикла ИС.</p>	16	
<b>Тема 2.3</b> Основные факторы, определяющие технологическую безопасность ИС	<p><b>Содержание</b></p> <p>1 Проблемы обеспечения безопасности ИС.</p> <p>2 Показатели технологической безопасности ИС.</p> <p>3 Требования к архитектуре и ИС и их компонентам для обеспечения безопасности функционирования.</p> <p>4 Ресурсы обеспечивающие технологическую безопасность ИС.</p>	16	
	<p><b>Практические работы</b></p> <p>1 Определение показателей безопасности ИС.</p> <p>2 Формулирование требования к архитектуре ИС и их компонентам для обеспечения безопасности функционирования.</p>	20	
<b>Тема 2.4</b> Методы обеспечения технологической безопасности ИС	<p><b>Содержание</b></p> <p>1 Непредумышленные дестабилизирующие факторы.</p> <p>2 Методы снижения угроз безопасности ИС, вызванных дефектами программных средств и баз данных.</p> <p>3 Оперативные методы повышения безопасности программных средств и баз данных.</p>	16	



	4	Особенности обеспечения технологической безопасности импортных программных средств и баз данных.		
<b>Тема 2.5</b> Определение реальной технологической безопасности ИС	<b>Содержание</b>		16	ОК 1-7, ПК 3.1-ПК 3.4, ЛР3, ЛР 4, ЛР 10, ЛР 14, ЛР 15, ЛР 1 – Р, ЛР 1-К
	1	Основные требования к средствам для определения технологической безопасности ИС.		
	2	Виды тестирования для определения технологической безопасности ИС.		
	3	Обработка результатов испытаний.		
	4	Методы определения технологической безопасности критических ИС.		
	5	Международные стандарты, поддерживающие испытания технологической безопасности ИС.		
	<b>Практические работы</b>		20	
	1	Разработка клиент-серверной ИС		
	2	Обеспечение безопасности и настройка прав доступа в ИС.		
<b>Самостоятельная работа при изучении раздела 2 ПМ 3.</b>			<b>60</b>	
<b>Примерная тематика домашних заданий</b> 1. Изучение функций, обеспечивающих безопасность в СУБД MS Access – 10 ч. 2. Изучение MS SQL Server – 20 ч. 3. Изучение простых алгоритмов шифрования – 30ч.				
<b>Учебная практика по защите доступа в сеть и защите передаваемых данных</b> <b>Виды работ:</b> • Организация защищенного канала передачи данных для удаленных офисов • Защита информации на локальном ПК • Защита информации в нутрии локальной сети.			<b>144</b>	
<b>Производственная практика</b> <b>Виды работ:</b> 1. Защита подключения к сети internet рабочих мест. 2. Организация ИБ на предприятии. 3. Оценка состояния ИБ на предприятии.			<b>180</b>	
<b>Всего</b>			<b>504</b>	

## **4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

### **4.1. Требования к минимальному материально-техническому обеспечению**

Реализация программы модуля предполагает наличие:

- мастерской монтажа и настройки объектов сетевой инфраструктуры;
- лаборатории программного обеспечения компьютерных сетей.
- полигонов:
  - администрирования сетевых операционных систем;
  - технического контроля и диагностики сетевой инфраструктуры.

Оборудование мастерской и рабочих мест мастерской монтажа и настройки объектов сетевой инфраструктуры:

Обжимные клещи, измерительные приборы, мультитестеры, коннекторы, кабели, персональные компьютеры, программное обеспечение для анализа работы сети и другое ПО.

Оборудование лаборатории и рабочих мест лаборатории программного обеспечения компьютерных сетей, программирования и баз данных:

Персональные компьютеры, сетевые операционные системы, программы, реализующие функции различных типов серверов, программы ведения учета аппаратного и программного обеспечения сети.

Реализация программы модуля не предполагает обязательную производственную практику.

### **4.2. Учебно-методическое обеспечение модуля**

Основная учебная литература:

1. Гончаренко, А. Н. Сетевые технологии : учебное пособие / А. Н. Гончаренко. — Москва : МИСИС, 2020. — 92 с. — ISBN 978-5-907227-22-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/178093>. — Загл. с экрана.

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск : ЮРГПУ (НПИ), 2022. — 216 с. — ISBN 978-5-9997-0805-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/292247> — Загл. с экрана.

3. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. — Вологда : Инфра-Инженерия, 2022. — 460 с. — ISBN 978-5-9729-0962-

9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/281867> — Загл. с экрана.

4. Олифер В. Г., Олифер Н. А. Безопасность компьютерных сетей. – М.: Горячая линия- Телеком, 2018. – 644 с.

Дополнительная учебная литература:

1. Уилсон Эд. Мониторинг и анализ сетей - 2002
2. Глушаков С.В. Хачиров Т.С. Настраиваем сеть своими руками 2007.
3. Коммутаторы локальных сетей D-link. Учебное пособие. М. 2006 г.
4. Локальные сети. Полное руководство: Пер. с англ.-СПб.: КОРОНА принт, 1999.— 624 с., ил. ISBN 5-88547-067-7 Microsoft.ru
5. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-е изд., М.: Издательский дом «Вильямс», 2005. -1168с.

#### **4.3 Информационные ресурсы сети Интернет и профессиональные базы данных**

6. Cisco Networking Academy [Электронный ресурс]: [интерактив. учеб.]. Режим доступа: <https://www.netacad.com/>

#### **4.4. Общие требования к организации образовательного процесса**

Занятия проводятся спаренными уроками продолжительностью один академический час, общая продолжительность спаренного урока – 2 академических часа (1,5 астрономических часа). Образовательный процесс включает в себя проведение лекционных занятий и лабораторных, чередующихся друг с другом.

Для закрепления полученных навыков предусмотрена учебная практика в разделе 1, которая проводится концентрированно.

Освоению данного профессионального модуля должно предшествовать изучение следующих дисциплин и модулей:

ОП.01	Основы информационных технологий
Раздел 1 ПМ.01	Выполнение работ по монтажу, наладке, эксплуатации и обслуживанию локальных компьютерных сетей.

#### **4.5. Кадровое обеспечение образовательного процесса**

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): назначаются лица, имеющие высшее образование по соответствующему профилю либо дополнительное образование или повышение квалификации по профилю модуля.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: назначаются лица, имеющие высшее образование по соответствующему профилю либо дополнительное образование или повышение квалификации по профилю модуля.

Инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин: Основы теории информации, Технологии физического уровня передачи данных, Архитектура аппаратных средств, Операционные системы

Основы программирования и баз данных, Компьютерная графика, Организация, принципы построения и функционирования компьютерных сетей.

## 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.	Уметь настраивать и конфигурировать ПО для резервного копирования данных	<i>Практическое задание</i>
ПК 3.2. Осуществлять меры по защите компьютерных сетей от несанкционированного доступа.	Уметь анализировать систему и принимать решения	<i>Практическое задание</i>
ПК 3.3. Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.	Уметь настраивать антивирус и межсетевой экран по заданным параметрам	<i>Практическое задание</i>
ПК 3.4. Осуществлять мероприятия по защите персональных данных.	Применять способы по защите информации методами шифрования.	<i>Практическое задание</i>

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.