

Министерство образования Ставропольского края  
Государственное бюджетное профессиональное образовательное учреждение  
«Ставропольский региональный многопрофильный колледж»



**УТВЕРЖДАЮ**  
Директор ГБПОУ СРМК

Е.В. Бледных

«01» июня 2022 г.

### **Программа производственной практики**

#### **ПМ.03 Обеспечение информационной безопасности компьютерных сетей**

<b>Профессия</b>	09.01.02 Наладчик компьютерных сетей
<b>Курс</b>	3
<b>Группа</b>	НК-31

Ставрополь 2022

ОДОБРЕНО

На заседании кафедры  
«Программного обеспечения и  
информационных технологий»

Протокол № 9 от 24.05. 2022 г.

Зав. кафедрой



Т.М. Белянская

СОГЛАСОВАНО:

Методист



О.С. Диба

Разработчики: преподаватель ГБПОУ СРМК А.А.Коляко

Рекомендована Экспертным советом государственного бюджетного профессионального образовательного учреждения «Ставропольский региональный многопрофильный колледж»

Заключение Экспертного совета №13 от 27.05.2022 г.

Программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по профессии **09.01.02 Наладчик компьютерных сетей** укрупненной группы профессий **09.00.00 Информатика и вычислительная техника**

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение «Ставропольский региональный многопрофильный колледж»

## СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ .....	5
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ .....	7
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ .....	9
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ.....	16
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	22
6. ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РАБОЧУЮ ПРОГРАММУ .....	25

# **1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

## **ПМ.03 Обеспечение информационной безопасности компьютерных сетей**

### **1.1 Область применения программы**

Программа профессионального модуля (далее программа) – является частью основной профессиональной образовательной программы в соответствии с ФГОС 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 и др.;

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, резервному копированию и восстановлению 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 – 480 часа, в том числе:

максимальной учебной нагрузки обучающегося – 192 часа, включая:

обязательной аудиторной учебной нагрузки обучающегося – 128 часов;

в том числе в форме практической подготовки – 20 часов

самостоятельной работы обучающегося – 64 часа;

учебной и производственной практики (в форме практической подготовки)– 288 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 и др.
ПК 3.4	Осуществлять мероприятия по защите персональных данных
ОК 1	Понимать сущность и социальную значимость, 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)
ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде лично и профессионального конструктивного «цифрового следа»
ЛР 13	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ЛР 14	Использовать информационные технологии в профессиональной деятельности

ЛР15	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ЛР 16	Активно применяющий полученные знания на практике
ЛР 17	Способный анализировать производственную ситуацию, быстро принимать решения
ЛР18	Проявлять доброжелательность к окружающим, деликатность, чувство такта и готовность оказать услугу каждому кто в ней нуждается.

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов (макс. учебная нагрузка и практики)	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика		
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов <i>(если предусмотрена рассредоточенная практика)</i>	
			Всего, часов	в т.ч. лабораторные работы и практические занятия, час	в т.ч. в форме практической подготовки, ак. час					
1	2	3	4	5	6	7	8	9	10	
ПК 3.1 ПК 3.2	Раздел 1. Осуществление защиты информации в компьютерных сетях	194	90	50	14	32			72	-
ПК 3.3 ПК 3.4	Раздел 2 Применение средств для борьбы с вирусными заражениями	142	38	18	6	32			72	
	Производственная практика, часов <i>(если предусмотрена итоговая (концентрированная) практика)</i>	144								144
	<b>Всего:</b>	<b>480</b>	<b>128</b>	<b>68</b>	<b>20</b>	<b>64</b>			<b>144</b>	<b>144</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, курсовая работ (проект) (если предусмотрены)	Объем часов	Уровень освоения	
1	2	3		
ПМ.03 Обеспечение информационной безопасности компьютерных сетей		480		
Раздел 1. Осуществление защиты информации в компьютерных сетях		90		
МДК.03.01. Информационная безопасность персональных компьютеров и компьютерных сетей		128		
Тема 1.1. Основы информационной безопасности	<b>Содержание учебного материала</b>		14	
	1	Введение в курс. Основные понятия и определения. Задачи обеспечения информационной безопасности сетей.		1
	2	Исторический опыт защиты информации		
	3	Информационная война, методы и средства ее ведения. Информационное противоборство. Информационное оружие, его классификация, его возможности.		
	4	Основные направления обеспечения информационной безопасности объектов информационной сферы в условиях информационной войны.		
	5	Угрозы, уязвимости корпоративных сетей и систем		2
	6	Угрозы безопасности информационных систем, как уже развернутых, так и создаваемых на территории России.		
	7	Понятие политики безопасности. Основные типы политики безопасности. Модели безопасности		2
	Лабораторные работы не предусмотрено	-		
	Практические занятия.	6		

	<ol style="list-style-type: none"> <li>1. Анализ киберпреступлений в мировой практике</li> <li>2. «Анализ причин, видов, каналов утечки и искажения информации»</li> <li>3. Защита информации от несанкционированного доступа (в форме практической подготовки)</li> </ol>			
	<b>Контрольные работы не предусмотрено</b>	-		
Тема 1.2 Методы защиты информации в компьютерных сетях	<b>Содержание учебного материала</b>	14		
	1   Угрозы развитию отечественной индустрии информации			
	2   Классификация методов и средств защиты компьютерной информации. Требования к программным и аппаратным компонентам СКЗИ		2	
	3   Технические средства защиты от утечек информации по проводным линиям			
	4   Принципы обеспечения эффективности системы физической защиты, путь и стратегии нарушителя			
	5   Идентификация и аутентификация пользователей, ограничение доступа в систему		2	
	6   Способы и протоколы аутентификации. Способы аутентификации, использующие пароли и цифровые сертификаты. Биометрическая аутентификация		3	
	7   Поиск и обнаружение устройств негласного съема информации.			
	<b>Лабораторные работы не предусмотрено</b>	-		
	<b>Практические занятия</b>	24		
	<ol style="list-style-type: none"> <li>1. «Формальная постановка и решение задачи обеспечения информационной безопасности компьютерных систем».</li> <li>2. «определение критериев оценки защищенности компьютерных систем, методов и средств обеспечения их информационной безопасности»</li> <li>3. Анализ информационной инфраструктуры государств (в форме практической подготовки)</li> <li>4. Анализ технических средств и методов защиты информации.</li> <li>5. Исследование программно-аппаратных средств обеспечения информационной безопасности.</li> <li>6. Обнаружение уязвимостей по сигнатурам</li> <li>7. Исследование сетевых помехоподавляющих фильтров</li> <li>8. Исследование оптоэлектронного канала утечки информации</li> <li>9. Выполнение настроек межсетевых экранов</li> <li>10. Выполнение программной аутентификация и идентификация в сетевых операционных системах (в форме практической подготовки)</li> <li>11. Применение методов разграничения доступа в сетевых операционных системах (в форме практической подготовки)</li> <li>12. Подготовка предварительного варианта концепции информационной безопасности компании</li> </ol>			
	<b>Контрольные работы не предусмотрено</b>		-	
Тема 1.3 Криптографические методы защиты информации	<b>Содержание учебного материала</b>		6	
	1   Криптографическая защита			2
	2   Меры по обеспечению надежности функционирования систем криптографической защиты информа-			2

		ции		
	3	Управление ключами в криптографических системах защиты информации. Назначение, классификация, требования к ключам		2
	<b>Лабораторные работы не предусмотрено</b>		-	
	<b>Практические занятия.</b> 1. Стандарты шифрования данных. Назначение, алгоритм шифрования, основные режимы работы 2. Изучение ПО для шифрования данных 3. Настройка и работа в ПО для шифрования данных 4. Шифрование данных в глобальных сетях 5. Симметричные криптосистемы: шифры перестановки 6. Симметричные криптосистемы: шифры простой замены. 7. Симметричные криптосистемы: шифры сложной замены.		14	
	<b>Контрольные работы не предусмотрено</b>		-	
Тема 1.4. Резервное копирование и восстановление данных в компьютерных сетях	<b>Содержание учебного материала</b>		6	
	1	Обеспечение отказоустойчивости и целостности информационных систем		
	2	Организация резервного копирования данных (в форме практической подготовки)		1
	3	Механизмы резервного копирования данных		
	<b>Лабораторные работы не предусмотрено</b>		-	
	<b>Практические занятия.</b> 1. Исследование средств для выполнения резервного копирования данных 2. Выполнение резервного копирования и восстановления данных средствами Windows (в форме практической подготовки) 3. Анализ проблем безопасности при работе в облачном пространстве, при выполнении резервного копирования (в форме практической подготовки)		6	
	<b>Контрольные работы не предусмотрено</b>		-	
<b>Раздел 2. Применение средств для борьбы с вирусными заражениями</b>			38	
<b>МДК.03.01. Информационная безопасность персональных компьютеров и компьютерных сетей</b>			128	
Тема 2.1 Борьба с вирусным заражением информации	<b>Содержание учебного материала</b>		10	
	1.	Основные средства защиты программного обеспечения. Программно-технические меры защиты информационных процессов. Анализ уязвимости информационных систем и сетей.		2
	2	Компьютерные вирусы и защита от них.		2

	3	Типовые удаленные сетевые атаки и их характеристика		2	
	4	Антивирусные программы и комплексы. Построение систем антивирусной защиты компьютерных систем и сетей		3	
	5	Профилактические мероприятия для защиты компьютерных сетей от вредоносного ПО		2	
	<b>Лабораторные работы не предусмотрено</b>			-	
	<b>Практические занятия.</b> 1. Определение классификации программ по защите информации. 2. Выполнение работ со средствами защиты программного обеспечения. (в форме практической подготовки) 3. Применение антивирусной защиты в информационных системах (в форме практической подготовки) 4. Выполнение настройки антивирусного ПО (в форме практической подготовки) 5. Работа с анализаторами перехвата данных			12	
<b>Контрольные работы не предусмотрено</b>		-			
Тема 2.2. Организационно-правовое обеспечение информационной безопасности	<b>Содержание учебного материала</b>		12		
	1	Изучение международных стандартов информационного обмена.		2	
	Правовое обеспечение информационной безопасности в РФ				
	2	Информационная безопасность в условиях функционирования в России глобальных сетей.		3	
	3	Организационно-технические мероприятия обеспечения безопасности в компьютерных сетях. порядков планирования организационно-технических мероприятий по защите компьютерной информации		2	
	Ответственность за нарушение правил работы с документами ограниченного доступа				
	<b>Лабораторные работы не предусмотрено</b>			-	
<b>Практические занятия.</b> 1. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности 2. Исследование международных и государственных стандартов безопасности компьютерной информации. Классификация автоматизированных систем и нормативные требования по обеспечению безопасности компьютерной информации 3. Выполнение работ по заполнению технической и отчетной документации		6			
<b>Контрольные работы не предусмотрено</b>		-			
<b>Самостоятельная работа при изучении ПМ. 03</b> Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите.			64		
Тематика внеаудиторной самостоятельной работы: Политика безопасности, модели систем безопасности, реагирование на нарушение режима безопасности. Идентифика-					

<p>ция/аутентификация с помощью биометрических данных. Парольная аутентификация. Одноразовые пароли. Блочные шифры. Сеть Файстеля. нормативно-правовой базы РФ в области ИБ. Изучение международного законодательства в области ИБ. Стандарты информационной безопасности. "Оранжевая книга" как оценочный стандарт. Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Гармонизированные критерии Европейских стран.</p> <p>Вибро-акустические каналы утечки речевой информации. Устройства дистанционного съема речевой информации. Специальные и узконаправленные микрофоны, лазерные подслушивающие устройства, их основные характеристики и способы использования. Организационные мероприятия и технические средства акустической защиты помещений от прослушивания.</p> <p>Побочные электромагнитные излучения и наводки (ПЭМИН) как один из каналов утечки информации. Методы и средства обнаружения устройств перехвата акустической информации в технических каналах связи.</p> <p>Характеристики и правила эксплуатации устройств защиты акустической информации в телефонных линиях и радиоканалах. Типичные преступления в сфере компьютерной информации.</p> <p>Концепция защиты от НСД. Классы защищенности автоматизированных систем от НСД. Принципы организации автоматизированного рабочего места и защиты информационной техники. Аппаратные и программные средства защиты компьютерной информации от НСД.</p> <p>Компьютерные вирусы и программы типа "Троянский конь", основные виды и принцип их действия. Профилактические мероприятия. Средства обнаружения и лечения компьютера от вирусов. Антивирусные программы. Настройки антивирусных программ.</p>	
<p><b>Учебная практика</b></p> <p><b>Виды работ:</b></p> <p>Выполнение работ с ресурсами Интернет по информационной безопасности. Выполнение работ по защите от угроз компьютерной безопасности и атак в сетях. Обеспечение информационной безопасности в облачном пространстве. Осуществление мероприятий по определению рисков информационной безопасности.</p> <p>Выполнение работ по систематизации структуры органов защиты информации предприятий.</p> <p>Выполнение работ по выявлению причинно-следственных связей процессов информатизации общества и компонентов информационной безопасности.</p> <p>Осуществление мероприятий по определению объектов защиты.</p> <p>Осуществление мероприятий по контролю эффективности защиты информации.</p> <p>Применение принципов защищенного электронного документооборота в телекоммуникационных сетях и алгоритмов постановки электронной подписи.</p> <p>Использование современного программного обеспечения для защиты авторских прав</p> <p>Осуществление мероприятий по защите от взлома компьютерных систем</p> <p>Выполнение процедур аутентификации пользователя на основе пароля. Выполнение работ по построению системы контроля целостности данных. Осуществление мероприятий по криптографической защите данных. Реализация криптографических алгоритмов.</p> <p>Реализация резервного копирования и восстановления данных</p> <p>Выполнение работ по различным видам нарушений работоспособности удаленного компьютера со стороны вредоносных программ.</p> <p>Выполнение работ по выявлению особенностей поведения вирусных и других вредоносных программ. Выполнение работ по предупреждению и обнаружению вирусных угроз. Проведение сравнительного анализа пакетов антивирусных программ.</p> <p>Выполнение работ по выявлению особенностей воздействия программных закладок на компьютеры</p> <p>Построение концепции информационной безопасности предприятия. Выполнение работ по заполнению отчетной и технической документации.</p>	<p>144</p>

Осуществление мероприятий по организации работы с персоналом в системе информационной безопасности.	
<p><b>Производственная практика</b></p> <p><b>Виды работ:</b></p> <p>Выполнение работ по изучению и анализу инструкций по технике безопасности на рабочих местах, схем аварийных выходов и мест нахождения пожарного инвентаря.</p> <p>Разработка модели структуры защиты информации предприятия.</p> <p>Выполнение работ с нормативно-правовой документацией, которая имеется на предприятии для обеспечения информационной безопасности.</p> <p>Выполнение работ по изучению и анализу должностных инструкций сотрудников вычислительного центра;</p> <p>Выполнение работ по описанию объектов информационной безопасности.</p> <p>Осуществление мероприятий по определению и описанию особенностей (профиля) каждой из групп вероятных нарушителей.</p> <p>Осуществление мероприятий по выявлению основных видов угроз информационной безопасности Предприятия.</p> <p>Выполнение работ по разработке модели организационного обеспечения информационной безопасности.</p> <p>Выявление, анализ и составление таблицы средств комплексной защиты от потенциальных угроз.</p> <p>Оценка эффективности системы информационной безопасности.</p> <p>Осуществление мероприятий по резервному копированию и восстановлению данных.</p> <p>Проверка компьютеров антивирусными программами.</p>	144
<b>Курсовое проектирование</b> <i>не предусмотрено</i>	-
<b>Всего:</b>	480

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

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

Реализация программы модуля предполагает наличие лаборатории **информационной безопасности**

#### **Лаборатории информационной безопасности:**

Оборудование учебного кабинета и рабочих мест кабинета

- посадочных мест по количеству обучающихся 25;
- рабочее место преподавателя 1;
- примерная проектная документация;

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 – операционные системы Windows, UNIX, антивирусные программы, криптоалгоритмы; объединенные сети (Cisco или др.), сетей доступа (ADSL или др., возможность конфигурации и администрирования сетевых операционных систем, межсетевые экраны)
- Компьютер учителя (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО – операционные системы Windows, UNIX, антивирусные программы, криптоалгоритмы, объединенные сети (Cisco или др.), сетей доступа (ADSL или др., возможность конфигурации и администрирования сетевых операционных систем, межсетевые экраны)
- 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, антивирусное ПО.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением
- интерактивная доска
- проектор
- примерная проектная документация

## **4.2. Информационное обеспечение обучения**

### **Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

#### **Основная литература**

1. Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. — 218 с. — ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/118458.html> (дата обращения: 04.04.2022). — Режим доступа: для авторизир. пользователей.

2. Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1189341> (дата обращения: 12.03.2022). — Режим доступа: по подписке.

3. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/102207.html> (дата обращения: 04.04.2022). — Режим доступа: для авторизир. Пользователей

4. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учебник / А.В. Назаров, А.Н. Енгальчев, В.П. Мельников. — Москва : КУРС : ИНФРА-М, 2022. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-06-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1860128> (дата обращения: 01.04.2022). — Режим доступа: по подписке.

#### **Дополнительные источники:**

5. Мэйволд, Э. Безопасность сетей : учебное пособие для СПО / Э. Мэйволд. — Саратов : Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/102183.html> (дата обращения: 04.04.2022). — Режим доступа: для авторизир. Пользователей

6. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL:

<https://znanium.com/catalog/product/1189327> (дата обращения: 26.03.2022). – Режим доступа: по подписке.

7. Емельянова, Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-466-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189325> (дата обращения: 26.03.2022). – Режим доступа: по подписке.

8. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189328> (дата обращения: 26.03.2022). – Режим доступа: по подписке.

9. Баранова, Е. К. Основы информационной безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2022. — 202 с. — (Среднее профессиональное образование). — DOI: <https://doi.org/10.29039/01806-4>. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1860126> (дата обращения: 01.04.2022). – Режим доступа: по подписке.

10. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1859978> (дата обращения: 01.04.2022). – Режим доступа: по подписке.

### **Печатные издания**

11. Мельников, В.П. Информационная безопасность: учебник /В.П. Мельников, А.И. Куприянов; под ред.В.П. Мельникова.-2-е изд., перераб. и доп.- Москва: КНОРУС, 2018.-268 с.- ISBN 978-5-406-05072-9.- (Среднее профессиональное образование). – Текст: непосредственный.

12. Эксплуатация объектов сетевой инфраструктуры: учебник для студ. учреждений сред.проф. образования / А. В. Назаров, А.И. Куприянов, В. П. Мельников, А. Н. Енгальчев.– Москва: Издательство Академия, 2018. — 368 с. [1] с.: ил. - (Топ-50:Профессиональное образование).- ISBN 978-5-4468-6458-4.-Текст: непосредственный

### **Журналы**

13. ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ: научный электронный журнал/учредители Воронежский государственный технический университет (Воронеж) .-ISSN: 1682-7813.- Число выпусков в год: 4,-Воронеж, 1998.- URL: <https://elibrary.ru/contents.asp?id=44034209> (дата обращения: 09.03.2022). – Режим доступа: по подписке

14. Медиа. Информация. Коммуникация: МИК: международный электронный научно образовательный журнал / учредитель Московский государственный гуманитарный университет им. М. А. Шолохова; редакция: И. В. Жилавская (главный редактор) [и др.]. - Москва, 2014 - . - Ежемес. - ISSN 2313-755X. - URL:<http://mic.org.ru/index.php> (дата обращения: 02.03.2022). - Текст : электронный.

#### **Нормативно-правовые документы**

1. Конституция Российской Федерации. <http://dehack.ru/intro/>
2. Уголовный кодекс Российской Федерации. <http://dehack.ru/intro/>
3. Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации». <http://dehack.ru/intro/>
4. Федеральный закон РФ 27.07.2006 г. N 152-ФЗ «О персональных данных». <http://dehack.ru/intro/>
5. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». <http://dehack.ru/intro/>
6. Руководящие документы ФСТЭК РФ: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#>
7. Доктрина информационной безопасности Российской Федерации <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=28679>
8. BS ISO/IEC 27005:20008 Ru. Информационные технологии - Методы обеспечения безопасности - Управление рисками информационной безопасности. [http://gtrust.ru/show\\_good.php?idtov=1137](http://gtrust.ru/show_good.php?idtov=1137).

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

При реализации компетентностного подхода предусматривается использование в образовательном процессе активных форм проведения занятий с применением электронных образовательных ресурсов, деловых и ролевых игр, индивидуальных и групповых проектов, анализа производственных ситуаций, психологических и иных тренингов, групповых дискуссий в сочетании с внеаудиторной работой для формирования общих и профессиональных компетенций обучающихся.

Учебная практика (производственное обучение) и производственная практика проводятся образовательным учреждением, при освоении обучающимися профессиональных компетенций в рамках профессиональных модулей, и могут быть реализованы, как концентрировано, так и рассредоточено, чередуясь с теоретическими занятиями в рамках профессиональных модулей.

Производственная практика должна проводиться в организациях, направление деятельности которых соответствует профилю подготовки обучающихся.

#### **4.4. Кадровое обеспечение образовательного процесса**

Наличие высшего профессионального образования, соответствующего направлению подготовки «Информатика и вычислительная техника».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов

Мастера: наличие 4-5 квалификационного разряда с обязательной стажировкой в профильных организациях не реже 1 раза в 3 года. Опыт деятельности в организациях соответствующей профессиональной сферы обязателен.

**а. Используемые активные и интерактивные формы занятий, образовательные технологии (методы и приемы):**

Вид занятия*	Используемые активные и интерактивные образовательные технологии
ТО	<p>Проблемная лекция, групповые дискуссии, лекция-провокация, разбор конкретных ситуаций, метод «круглого стола», семинар, мультимедийная презентация, коллективное взаимодействие (работа в парах, в тройках, изменяемые тройки), разыгрывание ситуаций.</p> <p><b>технология витагенного обучения</b> (актуализация жизненного опыта, сравнение объектов, работа по сопоставлению объектов, группировка и классификация, рефлексия); <b>интерактивные технологии обучения</b> (постановка проблемы, дискуссия, обсуждение проблемы в микрогруппах, эвристическая беседа, групповая работа с иллюстративным материалом); <b>технология ситуационного обучения</b> (анализ конкретных ситуаций; перенос усвоенных знаний в новую ситуацию);</p> <p><b>технология коллективного генерирования идей</b>(-«Мозговой штурм»решение эвристических задач, планирование действий, рефлексия); <b>технология ситуационного обучения</b> (анализ конкретных ситуаций, перенос усвоенных знаний в новую ситуацию), мультимедийные лекции</p>
ПР	<p>Уроки-соревнования, технология контекстного обучения ( разбор конкретных ситуаций, анализ конкретных задач, имитационное моделирование), индивидуальные и групповые проекты, частично-поисковая и исследовательская технологии, создание проблемной ситуации, <b>Практика с выполнением должностных обязанностей</b>, компьютерные симуляции (имитации)</p>
ЛР	не предусмотрено
СР	<p>Анализ реальных проблемных ситуаций, интернет-технология, работа в команде, тест-тренинги, , разыгрывание ситуаций, проектная технология.</p>
УП	<p>Обучение в командах достижений, Метод Jigsaw «Пила», проектный метод, <b>интерактивные технологии обучения, ИКТ технологии, технология витагенного обучения, Практика с выполнением должностных обязанностей, компьютерные симуляции (имитации)</b></p>

\*) ТО – теоретическое обучение, ПР – практические занятия, СР- самостоятельная работа, УП – учебная практика

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

<b>Результаты (освоенные профессиональ- ные компетенции)</b>	<b>Основные показатели оцен- ки результата</b>	<b>Формы и методы контроля и оценки</b>
ПК 3.1. Обеспечивать резерв- ное копирование данных	Владеть технологией резерв- ного копирования данных	<i>Экспертная оценка резуль- татов деятельности обу- чающихся в процессе освое- ния образовательной про- граммы:</i> <i>-на практических занятиях</i> <i>- при выполнении работ на</i> <i>различных этапах производ- ственной практики,</i> <i>-зачет по разделу практики</i>
ПК 3.2 Осуществлять меры по защите компьютерных сетей от несанкционированного досту- па	-Четкое понимание проблем информационной безопасно- сти в компьютерных сетях - Грамотно выявлять, класси- фицировать и анализировать угрозы информационной безопасности и формы их про- явления - Обоснованность разрабаты- ваемой политики в области информационной безопасно- сти	<i>Экспертная оценка резуль- татов деятельности обу- чающихся в процессе освое- ния образовательной про- граммы:</i> <i>-на практических занятиях</i> <i>- при выполнении работ на</i> <i>различных этапах производ- ственной практики,</i> <i>-зачет по разделу практики</i>
ПК 3.3 Применять специали- зированные средства для борьбы с вирусами, несанкционирован- ными рассылками электрон- ной почты, вредоносными программами и др.	- Обоснованность выбора и использования пакетов при- кладных программ для безо- пасного администрирования сетевых операционных систем - Построение системы антиви- русной защиты компьютерных сетей - Обеспечение программными и программно - аппаратными методами безопасности сетей доступа	<i>Экспертная оценка резуль- татов деятельности обу- чающихся в процессе освое- ния образовательной про- граммы:</i> <i>-на практических занятиях</i> <i>- при выполнении работ на</i> <i>различных этапах производ- ственной практики,</i> <i>-зачет по разделу практики</i>
ПК.3.4 Осуществлять мероприятия по защите персональных данных	-Выбор механизмов и средств обеспечения информационной безопасности - Владеть сервисами, обеспе- чивающими информационную безопасность в компьютерных системах и сетях - Владеть технологией аутен- тификации - Обеспечивать технологию защиты межсетевых обмена	<i>Экспертная оценка резуль- татов деятельности обу- чающихся в процессе освое- ния образовательной про- граммы:</i> <i>-на практических занятиях</i> <i>- при выполнении работ на</i> <i>различных этапах производ- ственной практики,</i> <i>-зачет по разделу практики</i>

	<p>данными</p> <ul style="list-style-type: none"> <li>- Грамотно оформлять документацию в области информационной безопасности</li> </ul>	
--	--	--

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.

<b>Результаты (освоенные общие компетенции)</b>	<b>Основные показатели оценки результата</b>	<b>Формы и методы контроля и оценки</b>
ОК1. Понимать сущность и социальную значимость, проявлять к ней устойчивый интерес	<ul style="list-style-type: none"> <li>- участие в работе научно-студенческих обществ,</li> <li>-выступления на научно-практических конференциях,</li> <li>-участие во внеурочной деятельности связанной с будущей профессией/ специальностью (конкурсы профессионального мастерства, выставки и т.п.)</li> <li>- высокие показатели производственной деятельности</li> </ul>	<p>Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:</p> <ul style="list-style-type: none"> <li>-на практических занятиях ( при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.)</li> <li>- при выполнении работ на различных этапах производственной практики</li> </ul>
ОК2. Организовывать собственную деятельность исходя из цели и способов ее достижения, определенных руководителем	- выбор и применение методов и способов решения профессиональных задач, оценка их эффективности и качества	
ОК 3. Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы	<ul style="list-style-type: none"> <li>-анализ профессиональных ситуаций;</li> <li>-решение стандартных и нестандартных профессиональных задач</li> </ul>	
ОК 4. Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач	<p>эффективный поиск необходимой информации;</p> <ul style="list-style-type: none"> <li>-использование различных источников, включая электронные, при изучении теоретического материала и прохождении различных этапов производственной практики</li> </ul>	
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	- использование в учебной и профессиональной деятельности различных видов программного обеспечения, в том числе специального, при оформлении презентации всех видов работ	

<p>ОК 6. Работать в команде, эффективно общаться с коллегами, руководством, клиентами</p>	<p>взаимодействие:</p> <ul style="list-style-type: none"> <li>- с обучающимися при проведении деловых игр, выполнении коллективных заданий (проектов),</li> <li>- с преподавателями, мастерами в ходе обучения,</li> <li>- с потребителями и коллегами в ходе производственной практики</li> </ul>	
<p>ОК 7. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)</p>	<p>Исполнение воинской обязанности, в том числе с применением полученных профессиональных знаний (для юношей)</p>	

**6. ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РАБОЧУЮ ПРОГРАММУ  
ПО ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ**

Дата	Содержание изменений	Содержание обновления компонента ППССЗ (ППКРС)	Обоснование обновления
«18 » мая 2021 г.	Изменение литературы	<p>В основные источники литературы внести источники:</p> <p>Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н.А. Руденков [и др.].. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <a href="http://www.iprbookshop.ru/102207.html">http://www.iprbookshop.ru/102207.html</a> (дата обращения: 26.03.2021). — Режим доступа: для авторизир. пользователей</p> <hr/> <p>Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учебник / А.В. Назаров, А.Н. Енгальчев, В.П. Мельников. - Москва : КУРС; ИНФРА-М, 2019. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-16-105198-6. - Текст : электронный. - URL: <a href="https://new.znaniium.com/catalog/product/1027558">https://new.znaniium.com/catalog/product/1027558</a> (дата обращения: 30.03.2020) Полный контингент</p> <p>В дополнительные источники литературы внести источники:</p> <p>СПО / Э. Мэйволд. — Саратов : Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <a href="http://www.iprbookshop.ru/102183.html">http://www.iprbookshop.ru/102183.html</a> (дата обращения: 26.03.2021). — Режим доступа: для авторизир. пользователей</p> <p>6. Суворова Г.М. Информационная безопасность : учебное пособие / Суворова Г.М.. — Саратов : Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <a href="http://www.iprbookshop.ru/86938.html">http://www.iprbookshop.ru/86938.html</a> (дата обращения: 26.03.2021). — Режим доступа: для авторизир. пользователей. - DOI: <a href="https://doi.org/10.23682/86938">https://doi.org/10.23682/86938</a></p> <p>Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ :</p>	<p>Приказ Министерства просвещения Российской Федерации от 17.12.2020 № 747 «О внесении изменений в федеральные государственные образовательные стандарты среднего профессионального образования»;</p> <p>Решение кафедры, протокол № 10 от «18 » мая 2021 г.</p>

ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189327> (дата обращения: 26.03.2021). – Режим доступа: по подписке.

Емельянова, Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-466-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189325> (дата обращения: 26.03.2021). – Режим доступа: по подписке.

Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189328> (дата обращения: 26.03.2021). – Режим доступа: по подписке.

Баранова, Е. К. Основы информационной безопасности : учебник / Е. К. Баранова, А. В. Бабаш. - Москва : РИОР : ИНФРА-М, 2021. — 202 с. — (Среднее профессиональное образование). - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1209579> (дата обращения: 26.03.2021). – Режим доступа: по подписке.

Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1191479> (дата обращения: 26.03.2021). – Режим доступа: по подписке.

Печатные издания

Богомазова, Г.Н. Обеспечение информационной безопасности компьютерных сетей: учебник для студ. учреждений сред. проф. образования / Г.Н Богомазова– М.: Издательский центр «Академия, 2017.-224 с.- (Профессиональное образование).-ISBN978-5-4468-3453-2.-Текст: непосредственный.

Печатные издания

Эксплуатация объектов сетевой инфраструктуры: учебник для студ. учреждений

		<p>сред.проф. образования / А. В. Назаров, А.И. Куприянов, В. П. Мельников, А. Н. Енгальчев.– Москва: Издательство Академия, 2018. – 368 с. [1] с.: ил. - (Топ-50:Профессиональное образование).- ISBN 978-5-4468-6458-4.-Текст: непосредственный</p> <p>Журналы</p> <p><b>ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ:</b> научный электронный журнал/учредители Воронежский государственный технический университет (Воронеж) .-ISSN: 1682-7813.- Число выпусков в год: 4,-Воронеж, 1998.- URL: <a href="https://elibrary.ru/contents.asp?id=44034209">https://elibrary.ru/contents.asp?id=44034209</a> (дата обращения: 09.03.2021). – Режим доступа: по подписке</p> <p>Медиа. Информация. Коммуникация: МИК: международный электронный научно образовательный журнал / учредитель Московский государственный гуманитарный университет им. М. А. Шолохова ; редакция: И. В. Жилавская (главный редактор) [и др.]. - Москва, 2014 - . - Ежемес. - ISSN 2313-755X. - URL: <a href="http://mic.org.ru/index.php">http://mic.org.ru/index.php</a> (дата обращения: 02.10.2014). - Текст : электронный.</p>	
18 мая 2021	Выделены практические работы в форме практической подготовки	20 часов	