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

УТВЕРЖДАЮ
Директор ГБПОУ СРМК
_____Е.В. Бледных
«___» _____ 2021 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Обеспечение информационной безопасности компьютерных сетей

Профессия	09.01.02 Наладчик компьютерных сетей
Курс	3
Группа	НК-31

Ставрополь 2021

ОДОБРЕНО
кафедрой
«Программного обеспечения и
информационных технологий»

Протокол № 11 от 15 июня 2021 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 № 12 от 21 июня 2021 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 8
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 15
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)

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, ак.часов	Производственная, ак.часов *(если предусмотрена рассредоточенная практика)*
			Всего, ак.часов	**в т.ч.** в форме практической подготовки, ак.час	**Лабораторные работы и практические занятия, ак.час**			
1	2	3	4	5	6	7	9	10
ПК 3.1 ПК 3.2	**Раздел 1.** .Осуществление защиты информации в компьютерных сетях	**194**	**90**	**14**	50	**32**	**72**	-
ПК 3.3 ПК 3.4	**Раздел 2** Применение средств для борьбы с вирусными заражениями	**142**	**38**	**6**	**18**	**32**	**72**	
	Производственная практика, часов *(если предусмотрена итоговая (концентрированная) практика)*	**144**						**144**
	Всего:	**480**	**128**	**20**	**68**	**64**	**144**	**144**

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	**Содержание учебного материала**		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	

	1. Анализ киберпреступлений в мировой практике 2. «Анализ причин, видов, каналов утечки и искажения информации» 3. Защита информации от несанкционированного доступа (в форме практической подготовки)		
	Контрольные работы *не предусмотрено*	-	
Тема 1.2 Методы защиты информации в компьютерных сетях	**Содержание учебного материала**		
	1 Угрозы развитию отечественной индустрии информации		
	2 Классификация методов и средств защиты компьютерной информации. Требования к программным и аппаратным компонентам СКЗИ	14	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 аутенфикации. Способы аутенфикации, использующие пароли и цифровые сертификаты. Биометрическая аутенфикация		3
	7 Поиск и обнаружение устройств негласного съема информации.		
	Лабораторные работы *не предусмотрено*	-	
	Практические занятия 1. «Формальная постановка и решение задачи обеспечения информационной безопасности компьютерных систем». 2. «определение критериев оценки защищенности компьютерных систем, методов и средств обеспечения их информационной безопасности» 3. Анализ информационной инфраструктуры государств (в форме практической подготовки) 4. Анализ технических средств и методов защиты информации. 5. Исследование программно-аппаратных средств обеспечения информационной безопасности. 6. Обнаружение уязвимостей по сигнатурам 7. Исследование сетевых помехоподавляющих фильтров 8. Исследование оптоэлектронного канала утечки информации 9. Выполнение настроек межсетевых экранов 10. Выполнение программной аутентификация и идентификация в сетевых операционных системах (в форме практической подготовки) 11. Применение методов разграничения доступа в сетевых операционных системах (в форме практической подготовки) 12. Подготовка предварительного варианта концепции информационной безопасности компании	24	
	Контрольные работы *не предусмотрено*	-	
Тема 1.3 Криптографические методы защиты информации	**Содержание учебного материала**		
	1 Криптографическая защита	6	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
	Лабораторные работы *не предусмотрено*		-	
	Практические занятия. 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	
	Контрольные работы *не предусмотрено*		-	
Тема 1.4. Резервное копирование и восстановление данных в компьютерных сетях	**Содержание учебного материала**		6	
	1	Обеспечение отказоустойчивости и целостности информационных систем		
	2	Организация резервного копирования данных (в форме практической подготовки)		1
	3	Механизмы резервного копирования данных		
	Лабораторные работы *не предусмотрено*		-	
	Практические занятия. 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	
	Контрольные работы *не предусмотрено*		-	
Раздел 2. Применение средств для борьбы с вирусными заражениями			*38*	
МДК.03.01. Информационная безопасность персональных компьютеров и компьютерных сетей			*128*	
Тема 2.1 Борьба с вирусным заражением информации	**Содержание учебного материала**		*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
	Лабораторные работы *не предусмотрено*		-	
	Практические занятия. 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*	
	Контрольные работы *не предусмотрено*		-	
Тема 2.2. Организационно-правое обеспечение информационной безопасности		**Содержание учебного материала**	*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. порядок планирования организационно-технических мероприятий по защите компьютерной информации		2
		Ответственность за нарушение правил работы с документами ограниченного доступа		
	Лабораторные работы *не предусмотрено*		-	
	Практические занятия. 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*	
	Контрольные работы *не предусмотрено*		-	
Самостоятельная работа при изучении ПМ. 03 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-				

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. 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. Побочные электромагнитные излучения и наводки (ПЭМИН) как один из каналов утечки информации. Методы и средства обнаружения устройств перехвата акустической информации в технических каналах связи. Характеристики и правила эксплуатации устройств защиты акустической информации в телефонных линиях и радиоканалах. Типичные преступления в сфере компьютерной информации. 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. 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.	
Учебная практика **Виды работ:** 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. Выполнение работ по систематизации структуры органов защиты информации предприятий. Выполнение работ по выявлению причинно-следственных связей процессов информатизации общества и компонентов информационной безопасности. Осуществление мероприятий по определению объектов защиты. Осуществление мероприятий по контролю эффективности защиты информации. Применение принципов защищенного электронного документооборота в телекоммуникационных сетях и алгоритмов постановки электронной подписи. Использование современного программного обеспечения для защиты авторских прав Осуществление мероприятий по защите от взлома компьютерных систем Выполнение процедур аутенфикации пользователя на основе пароля. Выполнение работ по построению системы контроля целостности данных. Осуществление мероприятий по криптографической защите данных. Реализация криптографических алгоритмов. Реализация резервного копирования и восстановления данных Выполнение работ по различным видам нарушений работоспособности удаленного компьютера со стороны вредоносных программ. 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. Выполнение работ по выявлению особенностей воздействия программных закладок на компьютеры Построение концепции информационной безопасности предприятия. Выполнение работ по заполнению отчетной и технической документации.	144

Осуществление мероприятий по организации работы с персоналом в системе информационной безопасности.	
Производственная практика **Виды работ:** Выполнение работ по изучению и анализу инструкций по технике безопасности на рабочих местах, схем аварийных выходов и мест нахождения пожарного инвентаря. Разработка модели структуры защиты информации предприятия. Выполнение работ с нормативно-правовой документацией, которая имеется на предприятии для обеспечения информационной безопасности. Выполнение работ по изучению и анализу должностных инструкций сотрудников вычислительного центра; Выполнение работ по описанию объектов информационной безопасности. Осуществление мероприятий по определению и описанию особенностей (профиля) каждой из групп вероятных нарушителей. Осуществление мероприятий по выявлению основных видов угроз информационной безопасности Предприятия. Выполнение работ по разработке модели организационного обеспечения информационной безопасности. Выявление, анализ и составление таблицы средств комплексной защиты от потенциальных угроз. Оценка эффективности системы информационной безопасности. Осуществление мероприятий по резервному копированию и восстановлению данных. Проверка компьютеров антивирусными программами.	144
Курсовое проектирование *не предусмотрено*	-
Всего:	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. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учебник / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. - Москва : КУРС; ИНФРА-М, 2019. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-16-105198-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1027558 (дата обращения: 30.03.2020)

2. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н.А. Руденков [и др.].. — Саратов : Профобразование, 2021. — 368 c. — ISBN 978-5-4488-1014-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102207.html (дата обращения: 26.03.2021). — Режим доступа: для авторизир. пользователей

Дополнительные источники:

3. Суворова Г.М. Информационная безопасность : учебное пособие / Суворова Г.М.. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html (дата обращения: 26.03.2021). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/86938

4. Баранова, Е. К. Основы информационней 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.

5. 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.

6. 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.

7. СПО / Э. Мэйволд. — Саратов : Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102183.html (дата обращения: 26.03.2021). — Режим доступа: для авторизир. пользователей

8. 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.

9. 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: 26.03.2021). – Режим доступа: по подписке.

Печатные издания

10. 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.

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

Журналы

12. 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: 09.03.2021). – Режим доступа: по подписке

13. Медиа. Информация. Коммуникация: МИК: международный электронный научно образовательный журнал / учредитель Московский государственный гуманитарный университет им. М. А. Шолохова ; редакционная коллегия: И. В. Жилавская (главный редактор) [и др.]. - Москва, 2014 - . - Ежемес. - ISSN 2313-755X. - URL: http://mic.org.ru/index.php (дата обращения: 02.10.2014). - 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/IES 27005:20008 Ru. Информационные технологии - Методы обеспечения безопасности - Управление рисками информационной безопасности. 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	Проблемная лекция, групповые дискуссии, лекция- провокация, разбор конкретных ситуаций, метод «круглого стола», семинар, мультимедийная презентация, коллективное взаимообучение (работа в парах, в тройках, изменяемые тройки), разыгрывание ситуаций. **технология витагенного обучения** (актуализация жизненного опыта ,сравнение объектов, работа по сопоставлению объектов, группировка и классификация, рефлексия); **интерактивные технологии обучения** (постановка проблемы, дискуссия ,обсуждение проблемы в микрогруппах, эвристическая беседа, групповая работа с иллюстративным материалом); **технология ситуационного обучения** (анализ конкретных ситуаций; перенос усвоенных знаний в новую ситуацию); **технология коллективного генерирования идей**(-«Мозговой штурм»решение эвристических задач, планирование действий, рефлексия); **технология ситуационного обучения** (анализ конкретных ситуаций, перенос усвоенных знаний в новую ситуацию), мультимедийные лекции
ПР	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, **Практика с выполнением должностных обязанностей,** компьютерные симуляции (имитации)
ЛР	не предусмотрено
СР	Анализ реальных проблемных ситуаций, интернет-технология, работа в команде, тест-тренинги, , разыгрывание ситуаций, проектная технология.
УП	Обучение в командах достижений, Метод Jigsaw «Пила», проектный метод, **интерактивные технологии обучения, ИКТ технологии, технология витагенного обучения, Практика с выполнением должностных обязанностей,** компьютерные симуляции (имитации)

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

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	Владеть технологией резервного копирования данных	*Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:* *-на практических занятиях* *- при выполнении работ на различных этапах производственной практики,* *-зачет по разделу практики*
ПК 3.2 Осуществлять меры по защите компьютерных сетей от несанкционированного доступа	-Четкое понимание проблем информационной безопасности в компьютерных сетях - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления - Обоснованность разрабатываемой политики в области информационной безопасности	*Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:* *-на практических занятиях* *- при выполнении работ на различных этапах производственной практики,* *-зачет по разделу практики*
ПК 3.3 Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами и др.	- Обоснованность выбора и использования пакетов прикладных программ для безопасного администрирования сетевых операционных систем - Построение системы антивирусной защиты компьютерных сетей - Обеспечение программными и программно - аппаратными методами безопасности сетей доступа	*Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:* *-на практических занятиях* *- при выполнении работ на различных этапах производственной практики,* *-зачет по разделу практики*
ПК.3.4 Осуществлять мероприятия по защите персональных данных	-Выбор механизмов и средств обеспечения информационной безопасности - Владеть сервисами, обеспечивающими информационную безопасность в компьютерных системах и сетях - Владеть технологией аутентификации - Обеспечивать технологию защиты межсетевого обмена	*Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы:* *-на практических занятиях* *- при выполнении работ на различных этапах производственной практики,* *-зачет по разделу практики*

	данными - Грамотно оформлять документацию в области информационной безопасности	

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.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК1. Понимать сущность и социальную значимость, проявлять к ней устойчивый интерес	- участие в работе научно-студенческих обществ, -выступления на научно-практических конференциях, -участие во внеурочной деятельности связанной с будущей профессией/ специальностью (конкурсы профессионального мастерства, выставки и т.п.) - высокие показатели производственной деятельности	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: -на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.) - при выполнении работ на различных этапах производственной практики
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	-анализ профессиональных ситуаций; -решение стандартных и нестандартных профессиональных задач	
ОК 4. Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач	эффективный поиск необходимой информации; -использование различных источников, включая электронные, при изучении теоретического материала и прохождении различных этапов производственной практики	
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	

ОК 6. Работать в команде, эффективно общаться с коллегами, руководством, клиентами	взаимодействие: - с обучающимися при проведении деловых игр, выполнении коллективных заданий (проектов), - с преподавателями, мастерами в ходе обучения, - с потребителями и коллегами в ходе производственной практики	
ОК 7.Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)	Исполнение воинской обязанности, в том числе с применением полученных профессиональных знаний (для юношей)	

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

		(дата обращения: 26.03.2021). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/86938 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: 26.03.2021). – 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 информационней 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/1191	

		479 (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 сред.проф. образования / А. В. Назаров, А.И. Куприянов, В. П. Мельников, А. Н. Енгалычев.– Москва: Издательство Академия, 2018. – 368 с. [1] с.: ил. - (Топ-50:Профессиональное образование).- ISBN 978-5-4468-6458-4.- Текст: непосредственный Журналы 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: 09.03.2021). – Режим доступа: по подписке Медиа. Информация. Коммуникация: МИК: международный электронный научно образовательный журнал / учредитель Московский государственный гуманитарный университет им. М. А. Шолохова ; редакционная коллегия: И. В. Жилавская (главный редактор) [и др.]. - Москва, 2014 - . - Ежемес. - ISSN 2313-755X. - URL: http://mic.org.ru/index.php (дата обращения: 02.10.2014). - Текст : электронный.	
18 мая 2021	Выделены практические работы в форме практической подготовки	20 часов	