Министерство образования Ставропольского края

Государственное бюджетное профессиональное образовательное учреждение
«Ставропольский региональный многопрофильный колледж»

УТВЕРЖДАЮ

Директор ГБПОУ СРМК
_____Е.В. Бледных

«20» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Обеспечение информационной безопасности компьютерных сетей

Ставрополь
2020

ОДОБРЕНО
на заседании кафедры
«Программного обеспечения и
информационных технологий»

Протокол № 1 от .08.2020 г.
Зав. кафедрой
_____ О.В. Краскова

СОГЛАСОВАНО:
Методист
_____О.С. Диба

Разработчики: преподаватель ГБПОУ СРМК Руденко Е.Ю., Есауленко Н.А.

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

Заключение Экспертного совета № от августа 2020 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»

Разработчики:

Руденко Е.Ю., преподаватель

СОДЕРЖАНИЕ

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;

самостоятельной работы обучающегося – 64 часа;

учебной и производственной практики – 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, часов	Производственная (по профилю специальности), часов *если предусмотрена рассредоточенная практика)*
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 3.1 ПК 3.2	**Раздел 1.** .Осуществление защиты информации в компьютерных сетях	194	90	50	-	32	–	72	-
ПК 3.3 ПК 3.4	**Раздел 2** Применение средств для борьбы с вирусными заражениями	142	38	18		32		72	
	Производственная практика (по профилю специальности), часов *(если предусмотрена итоговая (концентрированная) практика)*	144							144
	Всего:	480	128	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			580	
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			
	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 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 11. Применение методов разграничения доступа в сетевых операционных системах 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		2
	2	Меры по обеспечению надежности функционирования систем криптографической защиты информации	6	2
	3	Управление ключами в криптографических системах защиты информации. Назначение, классифика-		2

		ция, требования к ключам		
	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		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 3. Анализ проблем безопасности при работе в облачном пространстве, при выполнении резервного копирования		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		3

		систем и сетей		
	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. 3. Применение антивирусной защиты в информационных системах 4. Выполнение настройки антивирусного ПО 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 организацион- но-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. Идентификация/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. Осуществление мероприятий по организации работы с персоналом в системе информационной безопасности.	144

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:	580

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. Богомазова Г.Н. Обеспечение информационной безопасности компьютерных сетей: учеб. для студ. учреждений сред. проф. образования: / Г.Н. Богомазова. - М.: Издательский центр «Академия», 2017

Дополнительная литература

2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: 2016.

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.

Учебная литература IPR books

Электронные ресурсы

1. Беспроводные сети Wi-Fi [Электронный ресурс] / А. В. Пролетарский, И. В. Баскаков, Р. А. Федотов [и др.]. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 284 c. — 978-5-94774-737-9. — Режим доступа: http://www.iprbookshop.ru/52183.html

2. Берлин, А. Н. Высокоскоростные сети связи [Электронный ресурс] / А. Н. Берлин. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 437 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/57378.html

3. Буцык, С. В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс] : учебное пособие по дисциплине «Вычислительные системы, сети и телекоммуникации» для студентов, обучающихся по направлению 09.03.03 Прикладная информатика (уровень бакалавриата) / С. В. Буцык, А. С. Крестников, А. А. Рузаков ; под ред. С. В. Буцык. — Электрон. текстовые данные. — Челябинск : Челябинский государственный институт культуры, 2016. — 116 c. — 978-5-94839-537-1. — Режим доступа: http://www.iprbookshop.ru/56399.html

4. Гладких, Т. В. Информационные системы и сети [Электронный ресурс] : учебное пособие / Т. В. Гладких, Е. В. Воронова ; под ред. Л. А. Коробова. — Электрон. текстовые данные. — Воронеж : Воронежский государственный университет инженерных технологий, 2016. — 87 c. — 978-5-00032-189-8. — Режим доступа: http://www.iprbookshop.ru/64403.html

5. Информационные технологии [Электронный ресурс] : учебное пособие / Д. Н. Афоничев, А. Н. Беляев, С. Н. Пиляев, С. Ю. Зобов. — Электрон. текстовые данные. — Воронеж : Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2016. — 268 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/72674.html

6. Мэйволд, Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 571 c. — 5-9570-0046-9. — Режим доступа: http://www.iprbookshop.ru/73727.html

7. Нерсесянц, А. А. Моделирование инфокоммуникационных систем и сетей связи [Электронный ресурс] : учебное пособие по дисциплине «Мультисервисные сети связи» / А. А. Нерсесянц. — Электрон. текстовые данные. — Ростов-на-Дону : Северо-Кавказский филиал Московского технического университета связи и информатики, 2016. — 115 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61300.html

8. Оливер, Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер ; пер. И. В. Синицын. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 333 c. — 978-5-4488-0054-2. — Режим доступа: http://www.iprbookshop.ru/63577.html

9. Практикум по выполнению лабораторных работ по дисциплине Системы обнаружения вторжений в компьютерные сети [Электронный ресурс] / сост. Д. В. Костин. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 42 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61546.html

10. Сергеев, А. Н. Администрирование сетей на основе Windows [Электронный ресурс] : лабораторный практикум / А. Н. Сергеев, Е. В. Татьянич. — Электрон. текстовые данные. — Волгоград : Волгоградский государственный социально-педагогический университет, 2017. — 48 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62772.html

11. Чекмарев, Ю. В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс] / Ю. В. Чекмарев. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 184 c. — 978-5-4488-0071-9. — Режим доступа: http://www.iprbookshop.ru/63576.html

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	Было	Стало
28.08.2018	Внесены изменения в раздел 4 пункт 4.2 Информационное обеспечение обучения: Добавлена литература IPR books	-	Учебная литература IPR books 1. Рудаков А.В. Технология разработки программных продуктов: учебник для студ. учреждений сред. проф. образования. – 9-е изд., стер. – М.: Издательский центр «Академия, 2014 2. Рудаков А.В. Технология разработки программных продуктов: Практикум: учеб. пособие для студ. учреждений сред. проф. образования. – 9-е изд., стер. – М.: Издательский центр «Академия, 2014
29.08.2019	Внесены изменения в раздел 4 пункт 4.2 Информационное обеспечение обучения: Изменен список литературы,	**Было:** **Основная литература** 1. Мельников В.П. Информационная безопасность: учеб. пособие для сред. проф. образования. – М.: Академия. 2014 **Дополнительная литература** 2. Бабаш А.В., Баранова Е.К. Информационная безопасность: учебно-практическое пособие. – М.: Изд. Центр ЕАОИ, 2014. – 376 с. 3. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум (+CD): учебное пособие. – М.: КНОРУС, 2015. – 136 с. 4. Белов Е. Б., Лось В.П. и др. Основы информационной безопасности. М.: Горячая линия - Телеком, 2014. – 544 с. 5. Блэк У. Интернет: протоколы безопасности. Учебный курс. – СПб.: Питер, 2014. – 288 с. 6. Домарев В.В Безопасность информационных технологий. Методология создания	**Стало**: **Основная литература** 1. Богомазова Г.Н. Обеспечение информационной безопасности компьютерных сетей: учеб. для студ. учреждений сред. проф. образования: / Г.Н. Богомазова. - М.: Издательский центр «Академия», 2017 **Дополнительная литература** 2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: 2016. **Учебная литература IPR books**

	Изменена литература IPR books	систем защиты. – М.: ДиаСофт, 2014. **Учебная литература IPR books** 1. Рудаков А.В. Технология разработки программных продуктов: учебник для студ. учреждений сред. проф. образования. – 9-е изд., стер. – М.: Издательский центр «Академия, 2014 2. Рудаков А.В. Технология разработки программных продуктов: Практикум: учеб. пособие для студ. учреждений сред. проф. образования. – 9-е изд., стер. – М.: Издательский центр «Академия, 2014	1. Построение коммутируемых компьютерных сетей [Электронный ресурс] / Е.В. Смирнова [и др.]. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 428 c. http://www.iprbookshop.ru/52163.html 2. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 c. http://www.iprbookshop.ru/33857.html 3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. http://www.iprbookshop.ru/63594.html
19.06.2020	Изменена литература IPR books	Учебная литература IPR books 1. Построение коммутируемых компьютерных сетей [Электронный ресурс] / Е.В. Смирнова [и др.]. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 428 c. http://www.iprbookshop.ru/52163.html 2. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 c. http://www.iprbookshop.ru/33857.html 3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c.	Электронные ресурсы 1. Беспроводные сети Wi-Fi [Электронный ресурс] / А. В. Пролетарский, И. В. Баскаков, Р. А. Федотов [и др.]. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 284 c. — 978-5-94774-737-9. — Режим доступа: http://www.iprbookshop.ru/52183.html 2. Берлин, А. Н. Высокоскоростные сети связи [Электронный ресурс] / А. Н. Берлин. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 437 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/57378.html 3. Буцык, С. В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс] : учебное пособие по дисциплине «Вычислительные системы, сети и телекоммуникации» для студентов, обучающихся по направлению 09.03.03 Прикладная информатика (уровень бакалавриата) / С. В. Буцык, А. С. Крестников, А. А. Рузаков ; под ред. С. В. Буцык. — Электрон. текстовые данные. — Челябинск : Челябинский государственный институт культуры, 2016. — 116 c. — 978-5-94839-537-1. — Режим доступа: http://www.iprbookshop.ru/56399.html

		http://www.iprbookshop.ru/63594.html	4. Гладких, Т. В. Информационные системы и сети [Электронный ресурс] : учебное пособие / Т. В. Гладких, Е. В. Воронова ; под ред. Л. А. Коробова. — Электрон. текстовые данные. — Воронеж : Воронежский государственный университет инженерных технологий, 2016. — 87 c. — 978-5-00032-189-8. — Режим доступа: http://www.iprbookshop.ru/64403.html 5. Информационные технологии [Электронный ресурс] : учебное пособие / Д. Н. Афоничев, А. Н. Беляев, С. Н. Пиляев, С. Ю. Зобов. — Электрон. текстовые данные. — Воронеж : Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2016. — 268 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/72674.html 6. Мэйволд, Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 571 c. — 5-9570-0046-9. — Режим доступа: http://www.iprbookshop.ru/73727.html 7. Нерсесянц, А. А. Моделирование инфокоммуникационных систем и сетей связи [Электронный ресурс] : учебное пособие по дисциплине «Мультисервисные сети связи» / А. А. Нерсесянц. — Электрон. текстовые данные. — Ростов-на-Дону : Северо-Кавказский филиал Московского технического университета связи и информатики, 2016. — 115 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61300.html 8. Оливер, Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер ; пер. И. В. Синицын. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 333 c. — 978-5-4488-0054-2. — Режим доступа: http://www.iprbookshop.ru/63577.html 9. Практикум по выполнению лабораторных работ по дисциплине Системы обнаружения вторжений в компьютерные сети [Электронный

			ресурс] / сост. Д. В. Костин. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 42 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61546.html 10. Сергеев, А. Н. Администрирование сетей на основе Windows [Электронный ресурс] : лабораторный практикум / А. Н. Сергеев, Е. В. Татьянич. — Электрон. текстовые данные. — Волгоград : Волгоградский государственный социально-педагогический университет, 2017. — 48 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62772.html 11. Чекмарев, Ю. В. Вычислительные системы, сети и телекоммуникации [Электронный ресурс] / Ю. В. Чекмарев. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 184 с. — 978-5-4488-0071-9. — Режим доступа: http://www.iprbookshop.ru/63576.html