

ОДОБРЕНО

предметно-цикловой комиссией по УГС
11.00.00 Электроника, радиотехника и
системы связи

Протокол № 10 от 04 06 2021 г.

Председатель П(Ц)К



Подпись

Мирзаев З.Н

УТВЕРЖДАЮ

Зам. директора по учебной работе



Ф.Р.Ахмедова

Подпись

10 06 2021 г.



Рабочая программа учебной практики «ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» разработана на основе:

- Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.11 Сети связи и системы коммутации (базовой подготовки), входящей в состав укрупненной группы специальностей 11.00.00 Электроника, радиотехника и системы связи, утвержденного приказом Министерства Образования и науки Российской Федерации № 813 от 28 июля 2014 г., (зарегистрирован Министерством юстиции 19 августа 2014 г. рег. № 33646);

с учетом:

- Методических рекомендаций по разработке рабочих программ профессиональных модулей в пределах освоения основной профессиональной образовательной программы среднего профессионального образования (ППКРС и ППССЗ), разработанных Отделом профессионального образования Министерства образования и науки Республики Дагестан

в соответствии с рабочим учебным планом образовательной организации на 2021/2022 учебный год

Разработчики:

- Багаутдинова Зарема Магомедзапировна преподаватель дисциплин общего и профессионального цикла ГБПОУ РД «Технический колледж имени Р.Н. Ашуралиева»

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН
Государственное бюджетное профессиональное образовательное учреждение
«Технический колледж имени Р.Н Ашуралиева».

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и
информационно-коммуникационных сетей связи.
код и наименование дисциплины по ФГОС

Код и наименование специальности 11.02.11 « Сети связи и системы коммутации»

входящей в состав УГС 11.00.00 Электроника радиотехника и системы связи.
код и наименование укрупненной группы специальностей

Квалификация выпускника: Техник

Махачкала 2021 г.

СОДЕРЖАНИЕ

	стр.
1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	7
3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	9
4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	14
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	17

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.

1.1. Область применения программы

Примерная программа учебной практики (далее примерная программа) – является частью примерной основной профессиональной образовательной программы в соответствии с ФГОС по специальности (специальностям) СПО / профессии (профессиям) НПО **11.02.11 «Сети связи и системы коммутации»** в части освоения основного вида профессиональной деятельности (ВПД):

Выявления каналов утечки, установки и настройки специализированного оборудования по защите информации, проверки защищенности автоматизированных систем и информационно-коммуникационных сетей.

1. Выполнять монтаж и производить настройку сетей проводного и беспроводного абонентского доступа.
2. Осуществлять работы с сетевыми протоколами.
3. Обеспечивать работоспособность оборудования мультисервисных сетей.
4. Выполнять монтаж и первичную инсталляцию компьютерных сетей.
5. Инсталлировать и настраивать компьютерные платформы для организации услуг связи.
6. Производить администрирование сетевого оборудования.
7. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.
8. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.
9. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.
10. Выполнять монтаж оборудования телекоммуникационных систем.
11. Проводить мониторинг и диагностику телекоммуникационных.
12. Управлять данными телекоммуникационных систем.
13. Устранять аварии и повреждения оборудования телекоммуникационных систем, выбирать методы восстановления его работоспособности.
14. Выполнять монтаж и обеспечивать работу линий абонентского доступа и оконечных абонентских устройств.
15. Решать технические задачи в области эксплуатации телекоммуникационных систем.
16. Планировать и организовывать работу структурного подразделения.
17. Руководить работой структурного подразделения.
18. Анализировать процесс и результаты деятельности подразделения.
19. Проводить маркетинговые исследования рынка услуг связи для формирования бизнес-планов и бизнес-процессов.
20. Выбирать технологии для предоставления различных услуг связи в соответствии с заказами потребителей.

21. Заключать торговые сделки, коммерческие и страховые договоры при осуществлении деятельности организации связи.
22. Определять стратегию жизненного цикла услуг.
23. Выполнять монтаж, установку и настройку современного оборудования связи.
24. Проводить мониторинг информационно-коммуникационных сетей связи.
25. Управлять информационно-коммуникационными сетями связи.
26. Повышать компьютерную и технологическую грамотность персонала.

Примерная программа профессионального модуля может быть использована в программе профессиональной подготовки монтажника оборудования радио и телефонной связи, монтажника связи, электромонтера оборудования электросвязи и проводного вещания, электромонтера по ремонту линейно-кабельных сооружений телефонной связи и проводного вещания.

1.2. Цели и задачи модуля – требования к результатам освоения практики.

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной практики должен:

иметь практический опыт:

- выявления каналов утечки информации; определения необходимых средств защиты;
- проведения аттестации объекта защиты (проверки уровня защищенности); разработки политики безопасности для объекта защиты;
- установки, настройки специализированного оборудования по защите информации;
- выявления возможных атак на автоматизированные системы; установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;
- конфигурирования автоматизированных систем и информационно-коммуникационных сетей;
- проверки защищенности автоматизированных систем и информационно-коммуникационных сетей; защиты баз данных;
- организации защиты в различных операционных системах и средах; шифрования информации;

уметь:

- классифицировать угрозы информационной безопасности;¹
- проводить выборку средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;
- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;

- использовать программные продукты, выявляющие недостатки систем защиты; производить установку и настройку средств защиты; конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

- выполнять тестирование систем с целью определения уровня защищенности;

- использовать программные продукты для защиты баз данных; применять криптографические методы защиты информации;

знать:

- каналы утечки информации; назначение, классификацию и принципы работы специализированного оборудования;

- принципы построения информационно-коммуникационных сетей;

— возможные способы несанкционированного доступа; нормативно-правовые и законодательные акты в области информационной безопасности;

- правила проведения возможных проверок; этапы определения конфиденциальности документов объекта защиты;

- технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов;

- конфигурации защищаемых сетей; алгоритмы работы тестовых программ; собственные средства защиты различных операционных систем и сред;

- способы и методы шифрования информации выявления каналов утечки информации; определения необходимых средств защиты;

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – 36 часов

учебной практики – 36 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения программы учебной практики является овладение обучающимися видом профессиональной деятельности, **Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК.2.1	Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.
ПК.2.2	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению
ПК 2.3.	Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

3. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики (вариант для НПО)

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)		Практика		
			Обязательная аудиторная учебная нагрузка обучающегося		Самостоятельная работа обучающегося, часов	Учебная, часов	Производственная, часов
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов			
1	2	3	4	5	6	7	8
ПК.2.1ПК.2.2ПК.2.3.	Раздел 1. Обеспечение безопасной деятельности телекоммуникационных систем информационно-коммуникационных сетей связи.	36	36				
	Всего:	36					

* Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

3.2. Содержание обучения учебной практики

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	Коды компетенций, умений знаний, формированию которых способствует элемент программы
1	2	3	4
Раздел. 1	ПМ2. Обеспечение информационной безопасности телекоммуникационных систем и информационно- коммуникационных сетей связи.	36	
Тема 1. Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.	Содержание учебного материала	10	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8.ОК 9. ОК 10.
	1.		
	Практические занятия		
	1. Изучение Защита информации в операционной системе		
	2. Изучение стандартных настроек BIOS Setur.		
	3. Установление и настраивание антивирусной программы Doctor Web.		
4. Установление и настраивание антивирусной программы Avest.			
Тема 2. Изучение простейшего криптоанализа шифротекста.	Содержание учебного материала	10	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8.ОК 9. ОК 10.
	1.		
	Практические занятия		
	1. Исследование средств двухключевого шифрования данных.		
	2. Исследование электронной цифровой подписи информации.		
	3. Изучение способов защиты информации в системах поддержки принятия.		
4. Изучение стандарта ISO/IEC 15408 «Критерии оценки»			
Тема 3 Технические средства комплексной системы защиты информации	Содержание учебного материала	10	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8.ОК 9. ОК 10.
	1.		
	Практические занятия		
	1. Изучение Системы активной защиты (САЗ) ВОЛНА-3М «Аккорд-АМДЗ (аппаратный модуль доверенной загрузки)».		
	2 Тестовые испытания программных средств защиты.		
	3 Методы и технологии испытания аппаратного уровня комплексной защиты информации.		
	4.		
	Практические занятия		
	1.		
	1.		
Тема 4. Изучение технического регулирования в области	Содержание учебного материала	6	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4.
	1.		

защиты информации.	Практические занятия			ОК 5.ОК 6.ОК 7.ОК 8.ОК 9. ОК 10.
	1.	Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф»		
	2.	Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор»		
	3.	Аудит комплексной защиты информации предприятия		
Производственная практика <i>(для СПО – (по профилю специальности))</i>				
Виды работ				
Всего			36	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

- 1 – ознакомительный (узнавание ранее изученных объектов, свойств);
- 2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
- 3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие лабораторий информационной безопасности телекоммуникационной системы и информационно-коммуникационных сетей связи, полигона вычислительной техники.

Оборудование лабораторий и рабочих мест лабораторий:

- компьютеры (рабочие станции), сервер, локальная сеть, выход в глобальную сеть, проектор, экран, плазменная панель, комплект учебно-методической документации.

Оборудование полигона вычислительной техники:

- компьютеры (рабочие станции), сервер, локальная сеть, выход в глобальную сеть.

Реализация программы модуля предполагает обязательную учебную практику, которую рекомендуется проводить рассредоточенно.

Оборудование и технологическое оснащение рабочих мест:

- компьютеры (рабочие станции), локальная сеть, выход в глобальную сеть.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Основы информационной безопасности : учебное пособие / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина — 4-е изд. — М.: 2008. — 205 с. : ил.
2. Галатенко В. А. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с. — ISBN 5-9556-0053-1.
3. Малюк А. А., Горбатов В. С , Королев В. И. и др. Введение в информационную безопасность: Учебное пособие для вузов/ Под ред.В. С. Горбатова. - М.: Горячая линия – Телеком, 2011. – 288 с.: ил. Дополнительные источники:
4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с. — ISBN 5-94074-383-8.
5. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. — 176 с. — ISBN 978-985-463-258-2.
6. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с. — ISBN 978-5-388-00069-9.

Дополнительные источники:

1. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с. — ISBN 978-5-8041-0378-2.
2. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.
3. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. — 384 с. — ISBN 5-98453-001-5.
4. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000. — 428 с. — ISBN 5-93598-030-4.
5. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с. — ISBN 5-8459-0323-8, ISBN 1-5787-0264-X.
6. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).
7. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799—2005).
8. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. — М.: ПЕР СЭ-Пресс, 2005.
9. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.
10. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1 — 2006).
11. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).
12. Словарь терминов по безопасности и криптографии. Европейский институт стандартов по электросвязи
13. Поиск. Глоссарий.ru
14. Рекомендации по стандартизации «Техническая защита информации. Основные термины и определения» (Р 50.1.056-2005).
15. Государственный стандарт РФ «Аспекты безопасности. Правила включения в стандарты» (ГОСТ Р 51898-2002).
16. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004. — 992 с.

Интернет ресурсы:

Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний,

WWW.twirpx.com,

WWW.referent.ru,

WWW.kodeks-luks.ru/dws,

WWW.Consultant.ru/online.

4.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к учебной практике в рамках профессионального модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля

«Разработка программных модулей программного обеспечения для компьютерных систем».

Перед изучением модуля обучающиеся изучают следующие дисциплины «Компьютерное моделирование», «Теория электрических цепей», «Технология монтажа телекоммуникационных систем и информационно-коммуникационных сетей связи», «Основы программирования», «Правовое обеспечение профессиональной деятельности», «Безопасность жизнедеятельности».

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие высшего профессионального образования, соответствующего профилю модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» по специальности «Сети связи и системы коммутации».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав: высшее инженерное образование, соответствующее профилю модуля.

Мастера: обязательная стажировка в профильных организациях не реже 1-го раза в 3 года. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
<p>ПК.2.1. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.</p>	<ul style="list-style-type: none"> - Установление и настройка специализированного оборудования по защите информации; - Установление и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей связи; - Выявление возможных атак на автоматизированные системы; - Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей - Организация защиты в различных операционных системах и средах, шифрования информации. 	<ul style="list-style-type: none"> - Текущий контроль в форме:- защиты лабораторных занятий;- тестирования;- контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля. - Текущий контроль в форме:- защиты лабораторных занятий;- тестирования. - Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля.
<p>ПК.2.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению</p>	<ul style="list-style-type: none"> - Классифицировать угрозы информационной безопасности; - проводить выборку средств защиты в соответствии с выявленными угрозами; определять возможные виды атак; - осуществлять мероприятия по проведению аттестационных работ; 	<ul style="list-style-type: none"> - Текущий контроль в форме:- защиты лабораторных занятий;- тестирования; - контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля.

	<ul style="list-style-type: none"> - разрабатывать политику безопасности объекта; выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта; - использовать программные продукты, выявляющие недостатки систем защиты; - производить установку и настройку средств защиты; конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; - выполнять тестирование систем с целью определения уровня защищенности; - использовать программные продукты для защиты баз данных; применять криптографические методы защиты информации; 	<ul style="list-style-type: none"> - Текущий контроль в форме:- защиты лабораторных занятий; - - тестирования. - Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля. - Текущий контроль в форме:- защиты лабораторных занятий; - - тестирования; - - контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля. - Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля. - Текущий контроль в форме: - - защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля.
--	--	--

<p>ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.</p>	<p>- классификацию и принципы работы специализированного оборудования;</p> <p>- принципы построения информационно-коммуникационных сетей;</p> <p>- возможные способы несанкционированного доступа; нормативно-правовые и законодательные акты в области информационной безопасности;</p> <p>- правила проведения возможных проверок; этапы определения конфиденциальности документов объекта защиты;</p>	<p>Текущий контроль в форме:- защиты лабораторных занятий;</p> <p>- тестирования;</p> <p>- контрольных работ по темам МДК.</p> <p>Экзамены по разделу профессионального модуля.</p> <p>Текущий контроль в форме:</p> <p>- защиты лабораторных занятий;</p> <p>- тестирования.</p> <p>Текущий контроль в форме:</p> <p>- защиты лабораторных занятий;</p> <p>Зачеты по учебной практике и по разделу профессионального модуля.</p> <p>Текущий контроль в форме:</p> <p>- защиты лабораторных занятий;</p> <p>- тестирования;</p> <p>- контрольных работ по темам МДК.</p> <p>Экзамены по разделу профессионального модуля.</p> <p>Текущий контроль в форме:</p> <p>- защиты лабораторных занятий;</p> <p>Зачеты по учебной практике и по разделу профессионального модуля.</p> <p>Текущий контроль в форме:</p> <p>- защиты лабораторных занятий;</p>
--	--	--

	<p>- технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов;</p> <p>- конфигурации защищаемых сетей; алгоритмы работы тестовых программ; собственные средства защиты различных операционных систем и сред;</p> <p>- способы и методы шифрования информации выявления каналов утечки информации; определения необходимых средств защиты;</p>	<p>Зачеты по учебной практике и по разделу профессионального модуля.</p> <p>Текущий контроль в форме:</p> <ul style="list-style-type: none"> - защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК.
--	--	--

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
<p>ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.</p>	<p>– демонстрация интереса к будущей профессии</p>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p>
<p>ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач,</p>	<p>– выбор и применение методов и способов решения профессиональных задач в области разработки и администрирования баз данных;</p>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в</p>

оценивать их эффективность и качество.	– оценка эффективности и качества выполнения	процессе освоения образовательной программы
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	– решение стандартных и нестандартных профессиональных задач в области разработки и администрирования баз данных	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	– эффективный поиск необходимой информации; – использование различных источников, включая электронные	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	– разрабатывать, программировать и администрировать базы данных	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	– взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	– самоанализ и коррекция результатов собственной работы	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	– организация самостоятельных занятий при изучении профессионального модуля	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

<p>ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.</p>	<p>– анализ инноваций в области разработки и администрирования баз данных</p>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p>
<p>ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).</p>	<p>– решение ситуативных задач, связанных с использованием профессиональных компетенций</p>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p>

РЕЦЕНЗИЯ
на рабочую программу
учебной практики ПМ02 «Техническая эксплуатация инфокоммуникационных систем связи»

На рецензию представлена рабочая программа учебной практики ПМ02 «Техническая эксплуатация инфокоммуникационных систем связи», разработчиком которой является преподаватель ГБПОУ «Технический колледж имени Р.Н. Ашуралиева» Мирзасев Осман Нурмагомедович

Рабочая программа учебной практики ПМ02 «Техническая эксплуатация инфокоммуникационных систем связи», разработана на основе требований ФГОС СПО по специальности 11.02.15. Инфокоммуникационные сети и системы связи, в соответствии с рабочим учебным планом образовательной организации на 2021/2022 учебный год, с учетом Методических рекомендаций по разработке рабочей программы учебной дисциплины при реализации основной профессиональной образовательной программы среднего профессионального образования (ППКРС И ПСССЗ) разработанных Отделом профессионального образования Министерства образования и науки Республики Дагестан.

Учебная практика ПМ02 «Техническая эксплуатация инфокоммуникационных систем связи» является обязательной частью общепрофессиональных дисциплин ПСССЗ.

Рабочая программа практики ПМ02 «Техническая эксплуатация инфокоммуникационных систем связи», включает: титульный лист, содержание, раздел 1 «Паспорт рабочей программы учебной дисциплины», раздел 2 «Структура и примерное содержание», раздел 3 «Условия реализации рабочей программы», раздел 4 «Контроль и оценка результатов освоения дисциплины». Все разделы программы представлены и выполнены в соответствии с рекомендованной формой.

В паспорте программы указывается область применения программы, место дисциплины в структуре программы подготовки специалистов среднего звена, Цели и задачи дисциплины – требования к результатам освоения дисциплины, количество часов на освоение программы дисциплины.

В тематическом плане программы дисциплины содержится почасовое распределение видов учебной работы студентов, обеспечивается логическая последовательность и четкость в наименовании разделов и тем. Содержание теоретического материала, практических занятий и самостоятельной работы студентов соответствует целям и задачам освоения дисциплины с учётом ОК и ПК компетенций, формированию которых способствует элемент программы, уровни освоения обозначаются дидактически целесообразно.

Перечисленное оборудование лаборатории и рабочих мест лаборатории, в том числе персональные компьютеры с необходимым комплектом лицензионного программного обеспечения, технические средства обучения, печатные и электронные издания основной и дополнительной литературы, обеспечивают материально-технические и информационные условия реализации программы дисциплины.

В качестве рекомендаций составителю рабочей программы учебной дисциплины предлагается ежегодно корректировать содержание теоретических и практических занятий с учётом новых тенденций в области информационных технологий, обновлять перечень информационных источников.

Представленная на рецензию рабочая программа учебной дисциплины рабочая программа учебной практики ПМ02 «Техническая эксплуатация инфокоммуникационных систем связи», рекомендуется к практическому применению в образовательном процессе в профессиональных образовательных организациях, реализующих программу подготовки специалистов среднего звена по специальности 11.02.15. Инфокоммуникационные сети и системы связи.

Рецензент



Абдулаев М.А. Генеральный директор ООО «Каспий-Телеком».