МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н.АШУРАЛИЕВА»

Рабочая программа производственной практики профессионального модуля ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем иинформационно-коммуникационных сетей связи

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 – 2022 г.

СОГЛАСОВАНО
Генеральный директор
ООО «ЭЛЛКО»

_____ Будунов К.Б._
Подпись ФИО

УТВЕРЖДАЮ
зам. директора по учебной работе

_____ Ф.Р. Ахмедова
Подпись ФИО

«15» 06 2022 г.

ОДОБРЕНО
предметной (цикловой) комиссией по УГС 11.00.00. Электроника радиотехника и системы связи

Протокол № 10 от 15 июня 2022 г.

Председатель П(Ц)К

_____ З.Н. Мирзаев_
Подпись ФИО

Рабочая программа производственной практики профессионального модуля: 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., (Зарегистрировано в Минюсте России 19.08.2014 N 33646);

с учетом:

Методических рекомендаций по разработке рабочих программ учебных дисциплин при реализации 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 2022/2023 учебный год

Разработчик:
Магомедов Руслан Омарасхабович, преподаватель дисциплин профессионального цикла ГБПОУ РД «Технический колледж им. Р.Н. Ашуралиева».

Рецензенты / эксперты:
Будунов Каримула Будунович, генеральный директор ООО «ЭЛЛКО».

СОДЕРЖАНИЕ

1.ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1.Область применения примерной программы

Рабочая программа производственной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС поспециальности СПО **11.02.11** Сети связи и системы коммутаций.

Рабочая программа производственной практики может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке по специальностям: Сети связи и системы коммутаций.

1.2.Место производственной практики в структуре основной профессиональной образовательной программы

Цели и задачи производственной практики – требования к результатам освоения учебной дисциплины: с целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля 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 защитеинформации;

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; конфигурироватьавтоматизированные 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; применятькриптографические методы защиты информации;

знать:

каналы утечки информации; назначение, классификацию и принципы работыспециализированного оборудования;

принципы построения информационно-коммуникационных сетей;

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

правила проведения возможных проверок;

этапы определенияконфиденциальности документов объекта защиты;

технологии применения программных продуктов; возможные способы, местаустановки 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 утечкиинформации; определения необходимых средств защиты;

1.3. Организация практики

Для проведения производственной практики (по профилю специальности) в колледже разработана следующая документация:

– положение о практике;

– рабочая программа производственной практики (по профилю специальности);

– план-график консультаций и контроля за выполнением студентами программыпроизводственной практики (при проведении практики на предприятии);

– договоры с предприятиями по проведению практики;

– приказ о распределении студентов по базам практики.

В основные обязанности руководителя практики от колледжа входят:

– проведение практики в соответствии с содержанием тематического плана исодержания практики;

– установление связи с руководителями практики от организаций;

– разработка и согласование с организациями программы, содержания ипланируемых результатов практики;

– осуществление руководства практикой;

– контролирование реализации программы и условий проведения практики организациями, в том числе требований охраны труда, безопасности жиз-

недеятельности и пожарной безопасности в соответствии с правилами и нормами, в том числе отраслевыми;

– формирование группы в случае применения групповых форм проведения практики;

– совместно с организациями, участвующими в организации и проведении практики, организация процедуры оценки общих и профессиональных компетенций студента, освоенных им в ходе прохождения практики;

– разработка и согласование с организациями формы отчетности и оценочного материала прохождения практики.

Студенты при прохождении производственной практики обязаны:

– полностью выполнять задания, предусмотренные программойпроизводственной практики;

– соблюдать действующие в организациях правила внутреннего трудовогораспорядка;

– изучать и строго соблюдать нормы охраны труда и правила пожарной безопасности.

1.4. Количество часов на освоение программы производственной практики

Рабочая программа рассчитана на прохождение студентами практики в объеме 36 часа.

Распределение разделов и тем по часам приведено в примерном тематическом плане.

Базой практики являются предприятия, учреждения и организации различныхорганизационно-правовых форм и форм собственности.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

2.1. Объем производственной практики и виды работ

Вид учебных занятий, обеспечивающих практико-ориентированную подготовку	**Объем часов**
Всего занятий	**36**
в том числе:	
Инструктаж по ТБ. Изучение структуры предприятия (организации) и аппарата управления	5
- Выявление каналов утечки информации; определениянеобходимых средств защиты; - Проведение аттестации объекта защиты (проверки уровня защищенности); разработки политики безопасности для объекта защиты; - Установка, настройка специализированного оборудования позащите информации; - Выявление возможных атак на автоматизированные системы;установки и настройки программных средств защиты автоматизированных систем и информационно- коммуникационных сетей; - Конфигурирование автоматизированных систем и информационно-коммуникационных сетей;	25
Составление отчета о выполненной работе на практике.	4
Итоговая аттестация	2

2.2.Тематический план и содержание производственной практики

ПМ.02 Обеспечение информационной безопасностителекоммуникационных систем и информационно-коммуникационных сетей связи

Наименование разделов, тем, выполнение обязанностей на рабочих местах ворганизации	**Содержание учебного материала, лабораторные и практические работы,экскурсии, состав выполнения работ**	**Объем часов**	**Уровеньосвоения**
1	2	3	4
Раздел 1 **Предприятие – база прохождения практики**	**Содержание**	**10**	
Тема 1.1 Общие сведения о предприятии,		5	
	Требования охраны труда и пожарной безопасности.		1
	Изучение отраслевой принадлежности и организационнойструктуры предприятия.		
Тема 1.2 Выявление каналов утечки информации; определения необходимых средствзащиты	**Содержание**	5	
	Классификация угроз информационной безопасности; проведениевыборки средств защиты в соответствии с выявленными угрозами		2
Раздел 2		**10**	
Тема 2.1. Проведение аттестацииобъекта защиты (проверки уровня защищенности); разработки политикибезопасности для объекта защиты	**Содержание**	5	
	Определение возможных видов атак; осуществление мероприятиий по проведению аттестационных работ;		1

Тема 2.2. Установка, настройка специализированного оборудования по защитеинформации	**Содержание**	5	
	Разработка политики безопасности объекта;		2
	Выполнение расчетов и установка специализированного оборудованиядля максимальной защищенности объекта		3
Раздел 3		**16**	
Тема 3.1. - Выявление возможных атак на автоматизированные системы; установки и настройки программныхсредств защиты автоматизированных систем и сетей	**Содержание**	5	
	Использование программных продуктов, выявляющих недостатки системзащиты; производение установки и настройки средств защиты; конфигурирование автоматизированных систем и информационно- коммуникационных сетей в соответствии с политикой информационной безопасности;		3
Тема 3.2. - Конфигурированиеавтоматизированныхсистем иинформационно- коммуникационныхсетей	**Содержание**	5	
	Выполнение тестирования систем с целью определения уровнязащищенности;		2
Тема 3.3.	**Содержание**	4	
Оформление отчета	Определение состава и содержания отчета Оформление отчета. Сдача отчета в соответствии с содержанием тематического плана практики		3
Итоговая аттестация		**2**	

Для характеристики уровня освоения учебного материала используютсяследующие обозначения:

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

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Требования к минимальному материально-техническому обеспечению

Оборудование лабораторий и рабочих мест лабораторий:

- компьютеры (рабочие станции), сервер, локальная сеть, выход в глобальнуюсеть, проектор, экран, плазменная панель, комплект учебно-методическойдокументации.

Оборудование полигона вычислительной техники:

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

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.

Реализация профессионального модуля предполагает наличие объекта прохождения производственной практики (по профилю специальности).

Реализация профессионального модуля предполагает обязательную производственную практику, которую рекомендуется проводить концентрированно.

3.2. 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. — ISBN5-93598-030-4.

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 иопределения» (ГОСТ Р 50922-2006).

7. Национальный стандарт РФ «Информационная технология. Практические правилауправления 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 институтстандартов по электросвязи

13. Рекомендации по стандартизации «Техническая защита информации. Основныетермины и определения» (Р 50.1.056-2005).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Контроль и оценка результатов освоения производственной практики осуществляется преподавателем в процессе проведения практических занятий работ, тестирования, а также выполнения обучающимися индивидуальных практических заданий.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК.2.1. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.	- 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.	- Текущий контроль в форме:- защиты лабораторных занятий;- тестирования;- контрольных работ по темам МДК.
ПК.2.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению	- Классифицировать угрозы информационной безопасности; - проводить выборку средств защиты в соответствии с выявленными угрозами; - 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	- Текущий контроль в форме - - тестирования. .

	с политикой информационной безопасности; - выполнять тестирование систем с целью определения уровня защищенности; - использовать программные продукты для защиты баз данных; применять криптографические методы защиты информации;	
ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.	- 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;	- Текущий контроль в форме: - защиты лабораторных занятий; - тестирования. Текущий контроль в форме: - 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
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	– демонстрация интереса к будущей профессии	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	– выбор и применение методов и способов решения профессиональных задач в области разработки и администрирования баз данных; – оценка эффективности и качества выполнения	Интерпретация результатов наблюдений за деятельностью обучающегося в 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	– организация самостоятельных занятий при изучении профессионального модуля	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе

развития, заниматься самообразованием, осознанно планировать повышение квалификации.		освоения образовательной программы
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	– анализ инноваций в области разработки и администрирования баз данных	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

Разработчики:

ГБПОУ « Технический колледж им.Р.Н. Ашуралиева»	Преподаватель дисциплин проф. цикла	Магомедов Р.О.
(место работы)	(занимаемая должность)	(инициалы, фамилия)

Рецензенты/эксперты:

ООО «ЭЛЛКО».	Генеральный директор	К.Б. Будунов
(место работы)	(занимаемая должность)	(инициалы, фамилия)