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

Рабочая программа профессионального модуля ПМ.02. Обеспечение информационной безопасности телекоммуникационных систем и информационно-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.

ОДОБРЕНО

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

Протокол № 10 от 15 июня 2022 г.

Председатель П(Ц)К

___ _З.Н. Мирзаев_

Подпись

Рабочая программа 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

Разработчики:

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

Рецензенты / эксперты:

Будунов Каримула Будунович, генеральный директор ООО «ЭЛЛКО».

РЕЦЕНЗИЯ
на рабочую программу
учебной дисциплины « ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.»

На рецензию представлена рабочая программа профессионального модуля «ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.», разработчиком которой является преподаватель Багаутдинова Зарема Магомедзапировна преподаватель дисциплин общего и профессионального цикла ГБПОУ РД «Технический колледж имени Р.Н Ашуралиева» и Джамалутдинова М.Д преподаватель дисциплин общего и профессионального цикла ГБПОУ РД «Технический колледж имени Р.Н Ашуралиева»

Рабочая программа профессионального модуля «ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.» разработана на основе требований ФГОС СПО по специальности 11.02.11 Сети связи и системы коммутации, в соответствии с рабочим учебным планом образовательной организации на 2022/2023 учебный год, с учетом Методических рекомендаций по разработке рабочей программы профессионального модуля при реализации основной профессиональной образовательной программы среднего профессионального образования (ППКРС И ППССЗ) разработанных Отделом профессионального образования Министерства образования и науки Республики Дагестан.

Профессиональный модуль ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи. является обязательной частью модульного цикла ППССЗ.

Рабочая программы профессионального модуля включает: титульный лист, содержание, раздел 1 «Паспорт рабочей программы учебной дисциплины», раздел 2 «Результаты освоения профессионального модуля», раздел 3 «Структура и примерное содержание профессионального модуля», раздел 4 «Условия реализации профессионального модуля», раздел 5 «Контроль и оценка результатов освоения профессионального модуля», Все разделы программы представлены и выполнены в соответствии с рекомендованной формой.

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

В тематическом плане программы профессионального модуля. 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 профессионального модуля, 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 профессионального модуля.

В качестве рекомендаций составителю рабочей программы профессионального модуля 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 профессиональный модуль ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи. рекомендуется к практическому применению в образовательном процессе в профессиональных образовательных организациях, реализующих программу подготовки специалистов среднего звена по специальности 11.02.11 Сети связи и системы коммутации.

Рецензент _____Генеральный директор ООО «ЭЛЛКО» Будунов К.Б

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Примерная программа профессионального модуля (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 модуля

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 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 – 432 часов, в том числе:

максимальной учебной нагрузки обучающегося – **360** часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 240 часа;

самостоятельной работы обучающегося – 120 часов;

учебной практики – 36 часа.

Производственная практика -36 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля 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. СТРУРКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля *(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***
ПК1 ПК 2 ПК3	**Раздел 1.** Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**192**	**128**	48	**64**		
ПК1 ПК 2 ПК3	**Раздел 2** Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**168**	**112**	48	**56**		
	Учебная практика					**36**	
	Производственная практика, часов						36
	Всего:	**432**	**240**	96	**120**	**36**	**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 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	Коды компетенций, умений и знаний, формированию которых способствует элемент программы
1	2		3	4
Раздел. 1	**ПМ2. Обеспечение информационной безопасности телекоммуникационных систем и информационно- коммуникационных сетей связи.**		432	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.
	МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.		**128**	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.
Тема 1.1. Основные понятия и анализ угроз информационной безопасности сетей. Стандарты информационной безопасности.	Содержание учебного материала		22	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.	Основные понятия защиты информации и информационной безопасности.		
	2	Анализ угроз информационной безопасности.		
	3	Введение в сетевой информационный обмен. Использование сети Интернет		
	3.	Проблемы безопасности IP-сетей Угрозы и уязвимости беспроводных сетей		
	4.	Международные стандарты информационной безопасности		
	Лабораторные работы		4	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.	Модель ISO/OSI и стек протоколов TCP/IP		
	3.	Стандарты информационной безопасности в Интернете		
	Практические занятия.			
	1	Защита от атак по локальным и глобальным сетям	6	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.
	2	Изучение способов защиты информации		
Тема 1.2. Принципы криптографической защиты информации	Содержание учебного материала		26	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.	Основные понятия криптографической защиты информации		
	2.	Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования		
	3.	Комбинированная криптосистема шифрования		
	4.	Электронная цифровая подпись и функция хэширования Функция хэширования Управление крипто ключами		

	5	Классификация криптографических алгоритмов.		
	Лабораторные работы		14	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.	Алгоритм шифрования RSA		
	2.	Алгоритмы цифровой подписи		
	3.	Изучение простейшего криптоанализашифротекста.		
	Практические занятия			
	1.	Исследование электронной цифровой подписи информации с использованием PGP.	8	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.
	2	Изучение способов защиты информации в системах поддержки принятия решений.		

Тема 1.3. Технология аутентификации обеспечение безопасности операционных систем. Технологии межсетевых экранов.	**Содержание учебного материала**		46	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	Основные понятия аутентификации и идентификации.		
		Аутентификация, авторизация и администрирование действий пользователей		
	2	Методы аутентификации, использующие пароли и PIN-коды		
	3	Строгая аутентификация, основанная на симметричных и асимметричных алгоритмах Проблемы обеспечения безопасности ОС Угрозы безопасности ОС Понятие защищенной ОС Архитектура подсистемы защиты ОС.		
	4.	Функции межсетевых экранов Фильтрация трафика. Особенности функционирования МЭ на различных уровнях модели OSI		
	5.	Прикладной шлюз. Варианты исполнения МЭ. Формирование политики межсетевого взаимодействия		
	6.	Основные понятия и функции сети VPN. Персональные и распределенные сетевые экраны.		
	7	Средства обеспечения безопасности VPN. VPN-решения для построения защищенных сетей		
	Лабораторные работы		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.	Биометрическая аутентификация пользователя		
	2.	Аутентификация на основе PIN-кода		
	3.	Аутентификация на основе многоразовых паролей и одноразовых паролей		
	4.	Схемы сетевой защиты на базе МЭ.		
	5.	Схемы сетевой защиты на базе МЭ		
	Практические занятия		6	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4.
	1.	Классификация сетей VPN		

	2	Основные варианты архитектуры VPN		ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
Тема 1.4. Технологии обнаружения атак. Управление сетевой безопасностью.	**Содержание учебного материала**		34	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.	Анализ защищенности и обнаружение атак Средства анализа защищенности сетевых протоколов, сервисов и ОС.		
	2	Методы анализа сетевой информации. Классификация систем обнаружения атак IDS Компоненты и архитектура IDS. Методы реагирования		
	3	Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов.		
	4	Основные каналы распространения вирусов и других вредоносных программ		
	5	Антивирусные программы и комплексы. Построение системы антивирусной зашиты корпоративной сети.		
	6	Задачи управления системой сетевой безопасности.		
	7	Концепция глобального управления безопасностью.		
	8	Функционирование системы управления средствами безопасности.		
	Лабораторные работы		4	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.	Установление и настраивание антивирусной программы DoctorWeb.		
	2.	Установление и настраивание антивирусной программы Avast.		
	Практические занятия		4	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.	Архитектура управления средствами сетевой безопасности.		
	2	Аудит и мониторинг безопасности. Глобальная и локальная политики безопасности		
		Всего 128 в том числе 24 лаб 24 прак		
Раздел 2		**МДК02.02. Технология применения комплексной системы защиты информации в телекоммуникационных системах и сетях связи.**	**112**	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.
Тема 2.1. Построение и организация комплексной системы защиты информации	**Содержание учебного материала**		20	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.	Виды и свойства защищаемой информации. Факторы, воздействующие на защищаемую информацию. Сущность и задачи комплексной системы защиты информации		
	2.	Принципы организации КСЗИ. Роль системного подхода в создании КСЗИ		

	3.	Концепция информационной безопасности. Определение и нормативное закрепление состава защищаемой информации. Определение объектов защиты.		
	Лабораторные работы		6	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.	Требования КСЗИ Обобщенная модель защищенной системы. Этапы разработки и жизненный цикл КСЗИ.		
	Практические занятия			
	1.			
Тема 2.2 Законодательный уровень информационной безопасности.	**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.	Основные непреднамеренные и преднамеренные искусственные угрозы		
	2	Описание модели гипотетического нарушителя. Определение потенциальных каналов, методов и возможностей НСД к информации.		
	Лабораторные работы		4	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.	Классификация угроз безопасности. Изучение путей реализации угроз безопасности		
	2.	Источники, виды и способы дестабилизирующего воздействия на информацию.		
	Практические занятия			
	1.			
Тема 2.3. Защита информации в распределенных КС.	**Содержание учебного материала**		6	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.	Физические меры. Технические (программно-аппаратные) меры		
	Лабораторные работы		4	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.	Нормативно-правовые меры		
	2.	Морально-этические меры Административные меры		
	Практические занятия			
	1.			
Тема 2.4. Определение компонентов КСЗИ	**Содержание учебного материала**		24	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	Подсистема управления доступом (идентификации и аутентификации пользователей). Подсистема регистрации и учета. Подсистема обеспечения целостности. Криптографическая подсистема. Подсистема антивирусной защиты.		
	2	Подсистема резервного копирования и архивирования. Подсистема обнаружения атак. Подсистема обеспечения отказоустойчивости Подсистема централизованного управления ИБ.		
	Лабораторные работы		8	ПК.2.1ПК.2.2ПК2.3.
	1.	Требования к подсистемам ЗИ.		

	2.	Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации. Планирование восстановительных работ.		ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	3.	Подсистема межсетевого экранирования		
	4.	Сетевое сканирование		
	Практические занятия			
	1.			
Тема 2.5. Определение условий функционирования КСЗИ	**Содержание учебного материала**		28	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.	Определение условий функционирования КСЗИ. Технологическое и организационное построение КСЗИ. Кадровое обеспечение функционирования КСЗИ		
	2.	Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ. Нормативно-методическое обеспечение функционирования КСЗИ		
	3.	Назначение, структура и содержание управления КСЗИ Принципы и методы планирования функционирования КСЗИ Сущность и содержание контроля функционирования КСЗИ		
	4.	Управление КСЗИ в условиях чрезвычайных ситуаций. Состав методов и моделей оценки эффективности КСЗИ		
	Лабораторные работы		2	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.	Разработка модели КСЗИ		
	Практические занятия		6	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.	Анализ трафика и сбор критичной информации программами пассивного анализа		
	2	Обнаружение уязвимостей по сигнатурам		
	3	Оценка уязвимости коммутируемого доступа		
Тема 2. 6 Технические средства комплексной системы защиты информации	**Содержание учебного материала**			
	1	Причины, виды, каналы утечки и искажения информации.	24	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.
	2	Программно-аппаратные средства обеспечения информационной безопасности.		
	3	Анализ сетевой топологии и установленных сервисов.		
	Лабораторные работы			
	1.			
	Практические занятия		18	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	Методы защиты информации.		
	2	Изучение Системы активной защиты (САЗ) ВОЛНА-3М		
	3	«Аккорд-АМДЗ (аппаратный модуль доверенной загрузки)». Тестовые испытания программных средств защиты.		

		Методы и технологии испытания аппаратного уровня комплексной защиты информации. Анализ сетевой топологии и установленных сервисов. Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф» Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор» Аудит комплексной защиты информации предприятия		
		Всего 112 в том числе 24 ч лаб 24 практ		
Самостоятельная работа при изучении раздела ПМ . Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите			120	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.
Примерная тематика домашних заданий Основные программно-технические меры, управление Идентификация и аутентификация Стандарты и спецификации в области информационной безопасности**.** Законодательный уровень информационной безопасности. Административный уровень информационной безопасности.				
Учебная практика Изучение Защита информации в операционной системе Изучение стандартных настроек BIOS Setur Установление и настраивание антивирусной программы Doctor Web Установление и настраивание антивирусной программы Avest Изучение простейшего криптоанализа шифротекста. Исследование средств двухключевого шифрования данных Исследование электронной цифровой подписи информации. Изучение способов защиты информации в системах поддержки принятия. Изучение стандарта ISO/IEC 15408 «Критерии оценки» Технические средства комплексной системы защиты информации Изучение Системы активной защиты (САЗ) ВОЛНА-3М «Аккорд-АМДЗ (аппаратный модуль доверенной загрузки)». Тестовые испытания программных средств защиты. Методы и технологии испытания аппаратного уровня комплексной защиты информации. Изучение технического регулирования в области защиты информации Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф» Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор» Аудит комплексной защиты информации предприятия			36	

Производственная практика *(для СПО –* **(по профилю специальности)** **Виды работ**	Общие сведения о предприятии. Требования охраны труда и пожарной безопасности. Изучение отраслевой принадлежности и организационной структуры предприятия Выявление каналов утечки информации; определения необходимых средств защиты. Классификация угроз информационной безопасности; проведение выборки средств защиты в соответствии с выявленными угрозами Проведение аттестации объекта защиты (проверки уровня защищенности); разработки политики безопасности для объекта защиты Определение возможных видов атак; осуществление мероприятиий по проведению аттестационных работ; Установка, настройка специализированного оборудования по защите информации. Разработка политики безопасности объекта; Выполнение расчетов и установка специализированного оборудования для максимальной защищенности объекта Выявление возможных атак на автоматизированные системы; установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей Использование программных продуктов, выявляющих недостатки систем защиты; производение установки и настройки средств защиты; конфигурирование автоматизированных систем и информационно-коммуникационных сетей в соответствии с политикой информационной безопасности; Конфигурирование автоматизированных систем и информационно-коммуникационных сетей Выполнение тестирования систем с целью определения уровня защищенности; Оформление отчета Определение состава и содержания отчета Оформление отчета. Сдача отчета в соответствии с содержанием тематического плана практики	36	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.
	Всего	360	

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 ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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 ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

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. - 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.

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; 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;	- 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. - 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.

	- использовать программные продукты для защиты баз данных; применять криптографические методы защиты информации;	- Текущий контроль в форме: - - защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля.
ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.	- классификацию и принципы работы специализированного оборудования;	Текущий контроль в форме:- защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК. Экзамены по разделу профессионального модуля.
	- принципы построения информационно-коммуникационных сетей;	Текущий контроль в форме: - защиты лабораторных занятий; - тестирования.
	- возможные способы несанкционированного доступа; нормативно-правовые и законодательные акты в области информационной безопасности;	Текущий контроль в форме: - защиты лабораторных занятий; Зачеты по учебной практике и по разделу профессионального модуля.
	- правила проведения возможных проверок; этапы определения конфиденциальности документов объекта защиты;	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.
	- технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов;	Текущий контроль в форме: - защиты лабораторных занятий; Зачеты по учебной практике и по разделу профессионального модуля.
	- конфигурации защищаемых сетей; алгоритмы работы тестовых программ; собственные средства защиты различных операционных систем и сред;	Текущий контроль в форме: - защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК.
	- способы и методы шифрования информации выявления каналов утечки информации; определения необходимых средств защиты;	

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 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
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
ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).	– решение ситуативных задач, связанных с использованием профессиональных компетенций	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

Разработчики:

ГБПОУ РД Технический колледж имени Р.Н Ашуралиева	*Преподаватель*	*Багаутдинова З.М*
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*
ГБПОУ РД Технический колледж имени Р.Н Ашуралиева	*Преподаватель*	*Джамалутдинова М.Д*
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*

Эксперты:

_____	_____	_____
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*
_____	_____	_____
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*