Приложение 3.35
к образовательной программе
по специальности 11.02.10
Радиосвязь, радиовещание
и телевидение

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ ВЕЩАНИЯ

Рабочая программа разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.10 Радиосвязь, радиовещание и телевидение, утверждённого приказом Министерства образования и науки РФ от 28.07.2014 г. № 812 (зарегистрировано в Министерстве юстиции РФ 25.08.2014 г, № 33770)

Рабочая программа рассмотрена
на заседании ЦК радиосвязи и
телекоммуникационных систем
протокол № 11 от «15» июня 2022 г.
Председатель ЦК
_____ Т.М. Белкина

УТВЕРЖДАЮ
Зам. директора по УМР
_____/Т.Б. Балобанова
«__» _____2022 г.

Рабочую программу разработали:
преподаватель высшей квалификационной категории, инженер, преподаватель
_____ И.С. Михно

преподаватель высшей квалификационной категории, радиофизик, преподаватель СПО и ДПО
_____ Г.А. Удалова

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ ВЕЩАНИЯ

1.1. Цель и планируемые результаты освоения профессионального модуля:
Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД): Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания, в том числе профессиональными (ПК) и общими (ОК) компетенциями.

1.2 Перечень общих компетенций:

Код	Наименование общих компетенций
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

1.3 Перечень профессиональных компетенций:

Код	Наименование профессиональных компетенций
ПК3.1	Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.
ПК3.2	Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.
ПК3.3	Обеспечивать безопасное администрирование сетей вещания.
ДК 3	*Способность осуществлять проверку комплектности, работоспособности технических и программных средств, параметров абонентского и терминального телекоммуникационного оборудования*

1.4 В результате освоения профессионального модуля обучающийся должен обладать:

Код ПК, ДК, ОК	Практический опыт	Уметь	Знать
ПК 3.1, ПК 3.2,	– выявления каналов утечки	– классифицировать угрозы	– каналы утечки информации;

ПК 3.3, ДК 3 ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 7, ОК 8, ОК 9	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; – *подготовки*	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; – использовать	– назначение, классификацию и принципы работы специализированного оборудования; – принципы построения информационно-коммуникационных сетей; – возможные способы несанкционированного доступа; – законодательные и нормативные правовые акты в области информационной безопасности; – правила проведения возможных проверок; – этапы определения конфиденциальности документов объекта защиты; – структуру систем условного доступа и принцип их работы; – 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; – *правила проведения диагностических работ на абонентском и терминальном телекоммуникационном оборудовании;* – *алгоритмы работы диагностических программ,*

	рабочего места к проверке исправности абонентского и терминального телекоммуникационного оборудования; *– подготовки приборов для проверки работоспособности абонентского и терминального телекоммуникационного оборудования;* *– подготовки тестовых программ и вспомогательного оборудования для проверки работоспособности абонентского и терминального телекоммуникационного оборудования и проведения необходимых действий в соответствии с методиками поиска неисправности в нем;* *– подготовки абонентского и терминального телекоммуникационного оборудования к проведению диагностических работ;* *– диагностики абонентского и терминального телекоммуникационного оборудования;* *– измерения параметров абонентского и терминального телекоммуникационного оборудования;* *– поиска неисправностей абонентского и терминального*	программные продукты для защиты баз данных; – применять криптографические методы защиты информации; *– поддерживать состояние рабочего места в соответствии с требованиями охраны труда, пожарной, промышленной и экологической безопасности, правилами организации рабочего места;* *– готовить абонентское и терминальное телекоммуникационное оборудование к проведению диагностики;* *– использовать контрольно-измерительные приборы, инструменты и вспомогательное оборудование для проведения диагностики на абонентском и терминальном телекоммуникационном оборудовании;* *– применять техническую документацию при проведении диагностики на абонентском и терминальном телекоммуникационном оборудовании;* *– определять, обнаруживать и устранять*	*вспомогательного оборудования и процедур диагностики абонентского и терминального телекоммуникационного оборудования;* *– использование диагностических программ и вспомогательного оборудования для диагностики абонентского и терминального телекоммуникационного оборудования;* *– основы автоматизированной обработки информации;* *– эксплуатационная документация в части проведения диагностических работ на абонентском и терминальном телекоммуникационном оборудовании;* *– правила перевода абонентского и терминального телекоммуникационного оборудования из рабочего режима в режим диагностических работ;* *– правила подготовки абонентского и терминального телекоммуникационного оборудования к проведению диагностических работ;* *– конструкция, назначение и методика применения измерительного и вспомогательного оборудования;* *– правила хранения, выдачи и сдачи измерительного и*

	телекоммуникационного оборудования; *– устранения неисправностей, возникших при эксплуатации абонентского и терминального телекоммуникационного оборудования;* *– оформления технической документации о диагностированных неисправностях абонентского и терминального телекоммуникационного оборудования;* *– оформления сообщений о диагностированных неисправностях абонентского и терминального телекоммуникационного оборудования в службы ремонта и (или) технической поддержки;* *– уборки рабочего места после проведения диагностики абонентского и терминального телекоммуникационного оборудования;* *– сдачи абонентского и терминального телекоммуникационного оборудования в ремонт после проведения диагностики;* *– ввода абонентского и терминального телекоммуникационного оборудования в*	*неисправности, возникающие при эксплуатации абонентского и терминального телекоммуникационного оборудования;* *– производить необходимую при диагностических работах разборку абонентского и терминального телекоммуникационного оборудования;* *– производить сборку абонентского и терминального телекоммуникационного оборудования после проведения диагностических работ;* *– производить подключение абонентского и терминального телекоммуникационного оборудования после проведения диагностических работ;* *– производить подключение абонентского и терминального телекоммуникационного оборудования после проведения диагностических и ремонтных работ;* *– выполнять требования охраны труда, пожарной, промышленной и экологической безопасности при проведении диагностических работ абонентского и терминального*	*вспомогательного оборудования для диагностики абонентского и терминального телекоммуникационного оборудования;* *– правила оформления документов при диагностике абонентского и терминального телекоммуникационного оборудования;* *– устройство абонентского и терминального телекоммуникационного оборудования;* *– принципы работы абонентского и терминального телекоммуникационного оборудования;* *– методы анализа результатов диагностики абонентского и терминального телекоммуникационного оборудования, и установки их параметров в соответствие с действующими нормами;* *– устройство и принцип действия приборов и вспомогательного оборудования для измерений, проводимых при диагностических работах на абонентском и терминальном телекоммуникационном оборудовании;* *– сроки поверок приборов для измерений, используемых при проведении диагностических работ на абонентском и терминальном*

	работу после проведения ремонта; *– документирования и оформления результатов работы после проведения диагностики абонентского и терминального телекоммуникационного оборудования.*	*телекоммуникационного оборудования.*	*телекоммуникационном оборудовании;* *– условия хранения приборов для измерений, используемых при проведении диагностических работ на абонентском и терминальном телекоммуникационном оборудовании;* *– правила проведения измерений при диагностических работах на абонентском и терминальном телекоммуникационном оборудовании;* *– правила хранения технической документации на абонентское и терминальное телекоммуникационное оборудование, и ее оформления при проведении диагностических работ;* *– правила перевода абонентского и терминального телекоммуникационного оборудования из режима диагностических работ в рабочий режим;* *– наименование, маркировка, правила использования инструментов при проведении диагностических работ на абонентском и терминальном телекоммуникационном оборудовании;* *– наименование, маркировка, правила использования контрольно-измерительных приборов при проведении*

			диагностических работ на абонентском и терминальном телекоммуникационном оборудовании; *– принципы электропитания абонентского и терминального телекоммуникационного оборудования;* *– требования охраны труда, пожарной, промышленной и экологической безопасности при проведении диагностических работ на абонентском и терминальном телекоммуникационном оборудовании.*

1.5 Количество часов, отводимое на освоение профессионального модуля:

Всего часов:	Объем в часах
на освоение МДК	166
на практики	36
производственную	36
самостоятельную работу	66

2.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля:

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Объем ПМ, час.	Объем профессионального модуля, час.				
			Обучение по МДК, в час			Практики	СРС
			Всего, часов	Лабораторных и практических занятий, часов	Курсовых работ (проектов), часов	Производственная	
1	2	3	4	5	6	7	8
ПК 3.1, ПК3.2, ПК 3.3, ДК 3 ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7, ОК8, ОК9	**МДК.03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания**	**83**	**50**	24			**33**
ПК 3.1,ПК 3.2, ПК3.3 ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7, ОК8, ОК9	**МДК 03.02 Технология использования систем условного доступа в сетях вещания**	**83**	**50**	24			**33**
ПК 3.1, ПК3.2, ПК3.3, ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7, ОК8, ОК9, ДК 3	**ПП.03.01 Производственная практика**	**36**				36	
	Всего:	**202**	**100**	**48**		**36**	**66**

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся	Объем в часах
МДК.03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания		**83**
Тема 1.1 Понятия информационной безопасности, составляющие информационной безопасности	**Содержание учебного материала**	4
	1. Содержание и задачи дисциплины. Роль дисциплины в сфере профессиональной деятельности, связь с другими дисциплинами.	
	2. Актуальность проблемы обеспечения информационной безопасности современных многоканальных телекоммуникационных систем и сетей электросвязи.	
	3. Основные понятия и определения информационной безопасности.	
	4. Основные составляющие информационной безопасности: доступность, целостность, конфиденциальность.	
	5. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный, программно-технический.	
	Практическое занятие №1. Проведение анализа информации на предмет целостности	2
	Самостоятельная работа №1. Написать реферат по заданной теме	4
Тема 1.2 Угрозы информационной безопасности и их классификация	**Содержание учебного материала**	2
	1. Виды угроз информационной безопасности, их источники и классификация.	
	2. Классификация угроз информационной безопасности.	
	3. Критерии формирования целей защиты для каждого варианта классификации.	
	Практическое занятие №2. Анализ источников, каналов распространения и каналов утечки информации	2
	Самостоятельная работа №2. Написать реферат по заданной теме	4
Тема 1.3 Нормативно-правовые основы обеспечения информационной безопасности	**Содержание учебного материала**	2
	1. Статьи Конституции Российской Федерации в области информационной безопасности. Статьи Гражданского и Уголовного кодексов Российской Федерации в области информационной безопасности.	
	2. Законы и нормативные акты Российской Федерации в области информационной безопасности.	

	3.	Оценочные стандарты и технические спецификации в области информационной безопасности.	
	4.	Критерии доверенных систем. Уровень гарантированности системы.	
	Практическое занятие№3. Требования к безопасности информационных систем		2
	Практическое занятие№4. Определение классов защищенности средств вычислительной техники от несанкционированного доступа		2
	Самостоятельная работа №3. Составить презентацию		2
Тема 1.4 Принципы построения систем радиосвязи и сетей вещания. Основные угрозы информации в системах радиосвязи и сетях вещания	**Содержание учебного материала**		2
	1.	Принципы построения систем радиосвязи и сетей вещания.	
	2.	Уязвимость информации в системах радиосвязи и сетях вещания.	
	3.	Каналы утечки информации в системах радиосвязи и сетях вещания.	
	4.	Возможные способы несанкционированного доступа в системах радиосвязи и сетях вещания.	
	Самостоятельная работа №4. Составить презентацию		4
	Самостоятельная работа №5. Написать реферат по заданной теме		4
	Самостоятельная работа №6. Решение задач		4
Тема 1.5 Управление доступом в многоканальных телекоммуникационных системах и сетях электросвязи	**Содержание учебного материала**		2
	1.	Организация доступа в многоканальных телекоммуникационных системах и сетях электросвязи.	
	2.	Идентификация и аутентификация. Парольная, атрибутивная, биометрическая идентификация.	
	Практическое занятие №5. Планирование, создание и изменение учетных записей пользователей.		2
	Практическое занятие №6. Создание и администрирование групп пользователей.		2
	Самостоятельная работа №7. Решение задач		2
Тема 1.6 Защитные механизмы различных операционных систем и сред	**Содержание учебного материала**		2
	1.	Защитные механизмы ОС Windows 7 (XP).	
	2.	Защитные механизмы ОС Unix.	
	3.	Защитные механизмы ОС Linux.	
	Практическое занятие №7. Планирование и установка разрешений NTFS для файлов, папок отдельным пользователям и группам.		2
	Практическое занятие №8. Изменение параметров учетных записей пользователей.		2
	Практическое занятие №9. Настройка политики учетных записей.		2
	Практическое занятие №10. Настройка параметров безопасности операционных систем.		2
	Практическое занятие №11. Настройка политики безопасности		2

Тема 1.7 Антивирусные средства	**Содержание учебного материала**		2
	1.	Вирусы. Классификация вирусов.	
	2.	Средства и методы антивирусной защиты.	
	3.	Антивирусные программные и программно-аппаратные комплексы.	
	Самостоятельная работа №8. Написать реферат по заданной теме		5
Тема 1.8 Межсетевое экранирование	**Содержание учебного материала**		2
	1.	Назначение и виды межсетевых экранов (МЭ). Принцип их работы.	
	2.	Выбор схемы расположения межсетевого экрана.	
	3.	Настройка и использование межсетевого экрана.	
	4.	Конфигурирование межсетевого экрана.	
	Самостоятельная работа №9. Составить презентацию		2
Тема 1.9 Шифрование	**Содержание учебного материала**		6
	1.	Симметричные криптосистемы. Шифрование шифрами перестановок, замены и подстановки Система RSA.	
	2.	Криптосистемы с открытым ключом. Системы электронной подписи.	
	3.	Оценка криптостойкости шифров.	
	4.	Методы управления ключами. Инфраструктура открытых ключей PKJ.	
	5.	Программно-аппаратная реализация основных шифров.	
	Практическое занятие №12. Криптографические методы защиты информации. Шифр Цезаря.		2
Тема 1.10 Протоколирование и аудит	**Содержание учебного материала**		2
	1.	Назначение и функции протоколирования и аудита.	
	2.	Активный аудит. Выборочное протоколирование.	
	3.	Настройка протоколирования и аудита в различных О.С.	
	Самостоятельная работа №10. Решение задач		2
Промежуточная аттестация в форме комплексного экзамена (7 семестр)			
МДК.03.02 Технология использования систем условного доступа в сетях вещания			**83**
Тема 1.1. Проверка защищенности телекоммуникационных систем и сетей электросвязи	**Содержание учебного материала**		6
	1. Правила проведения проверок		
	2. Этапы определения конфиденциальности документов объекта защиты.		
	3. Аттестация объекта защиты.		
	Практическое занятие №1 Аттестация объектов информатизации в соответствии с требованиями информационной безопасности		2
	Самостоятельная работа №1 Методы проверки защищенности телекоммуникационных систем и сетей электросвязи (конспект)		4
	Самостоятельная работа №2 Аттестация объекта защиты (сообщение**)**		4

Тема 1.2. Конфигурирование телекоммуникационных систем и сетей электросвязи в соответствии с требованиями информационной безопасности	**Содержание учебного материала**	
	1.Основные требования информационной безопасности к современным телекоммуникационным системам и сетям электросвязи	6
	2. Определение состава оборудования. телекоммуникационных систем и сетей электросвязи в соответствии с требованиями информационной безопасности	
	3. Определение состава программного обеспечения. телекоммуникационных систем и сетей электросвязи в соответствии с требованиями информационной безопасности	
	4. Организация доступа к информации в современных телекоммуникационных системах и сетях электросвязи в соответствии с требованиями информационной безопасности	
	Практическое занятие 2 Конфигурирование сети электросвязи в соответствии с требованиями информационной безопасности	2
	Лабораторная работа №1 Защита информации в многопрофильном колледже Тюменского индустриального университета	2
	Самостоятельная работа №3 Состав оборудования телекоммуникационных систем и сетей электросвязи в соответствии с требованиями информационной безопасности (конспект).	4
	Самостоятельная работа №4 Конфигурирование телекоммуникационной системы в соответствии с требованиями информационной безопасности (алгоритм)	4
Тема 1.3. Состав и назначение комплексной системы информационной безопасности	**Содержание учебного материала**	
	1. Система физической защиты	6
	2. Система управления доступом	
	3. Система защиты программного обеспечения	
	4. Система защиты аппаратного обеспечения	
	Практическое занятие №3 Установка и настройка камер системы видеонаблюдения	2
	Практическое занятие № 4 Установка и настройка датчиков контроля вскрытия устройств	2
	Практическое занятие № 5 Установка и настройка датчиков тревожной сигнализации	2
	Практическое занятие № 6 Установка и настройка специализированного оборудования по защите информации	2
	Практическое занятие №7 Конфигурирование комплексной системы защиты информации	2
	Лабораторная работа №2 Каналы утечки информации по речевому каналу	4
	Самостоятельная работа№ 5 Состав и назначение комплексной системы информационной безопасности (таблица).	2
	Самостоятельная работа №6 Шифрование и дешифровка текста по различным алгоритмам по вариантам (реферат).	6
Тема 1.4. Конфигурирование	**Содержание учебного материала**	
	1.Проверка уровня защищенности объекта защиты. Оценка рисков.	8

комплексной системы защиты информации	2. Разработка политики безопасности для объекта защиты	
	3. Определение конфигурации комплексной системы защиты информации	
	4. Определение состава подсистем, составляющих комплексную систему защиты информации	
	Лабораторная работа №3 Поиск каналов утечки информации с помощью нелинейного локатора SEL SP-61/IVI «Катран».	4
	Самостоятельная работа №7 Составление протокола проверок объекта защиты в соответствии с требованиями информационной безопасности (оформление документации)	4
	Самостоятельная работа №8 Информационная безопасность для объекта защиты (алгоритм)	4
	Самостоятельная работа №9 Криптографические методы защиты информации (презентация)	1
Промежуточная аттестация в форме комплексного экзамена (7 семестр)		
Производственная практика		
Выполнение расчета и установка специализированного оборудования для максимальной защищенности объекта		
Установка и настройка средств и систем защиты.		
Конфигурация автоматизированных систем и информационно-коммуникационных сетей в соответствии с политикой информационной безопасности.		
Тестирование систем с целью определения уровня защищенности.		
Выявление каналов утечки информации.		
Проведение аттестации объекта защиты (проверки уровня защищенности).		**36**
Разработка политики безопасности для объекта защиты.		
Установка, настройки специализированного оборудования по защите информации.		
Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей.		
Конфигурирование автоматизированных систем и информационно-коммуникационных сетей.		
Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей.		
Организации защиты в различных операционных системах и средах.		
	максимальной учебной нагрузки обучающегося	**166**
	обязательной аудиторной учебной нагрузки обучающегося	**100**
	самостоятельной работы обучающегося	**66**
	производственной практики	**36**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

В целях реализации компетентностного подхода при изучении ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания используются активные и интерактивные формы проведения занятий (деловые и ролевые игры, дискуссия, диспут, круглые столы, кейс-метод, работа в малых группах, симуляции, мультимедиа-презентации, просмотр и обсуждение видеофильмов, социальные проекты, приглашение специалистов, экскурсии, творческие задания).

Применение на учебном занятии интерактивных форм работы, стимулирует познавательную мотивацию обучающихся, помогает поддержать мотивацию обучающихся к получению знаний, налаживанию позитивных межличностных отношений, помогает установлению доброжелательной атмосферы. Инициирование и поддержка исследовательской деятельности обучающихся в рамках реализации ими индивидуальных и групповых исследовательских проектов, дает возможность приобрести навык самостоятельного решения проблемы, навык генерирования и оформления собственных идей, навык уважительного отношения к чужим идеям, навык публичного выступления перед аудиторией, аргументирования и отстаивания своей точки зрения.

Для позитивного восприятия обучающимися требований преподавателя, привлечения их внимания к обсуждаемой на занятии информации, активизации их познавательной деятельности на учебных занятиях между преподавателем и обучающимися устанавливаются доверительные отношения.

На учебном занятии соблюдаются общепринятые нормы поведения, правила общения со старшими (преподавателем) и сверстниками (обучающимися), принципы учебной дисциплины и самоорганизации.

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы профессионального модуля обеспечена:

Лаборатория Информационной безопасности для проведения лекционных (теоретических) и практических занятий, междисциплинарной и модульной подготовки, № 405

УМК по дисциплине, дидактический материал.

I. Перечень лабораторного оборудования

Стойка кабельная СМУ-5 – 1 шт. Стойка мобильная СМУ 5 К3 – 1 шт. `

II. ПК, мультимедийное оборудование

Компьютер – 15 шт. Принтер – 1 шт.

III. Лицензионное программное обеспечение

Microsoft Windows (договор № 7810 от 14.09.2021 до 30.11.2022), Microsoft Office Professional Plus (договор № 7810 от 14.09.2021 до 30.11.2022), Zoom (бесплатная версия) – свободно-распространяемое ПО.

Лаборатория Компьютерных сетей для проведения лекционных (теоретических) и практических занятий, междисциплинарной и модульной подготовки, № 405

УМК по дисциплине, дидактический материал.

I. Перечень лабораторного оборудования

Стойка кабельная СМУ-5 – 1 шт. Стойка мобильная СМУ 5 К3 – 1 шт. Мультиплексор Т7-ГМ Телрос – 4 шт.

II. ПК, мультимедийное оборудование

Компьютер – 15 шт. Принтер – 1 шт.

III. Лицензионное программное обеспечение

Microsoft Windows (договор № 7810 от 14.09.2021 до 30.11.2022), Microsoft Office Professional Plus (договор № 7810 от 14.09.2021 до 30.11.2022), Zoom (бесплатная версия) – свободно-распространяемое ПО.

3.2 Информационное обеспечение обучения

3.2.1 Основные источники

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525 (дата обращения: 09.06.2022).

2. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/207095 (дата обращения: 09.06.2022). — Режим доступа: для авториз. пользователей.

3. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89451.html (дата обращения: 09.06.2022). — Режим доступа: для авторизир. пользователей.

3.2.2 Дополнительные источники

1. Гультяева, Т. А. Основы защиты информации : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 83 с. — ISBN 978-5-7782-3641-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91638.html (дата обращения: 09.06.2022). — Режим доступа: для авторизир. пользователей

2. Костин, В. Н. Методы и средства защиты компьютерной информации: криптографические методы для защиты информации : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 40 с. — ISBN 978-5-90695-334-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98201.html (дата обращения: 09.06.2022). — Режим доступа: для авторизир. пользователей

3. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102207.html (дата обращения: 09.06.2022). — Режим доступа: для авторизир. пользователей

4. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102017.html (дата обращения: 09.06.2022). — Режим доступа: для авторизир. пользователей

3.2.3 Профессиональная база данных

1 КонсультантПлюс: Справочно-правовая система : [сайт] – URL: http://www.consultant.ru/ (дата обращения 09.06.2022).- Текст: электронный.

3.2.4 Информационные ресурсы

1. Научное производственное объедение спектрон. [сайт] – URL: http:// www.spectron-ops.ru/ (дата обращения 09.06.2022).-Текст: электронный.
2. Научное производственное объедение протон. [сайт] – URL: http:// www.center-proton.ru (дата обращения 09.06.2022).-Текст: электронный.
3. Микроконтроллерная техника. Схемотехника. [сайт] – URL: http:// www.radio.ru/ (дата обращения 09.06.2022).-Текст: электронный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
1	2	4
ПК 3.1 Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.	- выявление каналов утечки информации; -определение возможных видов угроз; - выбор программно-аппаратных средств защиты информации в соответствии с выявленными угрозами; - выполнение расчета и установки специализированного оборудования для максимальной защищенности объекта; - проведение установки и настройки средств защиты; - конфигурирование автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности - установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 - тестирования по темам 1.1, 1.2, 1.3 Текущий контроль в форме устного опроса по темам МДК 03.02 темам 1.1 ; - выполнения ПЗ № 1 -выполнения СРС №1,2 входного теста
ПК 3.2 Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.	выявлять каналы утечки информации; - определение необходимых средств защиты; - классифицировать угрозы информационной безопасности; - проводить выбор средств защиты в соответствии с с выявленными угрозами; - определять возможные виды атак; - осуществлять мероприятия по проведения аттестационных работ; - разрабатывать политику	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 - тестирования по темам 1.1, 1.2, 1.3 Текущий контроль в форме устного опроса по темам МДК 03.02 Тема № 1.2

	безопасности объекта; - использовать программные продукты, выявляющие недостатки систем защиты; - выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта; - проводить установку и настройку средств защиты; - конфигурировать телекоммуникационные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; -проводить аттестации объекта защиты (проверки уровня защищенности); - разрабатывать политику безопасности для объекта защиты; - устанавливать и настраивать специализированное оборудование по защите информации; - устанавливать и настраивать программных средств защиты автоматизированных систем и информационно-коммуникационных сетей; - выполнять тестирование систем с целью определения уровня защищенности; - использовать программные продукты для защиты баз данных; - применять криптографические методы защиты информации.	- выполнения ПЗ № ,2; - выполнения ЛР №1; -выполнения СРС №№ ,3,4
ПК 3.3 Обеспечивать безопасное администрирование сетей вещания.	- проводить 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	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 - тестирования по темам 1.1, 1.2, 1.3 Текущий контроль в форме устного опроса по темам

	продукты для защиты баз данных; - применять криптографические методы защиты информации.	МДК.03.02: 1,3, 1.4 -выполнения ЛР №2,3 -выполнения ПЗ № 3,4,5,6,7 -выполнения СРС№5,6 7,8,9
ДК 3. Способность осуществлять проверку комплектности, работоспособности технических и программных средств, параметров абонентского и терминального телекоммуникационного оборудования	*- подготовка тестовых программ и вспомогательного оборудования для проверки работоспособности абонентского и терминального телекоммуникационного оборудования и проведения необходимых действий в соответствии с методиками поиска неисправности в нем;* *- подготовка абонентского и терминального телекоммуникационного оборудования к проведению диагностических работ;* *- диагностика абонентского и терминального телекоммуникационного оборудования.*	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 - тестирования по темам 1.1, 1.2, 1.3
ОК 01. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	– демонстрация знаний основных источников информации и ресурсов для решения задач и проблем в профессиональном и/или социальном контексте; – самостоятельный выбор и применение методов и способов решения профессиональных задач в профессиональной деятельности; – способность оценивать эффективность и качество выполнения профессиональных задач; – способность определять цели и задачи профессиональной деятельности; – знание требований нормативно-правовых актов в объеме, необходимом для выполнения профессиональной деятельности	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 №1,2
ОК 02. Организовывать собственную	– способность определять необходимые источники информации;	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты

деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	– умение правильно планировать процесс поиска; – умение структурировать получаемую информацию и выделять наиболее значимое в результатах поиска информации; – умение оценивать практическую значимость результатов поиска; – верное выполнение оформления результатов поиска информации; – знание номенклатуры информационных источников, применяемых в профессиональной деятельности; – способность использования приемов поиска и структурирования информации.	практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 № 1,2
ОК 03. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	– умение определять актуальность нормативно-правовой документации в профессиональной деятельности; – знание современной научной профессиональной терминологии в профессиональной деятельности; – умение планировать и реализовывать собственное профессиональное и личностное развитие	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 №3,4
ОК 04. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	– способность организовывать работу коллектива и команды; – умение осуществлять внешнее и внутреннее взаимодействие коллектива и команды; – знание требований к управлению персоналом; – умение анализировать причины, виды и способы разрешения конфликтов; – знание принципов эффективного взаимодействие с потребителями услуг;	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 №3,4

ОК 05. Использовать информационно-коммуникационные технологии в профессиональной деятельности	– демонстрация знаний правил оформления документов и построения устных сообщений; – способность соблюдения этических, психологических принципов делового общения; – умение грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе; – знание особенности социального и культурного контекста;	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 №5,6
ОК 06. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	− знание сущности гражданско - патриотической позиции, общечеловеческих ценностей; − значимость профессиональной деятельности по профессии;	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 №5,6
ОК 07. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	– умение соблюдать нормы экологической безопасности; – способность определять направления ресурсосбережения в рамках профессиональной деятельности; – знание правил экологической безопасности при ведении профессиональной деятельности; – знание методов обеспечения ресурсосбережения при выполнении профессиональных задач.	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 №5,6
ОК 08. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием,	– умение применять рациональные приемы двигательных функций в профессиональной деятельности; – демонстрация знаний	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10

осознанно планировать повышение квалификации	основ здорового образа жизни; знание средств профилактики перенапряжения.	Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 №7,8,9
ОК 09. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	– способность применения средств информационных технологий для решения профессиональных задач; – умение использовать современное программное обеспечение; – знание современных средств и устройств информатизации; – способность правильного применения программного обеспечения в профессиональной деятельности.	Текущий контроль по МДК.03.01 в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 - выполнения самостоятельных работ №1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Текущий контроль в форме -выполнения самостоятельных работ по МДК.03.02 №7,8,9