Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ 03. Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

по специальности
11.02.10 Радиосвязь, радиовещание и телевидение (углубленной подготовки)
квалификация
специалист по телекоммуникациям

Белгород 2020 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности **11.02.10 Радиосвязь, радиовещание и телевидение (углубленной подготовки)** в соответствии с профессиональным стандартом среднего профессионального образования по специальности **11.02.10 Радиосвязь, радиовещание и телевидение** утвержденного приказом Министерства образования и науки Российской Федерации от 28 июля 2014 г. № 812.

Рассмотрено цикловой комиссией Протокол заседания № 1 от « 31» августа 2020г. Председатель цикловой комиссии _____/Чобану Л.А./	Согласовано Зам. директора по УМР _____/Бакалова Е.Е./ «31» августа 2020г.	Утверждаю Зам. директора по УР _____ /Выручаева Н.В./ «31» августа 2020г.
Рассмотрено цикловой комиссией Протокол заседания № 1 от « » августа 2021г. Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от « » августа 2022г. Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от « » августа 2023г. Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от « » августа 2024г. Председатель цикловой комиссии _____/_____		

Организация-разработчик: ОГАПОУ «Белгородский индустриальный колледж»
Составитель:
преподаватель ОГАПОУ «Белгородского индустриального колледж»
Чобану Л.А.
Экспертиза:
(*внутренний рецензент*) ОГАПОУ «Белгородский индустриальный колледж», преподаватель, Потрясаев В.И.
(*внешний рецензент*) Филиал РТРС «Белгородский ОРТПЦ», директор, Моисеев С.П.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ. 03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности (специальностям) СПО ***11.02.10 Радиосвязь, радиовещание и телевидение*** **(углубленной подготовки)** в части освоения основного вида профессиональной деятельности (ВПД)**: Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания** и соответствующих профессиональных компетенций (ПК):

1. Использовать программно-аппаратные средства защиты информации в радиосвязи и вещания.

2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.

3. Обеспечивать безопасное администрирование сетей вещания.

Рабочая программа профессионального модуля может быть использована дополнительном профессиональном образовании и профессиональной подготовке работников в области защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи при наличии основного общего, среднего (полного) общего образования. Опыт работы не требуется.

Код по Общероссийскому классификатору профессий рабочих, должностей служащих и тарифных разрядов (ОК 016-94)	**Наименование профессий рабочих, должностей служащих**
1	2
10060	Антеннщик-мачтовщик
16019	Оператор связи
17553	Радиомеханик по обслуживанию и ремонту радиотелевизионной аппаратуры
17556	Радиомеханик по ремонту радиоэлектронного оборудования
17562	Радиомонтер приемных телевизионных антенн
17568	Радиотехник
19872	Электромонтер приемопередающей станции спутниковой связи
19876	Электромонтер по ремонту и обслуживанию аппаратуры и устройств связи
19878	Электромонтер станционного оборудования радиорелейных линий связи
19880	Электромонтер станционного оборудования радиофикации
19885	Электромонтер станционного радиооборудования
19887	Электромонтер станционного телевизионного оборудования
27853	Электромеханик средств радио и телевидения

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;
- 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;
- 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.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – 231 **часов**, в том числе:
максимальной учебной нагрузки обучающегося – 195 **часов**, в том числе:
обязательной аудиторной учебной нагрузки обучающегося – 130 часов;
самостоятельной работы обучающегося – 65 **часов** (всего),
в том числе консультаций – 46 **часов.**
учебной и производственной практики – 36 **часов**.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности **Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1	Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.
ПК 3.2	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.
ПК 3.3	Обеспечивать безопасное администрирование сетей вещания.
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.
ОК 4	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.
ОК 6	Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Быть готовым к смене технологий в профессиональной деятельности.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля ПМ 03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

Коды профессиональных компетенций	**Наименования разделов профессионального модуля***	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					***Практика***	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося,**		**Учебная,** часов	**Производственная (по профилю специальности),** *часов (если предусмотрена рассредоточенная практика)*
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего часов**	**в т.ч., курсовая работа (проект),** часов		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	***10***
ПК 3.1-3.3	**Раздел 1.**Ведение комплексной системы защиты информации в телекоммуникационных системах и сетях вещания	**195**	**130**	52	-	**65**	-	-	-
	Производственная практика (по профилю специальности)	**36**							**36**
	Всего:	**231**	**130**	**52**	-	**65**	-	-	**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 учебной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

**Учебная практика (по профилю специальности) может проводиться параллельно с теоретическими занятиями междисциплинарного курса (рассредоточено) или в специально выделенный период (концентрированно).

3.2 Содержание обучения по профессиональному модулю (ПМ):

ПМ 03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов	Уровень освоения
1	2		3	4
Раздел 1. Ведение комплексной системы защиты информации в телекоммуникационных системах и сетях вещания			**195**	
МДК 03.01. Технология применения комплексной защиты информации в системах радиосвязи и сетях вещания			**76**	
Тема 1.1. Концепция информационной безопасности	**Содержание**		**6**	
	1	**Концептуальная модель информационной безопасности**. Безопасность и защита, как одна из областей информатики. Система защиты информации. Система безопасности. Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Определение требований к уровню обеспечения информационной безопасности. Носители защищаемой информации.	**6**	2
	2	**Угрозы безопасности информации.** Понятие угроз информационной безопасности. Угрозы конфиденциальной информации. Виды преднамеренных угроз безопасности. Виды получения информации злоумышленниками: разглашение, утечка, несанкционированный доступ.		2
Тема 1.2. Методы и способы защиты информации	**Содержание**		**42**	
	1	**Основные принципы построения систем защиты информации.** Классификация программно-аппаратных средств защиты информации. Использование программ для обеспечения безопасности конфиденциальной информации. Защита информации от несанкционированных действий. Основные защитные механизмы: идентификация и аутентификация. Идентификация и установление подлинности объекта. Идентификация и установление подлинности документов. Регистрация действий пользователя. Разграничение и контроль доступа. Каналы утечки информации. Побочные электромагнитные излучения и наводки.	**18**	**2**

	2	**Криптографические средства защиты информации** Основные понятия и задачи криптографии. Классификация методов криптографического закрытия. Методы криптографических преобразований. Простейшие шифры перестановки и замены. Криптоанализ. Понятие криптографической стойкости шифров. Компьютеризация шифрования. Шифры с секретными ключами. Симметричные стандарты шифрования. Применение криптосистемы с открытым ключом для аутентификации пользователя со стороны автономного объекта. Кодирование информации. Скремблеры.		**3**
	3	**Защита в операционных системах.** Типовая структура подсистемы безопасности ОС и выполняемые ей функции: идентификация и аутентификация, разграничение доступа, аудит, подотчетность действий, защита обмена данных. Критерии защищенности ОС. Средства обеспечения безопасности в ОС семейств UNIX и Windows		**3**
	4	**Методы идентификации и проверки подлинности пользователей компьютерных систем.** Основные понятия и концепции идентификации и проверки подлинности пользователей компьютерных систем. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы цифровой подписи. Отечественный стандарт цифровой подписи. Биометрические средства идентификации пользователей.		**3**
	5	**Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet.**Многоуровневая защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Internet.		**2**
	6	**Защита информации в компьютерных сетях, антивирусная защита.** Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации в Internet.		**2**
	Лабораторные работы		**24**	
	1	Выявление каналов утечки информации		
	2	Подтверждение и проверка аутентичности и целостности информации.		

	3	Защита от несанкционированного доступа к информации		
	4	Разграничение доступа.		
	5	Создание резервных копий.		
	6	Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации в АСОИУ		
	7	Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем.		
	8	Изучение принципов идентификации и механизмов подтверждения подлинности пользователя. Правила формирования электронной цифровой подписи		
	9	Изучение средств защиты локальных сетей от несанкционированного доступа. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.		
	10	Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия.		
	11	Реализация информационных технологий для построения защищенной информационно-вычислительной сети		
	12	Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet. Угрозы, исходящие от использования «электронной почты».		
Тема 1.3 Защита информации в системах радиосвязи и сетях вещания	**Содержание**		**28**	
	1	**Технические средства обеспечения информационной безопасности радиоэлектронных средств**. Технические средства обеспечения информационной безопасности радиоэлектронных средств. Методы и технические средства радиоразведки, методы обнаружения сигналов, уровень которых ниже уровня информационного сигнала, методы ускоренного поиска частоты излучения и задержки импульсных потоков. Широкополосные сигналы, методы и средства формирования шумоподобных сигналов. Методы и средства формирования малоуровневых сигналов с быстрой перестройкой параметров.	**18**	
	2	**Глобальные информационные сети на базе систем подвижной радиосвязи третьего поколения.** Базовые механизмы защиты данных в беспроводных сетях. Технология DSSS и FHSS. Фильтрации MAC адресов. Аутентификация с использованием MAC-адреса. Использование механизмов защиты, встроенных в точки доступа. Протокол безопасности WEP. Шифрование по протоколу WEP. Защита беспроводных сетей на сетевом уровне. Использование IPSec для защиты трафика беспроводных клиентов. Применение технологии VPN для защиты беспроводных сетей. Стандарты WPA (Wi-FiProtectedAccess) и IEEE 802.11i. Угрозы для беспроводных сетей.		

	3	**Особенности защиты информации от ошибок в системе сотовой подвижной радиосвязи стандарта GSM.** Защита информации от ошибок. Сверточное кодирование и перемежение в полноскоростном речевом канале. Кодирование и перемежение в полноскоростном канале передачи данных. Кодирование и перемежение в каналах управления.		
	4	**Особенности обеспечения безопасности информации в системе сотовой подвижной радиосвязи стандарта GSM.** Общая характеристика безопасности связи. Секретность передачи данных.		
	5	**Практические аспекты защиты информации в системе сотовой подвижной радиосвязи с кодовым разделением каналов.** Особенности защиты информации в системе сотовой радиосвязи стандарта IS-95		
	Лабораторные работы		**10**	
	1	Исследование методов тестирования и контроля защищенных систем радиосвязи		
	2	Исследование методов защиты телетрафика в сетях и систем радиосвязи		
	3	Методы и средства защиты телефонных линий		
	4	Мониторинг и диагностика средств защиты беспроводной локальной сети стандарта IEEE 802.11		
	5	Исследование методов цифровой обработки сигналов на основе сигнальных процессоров в защищенных системах радиосвязи		
Консультации МДК 03.01			**26**	
МДК 03.02. Технология использования систем условного доступа в сетях вещания			**54**	
Тема 2.1. Основные направления защиты информации	**Содержание**		**20**	
	1	**Правовая защита информации**. Организация государственной системы защиты информации. Особенности регулирования прав собственности на информацию. Федеральные нормативные акты: законы, постановления, стандарты. Локальные нормативные акты: положения, приказы, инструкции. Задачи нормативно-правовой базы в регулировании права собственности на информацию.	**12**	**2**
	2	**Организационная защита информации.** Понятие организационной защиты. Организация защиты технических средств обработки и передачи информации. Администрирование и контроль безопасности информации в АС.		**3**

	3	**Инженерно-техническая защита информации** Виды инженерно-технической защиты информации. Охранные системы. Системы ограждения и физической изоляции. Системы опознавания. Технология защиты аппаратных средств ЭВМ: защита внешних накопителей информации, средств отображения, средств передачи данных. Детекторы полей.		**3**
	4	**Технические системы защиты информации.** Структура и принципы действия системы защиты информации. Понятие политики безопасности. Классификация программных средств защиты информации. Использование программ для обеспечения безопасности конфиденциальной информации.		**3**
	Лабораторные работы		**8**	
	1	Установка и настройка оборудования по защите информации		
	2	Обнаружение «радио-жучков»		
	3	Изучение принципа работы детектора поля.		
	4	Установка и настройка программных средств защиты информации		
Тема 2.2. Системы условного доступа в сетях вещания	**Содержание**		**34**	
	1	**Основные параметры оборудования защиты информации, передаваемой по сетям кабельного и наземного телевизионного вещания, от несанкционированного доступа.** Одноуровневая система ограничения доступа. Многоуровневые системы ограничения доступа.	**24**	
	2	**Системы условного доступа в сетях вещания**. Структурные схемы передающих и приемных частей систем ограничения доступа. Структурная схема модуля защиты. Принцип подключения к абонентскому приемнику последовательно соединенных модулей защиты		
	3	**Системы условного доступа для кабельного оператора.** Система условного доступа программно-аппаратное решение для ограничения доступа к программам цифрового ТВ. Система условного доступа Conax. Система условного доступа Crypton. Системы условного доступа CAS _ КТВ. Система условного доступа Stream Guard. Система условного доступа Safeview . Система условного доступа IP CAS / DRM.		
	Лабораторные работы		**10**	
	1-2	Изучение оборудования защиты информации, передаваемой по сетям кабельного		
	3-5	Изучение систем условного доступа для кабельного оператора		
Консультации МДК 03.02			**20**	

Самостоятельная работа при изучении раздела 1 ПМ03. 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. Написание реферата. Реферат расширяет содержание учебного материала. Задание выдается индивидуально. **Примерная тематика внеаудиторной самостоятельной работы:** Расчет и установка программно-аппаратных средств для максимальной защищенности объекта. Задание выдается индивидуально. Написание реферата. Реферат расширяет содержание учебного материала. Задание выдается индивидуально. Изучение биометрических систем идентификации. Изучение и настройка политики безопасности программных средств защиты. Изучение систем опознавания и оповещения. Изучение автоматизированные системы контроля доступа. Приемы работы с техническими средствами защиты информации. Характеристики модулированных сигналов. Принципы съема информации путем демодуляции (детектирования). Искажения информации в результате воздействия на сигналы помех. Виды помех. Методы обеспечения безопасности информации в условиях воздействия помех. Средства пожаротушения, тенденция развития средств пожаротушения. Резервное и аварийное электропитание. Основные характеристики источников резервного электропитания (батарей, аккумуляторов). Средства подавления сигналов закладных устройств в телефонных линиях и цепях электропитания. Принципы работы нелинейных локаторов. Физические принципы работы и способы применения обнаружителей пустот для выявления закладных устройств. Характеристики аналоговых и дискретных (импульсных) электрических сигналов, средств связи, радиолокационных станций, лазерных излучений и других. Признаки, характеризующие физические и химические свойства материальных тел. Понятие о демаскирующих объектах, сигналах и веществах. Методы синтеза информации. Пути автоматизации процессов добывания и обработки информации. Формальные модели безопасности. Криптографические методы защиты. Изучение стандартов шифрования. Исследование нарушений безопасности компьютерных систем. Исследование причин возникновения изъян защиты. Способы записи информации на различные виды носителей. Виды модуляции (манипуляции) сигналов. Функции сотрудников службы безопасности, обеспечивающие инженерно-техническую защиту информации. Сущность технического контроля эффективности защиты информации. Виды моделей и их возможности при исследовании проблем защиты информации.	**19**	
Производственная практика (по профилю специальности) **Виды работ:**	**36**	

1. Выявление каналов утечки информации 2. Определения необходимых средств защиты 3. Проведение аттестации объекта защиты (проверки уровня защищенности) 4. Разработка политики безопасности для объекта защиты 5. Установка, настройка специализированного оборудования по защите информации 6. Выявление возможных атак на автоматизированные системы 7. Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей 8. Конфигурирование автоматизированных систем и информационно-коммуникационных сетей 9. Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей 10. Защита баз данных 11. Организация защиты в различных операционных системах и средах 12. Шифрование информации 13. Понятие аудита информационной безопасности и цели его проведения 14. Практические примеры анализа защищенности корпоративной сети 15. Конфигурирование и настройка компьютерных сетей. 16. Администрирование компьютерных сетей. **17.** Защита сетевого трафика. 18. Изучение основ компьютерных методов шифрования информации по таблице ASCII-кодов перестановкой и заменой. 19. Анализ защищенности информационных систем		
Всего	**231**	

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 лаборатории «Информационной безопасности».

Оборудование лаборатории и рабочих мест:

- автоматизированное рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- маркерная доска;
-компьютеры (рабочие станции);
- локальная сеть;
- мультимедийный класс;
- комплект учебно-методической документации;
- комплект нормативно-правовой документации;
-лицензионное программное обеспечение.

Технические средства обучения:

-рабочее место преподавателя, оснащенное компьютером с лицензионным программным обеспечением, мультимедиа проектором и электронной доской.
- обучающие видеофильмы, презентации

Реализация программы профессионального модуля предполагает обязательную производственную практику (по профилю специальности). Производственную практику (по профилю специальности) рекомендуется проводить концентрированно в специально выделенный период на рабочих местах баз практики.

Оборудование и технологическое оснащение рабочих мест: необходимо наличие современной техники, использование новейших технологий, применение передовых методов организации труда, поддержание строгой дисциплины на производстве, наличие достаточного количества квалифицированного персонала, способного осуществлять систематическую помощь и контроль над процессом прохождения практики, а также наличие материалов, необходимых для составления отчета.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бубнов А.А. Основы информационной безопасности [Текст]: учеб. пособие для студентов учреждений среднего проф. образования. - 3-е изд., стер. - М.: Академия, 2017. - 256 с.

2. Бернет С. Криптография. Официальное руководство RSA Security = RSA Security'sOfficialGuidetoCriptographi / С. Бернет, С. Пэйн ; пер. с англ. под ред. А. И. Тихонова. - 2-е изд., стер. - М. : БИНОМ, 2017. - 381 с.

3. Зайцев А.П. Техническая защита информации М. Горячая линия-Телеком, 2018.-616с.

4. Ищейнов, В.Я. Информационная безопасность и защита информации: словарь

терминов и понятий: словарь / Ищейнов В.Я. — Москва: Русайнс, 2019. — 226 с.

5. Касперски Крис Компьютерные вирусы изнутри и снаружи / Крис Касперски. – СПб.: Питер, 2018. – 526 с.

6. Корнеев И.К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов. - М. : Проспект, 2018. - 333 с.

7. Краковский Ю.М.Информационная безопасность и защита информации : учеб. пособие / Ю. М. Краковский. - М. ; Ростов н/Д : МарТ, 2017. - 287 с.

8. Крылов, Г.О. Базовые понятия информационной безопасности: учебное пособие / Крылов Г.О., Ларионова С.Л., Никитина В.Л. — Москв : Русайнс, 2020. — 257 с.

9. Кузнецова, А.В. Искусственный интеллект и информационная безопасность общества: монография / Кузнецова А.В., Самыгин С.И., Радионов М.В. — Москва: Русайнс, 2020. — 118 с.

10. Куприянов А.И.Основы защиты информации : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М. : Academia, 2017. - 256 с.

11. Мельников В.П. Информационная безопасность [Текст] : Учебник / В. П. Мельников, А. И. Куприянов; Под ред.В,П. Мельникова. - 2-е изд., перераб. и доп. - М. : Академия, 2020. - 268 с.

12. Олифер В.Г. Сетевые операционные системы СПб: Питер, 2016.

13. Сингх С. , Книга шифров. М.: «Издательство Астрель», 2016 г.

14. Таненбаум Э., Компьютерные сети СПб.:Питер, 2016.

15. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с.

Дополнительные источники:

1. С.В. Дворянкин, Д.В. Девочкин "Методы закрытия речевых сигналов в телефонных каналах" “Конфидент”, №5 июль-сентябрь 2015г

2. Киреев С.Ф., Макевнин А.А. Противодействие средствам иностранной технической разведки в СВЧ- и ИК-диапазонах длин волн. Учебное пособие. 2016.

3. Мельников В.П. Информационная безопасность М.: «Академия», 2017, 336с.

4. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений СПО. – М.:ФОРУМ: ИНФРА – М, 2018.

5. В.В. Фомин, В.Н. Дудник, В.Е. Лепин, Т.В. Батенева, М.С. Подлубный "Способ кодирования речевых сигналов для устройств радио-и телефонной связи" -Сб “Техника радиосвязи”, вып 3 2017г.

Интернет-ресурсы:

1. Образовательный портал - http://www.edu.ru;
2. Интернет университет информационных технологий - http://www.intuit.ru;
3. Центр информационной безопасности - http://www.bezpeka.com

4.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к учебной практике в рамках профессионального модуля «**Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания**» является освоение производственной практики для

получения первичных профессиональных навыков в рамках профессионального модуля «Выполнение работ по профессии рабочего».

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу: наличие высшего профессионального образования, соответствующего профилю модуля «Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания» и специальности «Радиосвязь, радиовещание и телевидение».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой Инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1 Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.	- определение необходимых методов и средств защиты информации - демонстрация навыков работы с программными средствами защиты информации; - демонстрация навыков работы с техническими средствами защиты информации; - разработка модели защищенной системы радиосвязи и вещания;	Экспертная оценка защиты лабораторных работ Экспертная оценка выполнения практических занятий Компьютерное тестирование по МДК Оценка выполнения самостоятельной работы студентами Экспертная оценка выполнения практического задания по производственной практике Комплексный экзамен по модулю.
ПК 3.2 Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.	- анализ уровня защищенности сетевой инфраструктуры; - определение всех возможных угроз в сетевой инфраструктуре; - демонстрация навыков использования системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре; - моделирование структуры сети с учетом предъявленных требований; - выбор методов устранения уязвимостей в сети;	
ПК 3.3Обеспечивать безопасное администрирование сетей вещания.	- выбор не обходимой топологии сети; - выбор медов, принципов и способов защиты сети; - выбор специализированных средств ликвидации сетевых атак; - демонстрация навыков использования программных и технических средств защиты информации в сети	

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 –Видение сущности и социальной значимости своей будущей профессии, ее места в социально-экономическом развитии региона и страны –Освоение дополнительных рабочих профессий по профилю ПМ	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	–Определение цели и порядка работы –Обобщение результатов работы –Демонстрация навыков организации собственной деятельности, исходя из цели и способов ее достижения –Анализ рабочей ситуации, текущий и итоговый контроль, оценка и коррекция собственной деятельности	
ОК 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.	–Демонстрация готовности к принятию решений в различных производственных ситуациях –Соответствие принятых решений целям и задачам профессиональной деятельности –Соблюдение нормативно-правовой базы при принятии решений	
ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.	–Использование различных источников информации, включая электронные –Выбор необходимой информации с учетом целей и задач профессиональной деятельности –Оценка достоверности полученной информации –Структурирование профессиональной информации	
ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.	–Применение математических методов и ПК в техническом нормировании, проектировании и выполнении чертежей - Демонстрация владения информационными технологиями - Оформление результатов самостоятельной работы с использованием ИКТ	

ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.	–Взаимодействие с членами коллектива, преподавателями и мастерами, соблюдение норм этикета и профессиональной этики в ходе освоения профессионального модуля –Терпимость к другим мнениям и позициям –Нахождение продуктивных способов реагирования в конфликтных ситуациях	
ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.	–Демонстрация лидерских качеств – Анализ рабочей ситуации, осуществление текущего и итогового контроля деятельности подчиненных –Демонстрация ответственности за результаты своей работы	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	–Анализ собственной деятельности и корректировка траектории роста своего профессионального мастерства –Участие в исследовательской деятельности при выполнении проектов в процессе изучения ПМ –Демонстрация самостоятельного изучения дополнительных источников информации при изучении ПМ	
ОК 9. Быть готовым к смене технологий в профессиональной деятельности.	–Проявление интереса к инновациям в области в области профессиональной деятельности –Поиск и анализ новых технологий в области организации технического обслуживания, ремонта и восстановления узлов и агрегатов автомобилей отечественного и иностранного производства –Готовность к изучению и использованию новых технологий в профессиональной деятельности	