Министерство образования, науки и молодежи Республики Крым

Государственное бюджетное профессиональное образовательное учреждение
Республики Крым
«Симферопольский колледж радиоэлектроники»

УТВЕРЖДАЮ:
Директор
_____О.Ф. Касперова
«__30__»__08_____2019 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

по специальности: 11.02.10 Радиосвязь, радиовещание и телевидения

г. Симферополь
2019 год

Рабочая программа профессионального модуля ПМ.03 разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования **11.02.10 Радиосвязь, радиовещание и телевидение,** утвержденного приказом Министерства образования и науки от 28.07.2014 года № 812.

Организация разработчик Государственное бюджетное профессиональное образовательное учреждение Республики Крым «Симферопольский колледж радиоэлектроники»

Разработчики преподаватели ГБПОУ РК «Симферопольский колледж радиоэлектроники»

- Сапрыкин Сергей Юрьевич

Рассмотрена и одобрена на заседании цикловой методической комиссии №_4_
«_30_»_08_2019 г. Протокол №_1_
Председатель ЦМК_____ *Степанов А.Ю.*

СОГЛАСОВАНО:
Директор по работе с персоналом
ООО «Миранда Медиа»
_____ А.А.Сухов
«_30_»_08_2019 г.

СОГЛАСОВАНО:
Заместитель директора
по учебной работе
_____В.И. Полякова
«_30_»_08_2019 г.

2

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания»

1.1. Область применения программы

Рабочая программа профессионального модуля (далее программа ПМ) – является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО 11.02.10 Радиосвязь, радиовещание и телевидение в части освоения основного вида профессиональной деятельности (ВПД) - техническая эксплуатация информационно-коммуникационных сетей связи и вещания и соответствующих профессиональных компетенций (ПК):

1. Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.
2. Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.
3. Обеспечивать безопасное администрирование сетей 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;
- 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:

максимальной учебной нагрузки обучающегося – 513 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 342 часа;

самостоятельной работы обучающегося – 171 час;

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, 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.	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 ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

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
			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.** Применение комплексной системы защиты информации	**249**	**166**	80		**83**		**-**	**-**
ПК 3.1-3.3	**Раздел 2**. Применение программно-аппаратных средств защиты информации и систем условного доступа в системах радиосвязи и вещания	**264**	**176**	84		**88**			
	Производственная практика (по профилю специальности), часов	**36**							**36**
	Всего:	**513**	**342**	**164**	**-**	**171**	**-**	**-**	**36**

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	Объем часов	Уровень освоения
1	2	3	4
Раздел ПМ 1 Применение комплексной системы защиты информации			
МДК.03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания		**249**	
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание**	10	
	1. Безопасность операционных систем		2
	2. Проблемы обеспечения безопасности операционных систем		2
	3. Угрозы безопасности, защищенная операционная система		2
	4. Архитектура подсистемы защиты операционных систем		2
	5 Функции подсистемы защиты операционных систем, идентификация, аутентификация доступа		2
	Практические занятия	4	2
	1. Настройка операционной системы Windows		
	Лабораторные занятия	8	
	1. Шифрование методом подстановки		2
	2. Дешифрование методом подстановки		2
Тема 1.2. Технологии межсетевых экранов	**Содержание**	12	
	1. Функции межсетевых экранов		2
	2. Фильтрация трафика, выполнение функций посредничества, дополнительные возможности межсетевых экранов		2
	3. Особенности функционирования межсетевых экранов сетей связи		2
	4. Особенности функционирования межсетевых экранов сетей связи		2
	5. Прикладной шлюз, варианты исполнения межсетевых экранов, формирование политики межсетевого взаимодействия		2
	6. Схемы подключения межсетевых экранов, персональные и распределенные межсетевые экраны, проблемы безопасности межсетевых экранов		2
	Практические занятия	16	
	1. Оформление конфиденциальных документов		2
	2. Проведение анализа защищенности объекта защиты информации		2
	3. Проведение анализа защищенности систем защиты информации		2
	Лабораторные занятия	10	
	1. Шифрование методом перестановки		2

	2.	Программная реализация схемы Файстеля		2
Тема 1.3. Технологии защиты на прикладном уровне	**Содержание**		10	
	1.	Управление идентификацией и доступом		2
	2.	Особенности управления доступом, функционирование системы управления доступом		2
	3.	Организация защищенного удаленного доступа		2
	4.	Инфраструктура управления открытыми ключами		2
	5.	Принципы функционирования PKI.		2
	Практические занятия		16	
	1.	Информационные отношения как объект правового регулирования		2
	2.	Допуск должностных лиц и граждан к государственной тайне		2
	3.	Разработка должностных инструкций для лиц, ответственных обеспечение информационной безопасности		2
	Лабораторные занятия		22	
	1.	Программная реализация RSA		2
	2.	Программная реализация DES		2
	3.	Программная реализация MD5		2
Тема 1.4. Каналы утечки информации	**Содержание**		20	
	1.	Классификация, физическая сущность, электромагнитные каналы утечки информации		2
	2.	Технические каналы утечки речевой информации		2
	3.	Характеристика акустического, виброакустического каналов утечки информации		2
	4.	Технические средства и методы получения информации по акустическому каналу		2
	5.	Выявление каналов утечки информации		2
	6.	Технические средства выявления каналов утечки информации		2
	7.	Возможные способы несанкционированного доступа		2
	8.	Способы защиты от каналов утечки информации		2
	9.	Способы, места установки, настройка технических и программных средств защиты		2
	Практические занятия		-	
	Лабораторные занятия		-	
Тема 1.5. Технологии защищенности и обнаружения атак в системах радиосвязи	**Содержание**		12	
	1.	Технология анализа защищенности		2
	2.	Средства анализа защищенности сетевых протоколов и сервисов		2
	3.	Методы анализа сетевой информации, классификация систем обнаружения атак		2
	4.	Защита от вирусов		2
	5.	Классификация компьютерных вирусов		2
	6.	Жизненный цикл вирусов, каналы распространения		2
	Практические занятия		4	2
	1.	Работа с анализатором протоколов Wireshark		
	Лабораторные занятия		-	
Тема 1.6. Управление безопасностью в системах	**Содержание учебного материала**		12	
	1.	Задачи и архитектура управления информационной безопасности в системах радиосвязи		2

радиосвязи	2.	Сущность управления информационной безопасностью в системах радиосвязи		2
	3.	Архитектура управления средствами безопасности		2
	4.	Концепция глобального управления безопасностью, глобальная и локальная политика безопасности		2
	5.	Аудит и мониторинг безопасности систем радиосвязи		2
	6.	Сущность и особенности аудита и мониторинга информационной безопасности систем радиосвязи		2
	Практические занятия		-	
	Лабораторные занятия		-	
	Самостоятельная работа обучающихся		-	
Тема 1.7. Основы технологии виртуальных защищенных сетей	**Содержание учебного материала**		10	
	1.	Построение виртуальных защищенных сетей (VPN)		2
	2.	Основные понятия, классификация и функции сетей VPN, средства обеспечения безопасности VPN		2
	3.	Варианты архитектуры и принципы построения виртуальных защищенных каналов		2
	4.	Логическая структура и компоненты PKI		2
	5.	Дифференцированный зачет		2
	Практические занятия		**-**	
	Лабораторные занятия		**-**	
Самостоятельная работа при изучении раздела ПМ 3 Подготовка к выполнению лабораторной работы Подготовка к практическому занятию Оформление отчета Чтение дополнительной литературы			**83**	
Раздел ПМ 2. Применение программно-аппаратных средств защиты информации и систем условного доступа в системах радиосвязи и вещания			**264**	
МДК.03.02. Технология использования систем условного доступа в сетях вещания			**264**	
Тема 2.1. Основные понятия и направления обеспечения информационной безопасности	**Содержание**		12	
	1.	Основные понятия защиты информации и информационной безопасности		2
	2.	Защита информации, информационная безопасность		2
	3.	Модель информационной безопасности		2
	4.	Угрозы информационной безопасности		2
	5.	Классификация угроз информационной безопасности		2
	6.	Анализ угроз информационной безопасности		2
	Практические занятия		-	

	Лабораторные занятия			
	1. Шифрование методом поли алфавитной подстановки			
Тема2.2. Правовые основы и стандарты информационной безопасности	**Содержание**		30	
	1.	Правовые основы информационной безопасности		2
	2.	Роль стандартов информационной безопасности		2
	3.	Международные стандарты информационной безопасности Стандарты ISO/IEC 17799:2002		2
	4.	Немецкий стандарт BSI, международный стандарт ISO 15408		2
	5.	Отечественные стандарты информационной безопасности Российские стандарты ГОСТ Р ИСО/МЭК 15408-1-2002		2
	6.	Стандарт ГОСТ Р ИСО/МЭК 15408-2-2002		2
	7.	Стандарт ГОСТ Р ИСО/МЭК 15408-3-2002		2
	8.	Стандарт ГОСТ Р 50739-95, ГОСТ Р 50922-96		2
	9.	Стандарт ГОСТ Р ИСО 7498-2-99		2
	10.	Стандарты информационной безопасности в Интернете		2
	11.	Решения по информационной безопасности в протоколах TCP/IP		2
	12.	Решения по информационной безопасности в протоколах SMTP, POP		2
	13.	Политика безопасности. Основные понятия политики безопасности		2
	14	Структура политики безопасности: базовая политика безопасности		2
	15.	Специализированные политики безопасности, процедуры безопасности		2
	Практические занятия		-	
	Лабораторные занятия		12	
	1.	Шифрование методом полиалфавитной подстановки		2
	2.	Дешифрование методом полиалфавитной подстановки		2
	3.	Шифрование методом гаммирования		2
Тема 2.3. Принципы и алгоритмы криптографической защиты информации в системах радиосвязи	**Содержание**		38	
	1.	Основные понятия криптографической защиты информации		2
	2.	Сущность, классификация, принципы криптографической защиты информации, программно-аппаратных средств защиты информации		2
	3.	Симметричные криптосистемы шифрования		2
	4.	Сущность, классификация, симметричные алгоритмы шифрования		2
	5.	Сущность, классификация, основные понятия, блочные алгоритмы шифрования		2
	6.	Асимметричные криптосистемы шифрования		2
	7.	Сущность, классификация, сущность, классификация, алгоритм шифрования RSA		2
	8.	Схема Рабина		2
	9.	Схема Эль-Гамаля		2
	10.	Алгоритм Полига-Хеллмена		2
	11.	Электронная цифровая подпись и функция хэширования		2
	12.	Сущность, классификация, основные процедуры цифровой подписи и функция хэширования		2
	13.	Отечественные криптосистемы шифрования		2
	14.	Основные алгоритмы, электронная цифровая подпись, функция хэширования		2

	15.	Технологии аутентификации		2
	16.	Аутентификация, авторизация и администрирование действий пользователей		2
	17.	Управление криптографическими ключами		2
	18	Генерация, хранение и распределение ключей		2
	19	Общий подход к использованию протоколов		2
	Практические занятия		42	
	1.	Система сотовой связи GSM-900		2
	2.	Структура логических каналов управления и алгоритмы функционирования систем GSM		2
	3.	Интерфейсы, терминальное оборудование, структура TDMA кадров в стандарте GSM		2
	4.	Оборудование подвижных и базовых станций, центра коммутации		2
	5.	Классификация систем персонального радиовызова, пейджеры, репитеры, основные протоколы передачи информации		2
	6.	Изучение методов кодирования речевых сигналов в стандарте TETRA транкинговых сетей		2
	7.	Принципы построения и типы транкинговых систем		2
	Лабораторные занятия		30	
	1.	Вычисление наибольшего делителя для двух чисел при помощи алгоритма Евклида		2
	2.	Программная реализация алгоритма шифрования ГОСТ		2
	3.	Программная реализация генератора простых чисел		2
	4.	Программная реализация алгоритма вычисления символа Лежандра		2
	5	Программная реализация алгоритма вычисления символа Якоби		2
	6	Программная реализация SHA-1		2
Тема 2.4. Основные понятия и принципы функционирования системы условного доступа в сетях вещания	**Содержание**		12	
	1	Система условного доступа (Conditional Access System) — программно-аппаратный механизм для ограничения доступа.		2
	2	Классификация по алгоритму скремблирования – закрытые и на основе единого алгоритма		2
	3	Примеры систем условного доступа. BISS (Basic Interoperable Scrambling System) — система условного доступа для спутниковых каналов связи.		2
	4	Кодировки спутникового телевидения. Основные кодировки, их основные характеристики.		2
	5	Система ограниченного доступа «Роскрипт» для мультимедийных сетей Функциональная схема системы ограниченного доступа.		2
	6	Дифференцированный зачет		2
	Практические занятия		-	
	Лабораторные занятия		-	
Самостоятельная работа при изучении раздела ПМ 2			**88**	
Производственная практика (для СПО – (по профилю специальности) **Виды работ** - выявление каналов утечки информации; - определение необходимых средств защиты; - проведение аттестации объекта;			**72**	

- разработки политики безопасности для объекта защиты; - установка, настройка специализированного оборудования по защите информации; - выявление возможных атак на автоматизированные системы; - 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; - защита баз данных		
Всего	**513**	

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 учебных кабинетов «Обеспечения информационной безопасности в телекоммуникационных сетях и сетях вещания»

Оборудование учебного кабинета и рабочих мест кабинета «Безопасности систем и информационно-коммуникационных сетей связи»:

1. Комплект нормативной документации и стандартов информационной безопасности.
2. Комплект учебно-методической документации.
3. Стенды и наглядные пособия.

Технические средства обучения:

интерактивная доска (раздвижной экран), проектор.

Оборудование лаборатории и рабочих мест лаборатории:

1. Виртуальная лаборатория с установкой на рабочих местах ПЭВМ.
2. Оборудованное рабочее место руководителя занятий: ноутбук, МФУ.
3. Раздаточный материал:
    а) схемы;
    б) карточки-задания;
    в) справочные таблицы.
5. Лабораторные стенды (макеты) для проведения соответствующих лабораторных занятий.
6. Локальная сеть и доступ с рабочих мест к ресурсам Internet.

Реализация программы модуля предполагает обязательную производственную практику.

Оборудование и технологическое оснащение рабочих мест:

1. Контрольно-измерительная система по исследованию цифровой обработки сигналов и измерению электромагнитных излучений и наводок в телекоммуникационных системах.
2. Программно-аппаратный комплекс защищенной телекоммуникационной сети.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бубнов А.А. «Основы информационной безопасности»: учеб. пособие для студ. учреждений сред. проф. образования / Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. – М. : Издательский центр «Академия», 2015. -256с.
2. Партыка Т.Л., Попов И.И. «Информационная безопасность: учебное пособие для студентов учреждений среднего проф.обр.»,2016, Знаниум
3. Назаров А.В., Мельников В.П. Эксплуатация объектов сетевой инфрастуктуры, издательский центр Академия, 2014
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей, ИД «ФОРУМ»: ИНФРА-М, 2017 – 416с.

Дополнительные источники:

1. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере – М. Форум, 2009. – 368 с.
2. Гордейчик С. В., Дубровин В. В. Безопасность беспроводных сетей. – М.: Горячая линия – Телеком, 2008. – 288 с.

3. Вишневский В. М., Портной С. Л., Шахнович И. В. Энциклопедия WiMAX. Путь к 4G. – М.: Техносфера, 2009. – 472 с.
4. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г.
5. Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности"
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
8. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
9. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
10. Федеральный закон РФ от 29 июля 2004 г № 98-ФЗ «О коммерческой тайне».
11. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».
12. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
13. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
14. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.
15. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация

автоматизированных систем и требования по защите информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.

16. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации Решение председателя Гостехкомиссии России от 25 июля 1997 г.
17. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования Решение председателя Гостехкомиссии России от 25 июля 1997 г.
18. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России.
19. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России.
20. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.
21. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России.
22. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России.
23. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России.

Интернет-источники

1. Информационна безопасность бизнеса *http://www.infosecurity.ru*
2. Информзащита. Системный интегратор *http://www.infosec.ru*

4.3. Общие требования к организации образовательного процесса

Условием допуска к производственной практике (по профилю специальности) в рамках профессионального модуля «Обеспечение информационной безопасности систем радиосвязи и вещания» является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля «Выполнение работ по профессии рабочего», а так же изучение освоение дисциплин общепрофессионального цикла и профессиональных модулей.

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 систем радиосвязи и вещания» и специальности «Радиосвязь, телевидение и радиовещание».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

Инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов и учебных дисциплин общепрофессионального цикла.

Мастера: наличие 5–6 квалификационного разряда с обязательной стажировкой в профильных организациях не реже 1-го раза в 3 года.

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**
Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.	– порядок применения программно-аппаратных средств защиты информации; – изложение криптографических методов защиты информации; – обоснование выбора программно-аппаратных средств защиты информации.	*Текущий контроль в форме:* *- тестирование;* *- защиты отчетов по лабораторным и практическим занятиям.* *Зачеты по учебной и производственной практике профессионального модуля.* *Квалификационный экзамен по модулю.*
Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, давать рекомендации по их устранению	– соответствие решений по информационной безопасности угрозам уязвимости сетевой инфраструктуры; – изложение методики анализа защищенности сетевой инфраструктуры.	
Обеспечивать безопасное администрирование систем и сетей	– применение программных и аппаратных методов тестирования безопасности систем и сетей; – демонстрация навыков безопасного конфигурирования систем и сетей радиосвязи и вещания	

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**
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*
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 по обеспечению информационной безопасности систем радиосвязи; – оценка эффективности и качества обеспечения информационной безопасности систем радиосвязи.	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	– выбор и применение методов и способов решения профессиональных задач по обеспечению информационной безопасности систем радиосвязи.	
Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	– эффективный поиск необходимой информации в различных источников, включая электронные.	
Использовать информационно-	– работа на телекоммуникационном	

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
коммуникационные технологии в профессиональной деятельности	оборудовании.	
Работать в коллективе и команде, эффективно общаться с коллегами, руководством потребителями	– взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения.	
Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	– применение профессиональных знаний и навыков; – самоанализ и коррекция результатов собственной работы.	
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	– организация самостоятельных занятий при изучении профессионального модуля.	
Ориентироваться в условиях частой смены технологий в профессиональной деятельности	– анализ инноваций в области информационной безопасности систем радиосвязи.	