МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БАШКОРТОСТАН
Государственное бюджетное профессиональное образовательное учреждение
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности

СОГЛАСОВАНО
Зам. директора
_____ А.В.Арефьев
« » _____2019 г.

УТВЕРЖДАЮ
Зам. директора
_____ Л.Р. Туктарова
« » _____2019 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи

название программы профессионального модуля

Специальность:
11.02.09. Многоканальные телекоммуникационные системы

Уровень подготовки: базовый

СОГЛАСОВАНО
Зав. кафедрой
_____ Э.Р. Кабирова

РАЗРАБОТАЛИ:
Преподаватель А.Н. Мочалов

Уфа 2019 г

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1.Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы ГБПОУ УКРТБ в соответствии с ФГОС третьего поколения по специальности СПО:

11.02.09 Многоканальные телекоммуникационные системы

код *наименование специальности (уровень подготовки)*

в части освоения основного вида деятельности (ВД):

Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.

ПК 3.2. Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, давать рекомендации по их устранению.

ПК 3.3. Обеспечивать безопасное администрирование телекоммуникационных систем и сетей электросвязи.

Рабочая программа профессионального модуля может быть использована в дополнительном образовании в рамках подготовки специалистов по курсу «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи».

1.2 Цели и задачи дисциплины – требования к результатам освоения дисциплины

В результате освоения профессионального модуля обучающийся должен иметь практический опыт:

- выявление каналов утечки информации;
- определение необходимых средств защиты;
- проведения аттестации объекта защиты (проверки уровня защищенности);
- разработки политики безопасности для объекта защиты;
- установки, настройки специализированного оборудования по защите информации;
- выявление 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;

В результате освоения профессионального модуля обучающийся должен уметь:
- классифицировать угрозы информационной безопасности;
- проводить выбор средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;
- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- использовать программные продукты, выявляющие недостатки систем защиты;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
- производить установку и настройку средств защиты;
- конфигурировать автоматизированные системы информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
- выполнять тестирование системы с целью определения уровня защищенности;
- использовать программные продукты для защиты баз данных;
- применять криптографические методы защиты информации;

В результате освоения профессионального модуля обучающийся должен знать:
- каналы утечки информации;
- назначение, классификацию и принципы работы специализированного оборудования;
- принципы построения информационно-коммуникационных сетей;
- возможные способы несанкционированного доступа;
- нормативно-правовые и законодательные акты в области информационной безопасности;
- правила проведения возможных проверок;
- этапы определения конфиденциальности документов объекта защиты;
- технологии применения программных продуктов;
- возможные способы, места установки и настройки программных продуктов;
- конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- средства защиты различных операционных систем и сред;
- способы и методы шифрования информации.

Количество часов на освоение профессионального модуля:

Всего - 172 часа, в том числе:
максимальной учебной нагрузки обучающегося - 136 часа
обязательной аудиторной учебной нагрузки обучающегося - 96 часов
самостоятельной работы обучающегося - 40 часа
учебной практики - 36 часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ.

Результатом освоения программы профессионального модуля является овладение обучающимися видом деятельности

Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи

в том числе профессиональными (ПК) и общими (ОК) компетенциями по базовой и углубленной подготовке:

Код	Наименование результата обучения
ПК 3.1	Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.
ПК 3.2	Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, давать рекомендации по их устранению.
ПК 3.3	Обеспечивать безопасное администрирование телекоммуникационных систем и сетей электросвязи.
Базовая подготовка	
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.

3. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Код профессиональных компетенций	Наименования разделов профессионального модуля*	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		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		
ПК 2.1 ПК 2.2 ПК 2.3	**Раздел 1.** Владение технологией применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**88**	**60**	32	**-**	**28**	**-**	**-**	**-**

* Раздел профессионального модуля – часть примерной программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

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

ПК 2.1 **ПК 2.2** **ПК 2.3**	**Раздел 2.** Владение технологией применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**48**	**36**	16	**-**	**12**	**-**	**-**	**-**
	Учебная практика, часов	**36**						36	
	Всего:	**172**	**96**	48	**-**	**40**	**-**	**36**	**-**

3.2 Содержание обучения по профессиональному модулю

Наименование разделов и профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)		Объем часов	Уровень освоения
				Базовая подготовка
1	**2**		**3**	
VI семестр				
Раздел 1. Владение технологией применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи			**88**	
МДК 01. Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи			**88**	
Тема 1.1 Конфигурирование защищаемых сетей **Заочное обучение:**	**Содержание учебного материала**		**6**	
	1	**Конфигурация защищаемых сетей.** Полностью контролируемые системы. Частично контролируемые системы. Операционные системы Windows 7, Windows 8, Windows XP,	2	2

Аудиторное обучение: 2 часа **Практические занятия – 2 часа**		Linux, QNX и другие.		
	Практические занятия		4	
	1-2	Конфигурирование автоматизированных систем и информационно-коммуникационных сетей в соответствии с политикой информационной безопасности		
Тема 1.2 Собственные средства защиты различных операционных систем и сред **Заочное обучение:** **Аудиторное обучение: 2 часа** **Практические занятия – 2 часа**	**Содержание учебного материала**		**8**	
	1	**Обзор современных систем управления сетевой защитой.** Классификация систем защиты, перспективы и тенденции в развитии систем защиты	2	1
	2	**Технологии аутентификации.** Аутентификация, авторизация и администрирование действий пользователя	2	1
	3	**Методы аутентификации.** Пароли. PIN-коды. Методы надежного составления паролей.	2	1
	4	**Строгая аутентификация.** Односторонняя аутентификация. Двухсторонняя аутентификация.	2	1
Тема 1.3 Технологии применения программных продуктов. Возможные способы, места установки и настройки программных продуктов. **Заочное обучение:** **Аудиторное обучение: 2 часа** **Практические занятия – 2 часа**	**Содержание учебного материала**		**20**	
	1	**Технологии защиты от вирусов.** Компьютерные вирусы и проблемы антивирусной защиты.	2	2
	2	**Классификация компьютерных вирусов.** Жизненный цикл вирусов. Основные каналы распространения вирусов и вредоносных программ	2	3
	3	**Архитектура подсистемы защиты операционной системы Windows 7.** Особенности Операционной системы Windows. Возможности администратора.	2	3
	4	**Локальная политика безопасности.** Локальная политика безопасности. Настройка. Администрирование системы.	2	3
	Практические занятия		12	
	3-4	Использование программных продуктов. Использование программных продуктов, выявляющих недостатки систем защиты антивирусных продуктов		

	5-6	Использование программных продуктов локальной политики безопасности Windows. Установка, настройка		
	7-8	Использование программных продуктов политики паролей. Установка, настройка		
Тема 1.4 Возможные способы несанкционированного доступа **Заочное обучение:** **Практические занятия – 2 часа**	**Содержание учебного материала**		**14**	
	1	**Разграничение доступа к объектам Операционной системы.** Модели доступа. Дискреционная модель. Мандатная модель. Роли	2	2
	Практические занятия		12	
	9-10	Классифицирование угроз информационной безопасности. Проведение оценки степени вероятности реализации угроз		
	11-12	Проведение выборки средств защиты и нейтрализации угроз в соответствии с выявленными угрозами		
	13-14	Определение возможных видов атак (моделирование схемы технических каналов утечки информации)		
Тема 1.5 Назначение. Классификация и принципы работы специализированного оборудования.	**Содержание учебного материала**		**6**	
	1	**ActiveDirectory** Комплексная система организации управления доступом. Инсталляция. Настройка.	2	3
	Практические занятия		4	
	15-16	Выполнение установки и настройки средства защиты-виртуального токена (межсетевого экрана)		
Тема 1.6 Каналы утечки информации	**Содержание учебного материала**		**6**	
	1	**Особенности утечки информации.** Типовая структур и виды технических каналов утечки информации. Основные показатели технических каналов утечки информации.	2	2
	2	**Радиоэлектронные каналы утечки информации.** Виды радиоэлектронных каналов утечки информации. Распространение опасных электрических и радиосигналов в радиоэлектронном канале утечки информации.	2	1
	3	**Оптические каналы утечки информации.** Оптико-электронный канал. Оптические диапазоны.	2	1

Самостоятельная работа при изучении раздела ПМ 1. 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 Поиск в интернете и оформление заданной информации в рамках изучаемой дисциплины Подготовка докладов Работа со справочной и нормативной литературой **Самостоятельная работа при изучении раздела ПМ 1 (заочное отделение)** 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 Поиск в интернете и оформление заданной информации в рамках изучаемой дисциплины Подготовка докладов Работа со справочной и нормативной литературой		**28** **14**	
Примерная тематика домашних заданий			
1.1	1. Чтение и анализ литературы: [3] стр. 223-229		
1.2	1. Чтение и анализ литературы: [3] стр. 223-229		
	2. Чтение и анализ литературы: [3] стр. 172-176		
	3. Чтение и анализ литературы: [3] стр. 176-186		
	4. Чтение и анализ литературы: [3] стр. 188-196, решение вариативных задач		
1.3	1. Чтение и анализ литературы: [3] стр. 444-446, решение вариативных задач		
	2. Чтение и анализ литературы: [3] стр. 454-465, решение вариативных задач		
	3. Чтение и анализ литературы: [3] стр. 229-231		
	4. Чтение и анализ литературы: [3] стр. 231-239		
1.4	1. Чтение и анализ литературы: [3] стр. 231-239		
1.5	1. Чтение и анализ литературы: [3] стр. 488-491		
1.6	1. Чтение и анализ литературы: [4] стр. 7-10		
	2. Чтение и анализ литературы: [4] стр. 7-14		
	3.Чтение и анализ литературы: [4] стр. 12-14		

Раздел 2 Владение технологией применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи			**48**	
МДК 02. Технология применения комплексной системы защиты информации			**48**	
Тема 2.1 Нормативно-правовые и законодательные акты в области информационной безопасности **Заочное обучение:** **Аудиторное обучение - 1 часа** **Практические занятия – 1 часа**	**Содержание учебного материала**		**4**	
	1	**Актуальность информационной безопасности в системе национальной безопасности России. Сущность и понятие информационной безопасности.** Национальные интересы в информационной сфере. Влияние процессов информатизации общества на составляющие национальной безопасности. Понятие информационной безопасности. Характеристика составляющих информационной безопасности. Источники и содержание угроз в информационной сфере. Состояние информационной безопасности России и основные задачи по ее обеспечению.	2	1
	2	**Принципы обеспечения информационной безопасности.** Общеметодологические принципы обеспечения информационной безопасности. Концептуальная модель информационной безопасности.	2	1
Тема 2.2 Принципы построения информационно-коммуникационных сетей **Заочное обучение:** **Аудиторное обучение - 1 час** **Практические занятия – 1 час**	**Содержание учебного материала**		**6**	
	1	**Обеспечение информационной безопасности сетей.** Способы обеспечения информационной безопасности сетей. Пути решения проблем защиты информации в сетях.	2	2
	Практические занятия		4	
	1	Использование программных продуктов для защиты баз данных-методом шифрования		
	2	Разработка политики безопасности объекта: выполнение расчета и установки специализированного оборудования для максимальной защиты		

		объекта		
Тема 2.3 Способы и методы шифрования информации **Заочное обучение:** **Аудиторное обучение - 1 час** **Практические занятия – 1 час**	**Содержание учебного материала**		**8**	
	1	**Криптографические методы.** Шифрование. Кодирование. Стенография. Сжатие.	2	2
	2	**Традиционные шифры с симметричным ключом.** Шифры замены. Шифры перестановки. Поточные и блочные шифры. Механизация шифрования.	2	3
	Практические занятия		4	
	3-4	Применение криптографических методов защиты информации		
Тема 2.4 Этапы определения конфиденциальности документов объекта защиты **Заочное обучение:** **Аудиторное обучение - 1 час** **Практические занятия – 1 час**	**Содержание учебного материала**		**10**	
	1	**Целостность сообщения.** Случайная модель Oracle. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. Анализ безопасности хэш-функций. Атаки на хэш-функции.	2	3
	2	**Электронная цифровая подпись.** Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.	2	2
	3	**Установление подлинности объекта.** Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены.	2	2
	Практические занятия		4	
	5	Осуществление мероприятий по проведению аттестационных работ – (составлении перечня мероприятий, для проведения процедуры лицензирования предприятий)		
Тема 2.5 Правила проведения возможных проверок	**Содержание учебного материала**		**2**	
	1	**Аудит безопасности операционных систем.** Методы проведения контрольных, проверочных мероприятий. Программные средства аудита.	2	1
Тема 2.6 Алгоритма работы тестовых программ	**Содержание учебного материала**		**6**	
	1	**Алгоритмы работы тестовых программ.** Составление алгоритма хэш-функции. Составление алгоритма шифра	2	3

	Практические занятия		4	
	6	Выполнение тестирования систем с целью определения уровня защищенности		
Самостоятельная работа при изучении раздела ПМ 2. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленных преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя Оформление лабораторных работ, отчетов и подготовка к их защите Поиск в интернете и оформление заданной информации в рамках изучаемой дисциплины Подготовка докладов Работа со справочной и нормативной литературой **Самостоятельная работа при изучении раздела ПМ 2.** (заочное отделение) Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленных преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя Оформление лабораторных работ, отчетов и подготовка к их защите Поиск в интернете и оформление заданной информации в рамках изучаемой дисциплины Подготовка докладов Работа со справочной и нормативной литературой			**12** **40**	
Примерная тематика домашних заданий				
2.1	1. Чтение и анализ литературы: [1] стр. 10-14 2. Чтение и анализ литературы: [1] стр. 27-42, [3] стр. 9-15			
2.2	1. Чтение и анализ литературы: [3] стр. 40-42			
2.3	1. Чтение и анализ литературы: [1] стр. 28-32 2. Чтение и анализ литературы: [1] стр. 71-114			
2.4	1. Чтение и анализ литературы: [1] стр. 366-386 2. Чтение и анализ литературы: [1] стр. 419-441 3. Чтение и анализ литературы: [1] стр. 448-468			
2.5	1. Чтение и анализ литературы: [3] стр. 239-241			
2.6	1. Чтение и анализ литературы: [3] стр. 241-252			

Учебная практика **Виды работ:**	**Содержание**		**36**	
	1	Выявление каналов утечки информации; Определение необходимых средств защиты; Проведения аттестации объекта защиты (проверки уровня защищенности);	6	
	2	Разработка политики безопасности для объекта защиты; Установка, настройка специализированного оборудования по защите информации;	6	
	3	Выявление возможных атак на автоматизированные системы;	6	
	4	Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;	6	
	5	Конфигурирование автоматизированных систем и информационно-коммуникационных сетей; Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей;	6	
	6	Защита баз данных; Организация защиты в различных операционных системах и средах; Шифрование информации;	6	
Всего:			**172**	
Заочное обучение: всего 22 ч, из которых лекции 10 ч, практические занятия – 12 ч				

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:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-методических документации;
- дидактические материалы.
- учебно-наглядные пособия по дисциплине «Информационная безопасность и защита информации»:

-плакаты:

- «Модель информационной безопасности»;
- «Технические каналы утечки информации»;
- «Односторонне функции шифрования»;
- «Модель угроз информационной безопасности»;
- «Сертификаты открытых ключей»

- презентации:

- «Технические средства защиты информации»;
- «Инженерно технические средства защиты информации»;
- «Средства криптографической защиты информации »;

- учебный фильм:

- «Зашифрованная война»

- мультимедиа проектор, компьютер преподавателя;

Технические средства обучения:

- персональные компьютеры (объединенные в учебную локально-вычислительную сеть с выходом в сеть Интернет) по количеству обучающихся с лицензионным программным обеспечением: ОС WindowsXP, WindowsServer, ОС Unix;
- учебно-лабораторный комплекс «Криптон» (Платы «Криптон-замок», аппаратные абонентские и сетевые шифраторы, программное обеспечение);
- учебно - лабораторный комплекс беспроводной сети Wi-Fi; - лабораторное измерительное оборудование:
- осциллограф - 2 шт.;
- частотомер - 2 шт.;
- генератор - 1 шт.;
- мультиметр - 4 шт.;
- источник питания - 6 шт.;

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: РиС, 2015. - 586 с.

2. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2017. - 368 с.

3. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 392 с.

4. Ищейнов, В.Я. Защита конфиденциальной информации: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2016. - 256 с.

5. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.

6. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2017. - 352 с.

7. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.

8. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2015. - 592 с.

9. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2015. - 702 с.

Дополнительные источники:

1. Руководство администратора ППКОП «Астра»
2. Руководство администратора КТМ-256

Интернет ресурсы:

1. http://www.fstec.ru
2. http://www.ancad.ru
3. http://www.locks.ru
4. Электронно-библиотечная система. [Электронный ресурс] – режим доступа: http://znanium.com/ (2002-2019)

4.3. Общие требования к организации образовательного процесса.

Освоение профессионального модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» производится в соответствии с учебным планом по специальности 11.02.09. Многоканальные телекоммуникационные системы и календарным графиком.

Образовательный процесс организуется строго по расписанию занятий. График освоения профессионального модуля предполагает последовательное освоение МДК «Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи» и «Технология применения комплексной системы защиты информации», включающих в себя как теоретические, так и лабораторно-практические занятия.

Освоению модуля предшествует обязательное изучение учебных дисциплин: «Теория электросвязи», «Физика», «Основы телекоммуникаций», «Электронная техника» и профессионального модуля «Техническая эксплуатация информационно-коммуникационных сетей связи».

При проведении лабораторных работ / практических занятий проводится деление групп студентов на подгруппы, численность не более 15 человек. Лабораторные работы проводятся в специальной лаборатории информационной безопасности.

В процессе освоения профессионального модуля предполагается проведение рубежного контроля знаний, умений у студентов. Сдача рубежного контроля является обязательной для всех обучающихся. Результатом освоения профессионального модуля выступают профессиональные компетенции, оценка которых представляет собой создание и сбор свидетельств деятельности на основе заранее определенных критериев.

С целью оказания помощи студентам при освоении теоретического и практического материала, выполнения самостоятельной работы разрабатываются учебно-методические комплексы.

С целью методического обеспечения прохождения практики разрабатываются учебно-методические рекомендации для студентов.

При освоении профессионального модуля каждым преподавателем устанавливаются часы дополнительных занятий, в рамках которых для всех желающих проводятся консультации. График проведения консультаций развешен на входной двери каждой лаборатории.

Обязательным условием допуска к учебной практике в рамках профессионального модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» является выполнение всех лабораторных/практических работ в рамках профессионального модуля.

Текущий учет результатов освоения профессионального модуля производится в журнале по профессиональному модулю. Наличие оценок по лабораторным и практическим работам и рубежному теоретическому контролю являются для каждого студента обязательным. В случае отсутствия оценок по ЛПР и ТРК студент не допускается до сдачи квалификационного экзамена по профессиональному модулю.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): высшее образование, соответствующее профилю преподаваемого модуля.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой.

Инженерно-педагогический состав: высшее техническое образование; опыт работы в должности, связанной с направлением деятельности, соответствующей профилю подготовки обучающихся.

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

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Форма и методы контроля и оценки**
ПК 3.1. Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.	- проведение выбора программно-аппаратных средств защиты для конкретной ситуации. - использование установленных программно-аппаратных средств защиты для защиты информации.	Выполнение и защита лабораторных и практических работ. Тестирование, зачеты по учебной практике и по каждому из разделов профессионального модуля
ПК 3.2. Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, давать рекомендации по их устранению.	- знание системы защищенности информации - выполнение анализа систем защищенности информации - использование анализа систем защищенности для обнаружения уязвимости в сетевой инфраструктуре - разработка рекомендаций по устранению уязвимости в сетевой инфраструктуре	Выполнение и защита лабораторных и практических работ. Тестирование, зачеты по учебной практике и по каждому из разделов профессионального модуля
ПК 3.3. Обеспечивать безопасное администрирование телекоммуникационных систем и сетей электросвязи.	- участвует в администрировании аппаратных средств шифрования - участвует в администрировании системы контроля доступа к сетям связи - участвует в администрировании внедренных средств защиты информации	Выполнение и защита лабораторных и практических работ. Тестирование, зачеты по учебной практике и по каждому из разделов профессионального модуля

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.

Базовая подготовка

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.	Понимание сущности и социальной значимости профессии, проявление к ней устойчивый интерес.	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.	Организация собственной деятельности, выбор типовых методов и способов выполнения профессиональных задач, оценка их эффективности и качества	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	Принятие решений в стандартных и нестандартных ситуациях и нести за них ответственность	
Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	Осуществление поиска и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	
Использовать информационно-коммуникационные технологии в профессиональной деятельности.	Использование информационно-коммуникационных технологий в профессиональной деятельности	
Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	Работа в коллективе и команде, эффективное общение с коллегами, руководством, потребителями.	
Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	Взятие на себя ответственности за работу членов команды (подчиненных), результат выполнения заданий	
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	Определение задачи профессионального и личностного развития, повышать самообразование, сознательное планирование повышение квалификации.	
Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Ориентация в условиях частой смены технологий в профессиональной деятельности	

Приложение 1
Обязательное

КОНКРЕТИЗАЦИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ МОДУЛЯ

ПК 3.1. Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.	
Иметь практический опыт: - установки и настройки специализированного оборудования по защите информации - установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей - конфигурирования автоматизированных систем и информационно-коммуникационных сетей.	**Виды работ на практике:** Ознакомление с программно-аппаратными средствами защиты информации, их подключение. Ознакомление с программными средствами защиты информации, их настройка. Ознакомление с организацией системы контроля доступа на предприятии. Ознакомление, организации, настройка проводной защищенной сети. Ознакомления, организации, настройка беспроводной локальной сети. Участие в организации работ по защите локальных сетей на предприятии связи. Выбор программных средств шифрования.
Уметь: - проводить выборку средств защиты в соответствии с выявленными угрозами - выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта - использовать программные продукты выявляющие недостатки систем защиты	**Тематика практических занятий.** Использование программных продуктов, выявляющих недостатки систем защиты – антивирусных продуктов Использование программных продуктов локальной политики безопасности Windows, установка, настройка Использование программных продуктов политики паролей, установка, настройка Выполнение установки и настройки средств защиты – виртуального токена (межсетевого экрана) Разработка политики безопасности выполнение расчета и установки % выполнение расчета и установки специализированного оборудования для максимальной защиты объекта (расчет сетевых помехозащищающих фильтров, полосно-пропускающих и полосно-заграждающих фильтров.) Использование программных продуктов для защиты баз данных методом шифрования
Знать: - средства защиты различных операционных систем и сред; - технология применения	**Перечень тем:** Собственные средства защиты различных операционных систем и сред Технологии применения программных продуктов. Возможные способы, места установки и настройки программных продуктов Назначение, классификации и принципы работы специализированного оборудования

программных продуктов; - возможные способы, места установки и настройки программных продуктов; - назначение, классификации и принципы работы специализированного оборудования; - принципы построения информационно-коммуникационных сетей	«Принципы построения информационно-коммуникационных сетей»
Самостоятельная работа студента	**Тематика самостоятельной работы** Самостоятельная проработка конспектов занятий, учебной и специальной 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.
ПК 3.2. Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, давать рекомендации по их устранению.	
Иметь практический опыт: - выявления каналов утечки, определения необходимых средств защиты - выявления возможных атак на автоматизированные системы - проверки защищенности автоматизированных систем и информационно-коммуникационных сетей - защита баз данных	**Виды работ на практике:** Участие в организации работ по защищенности персональных компьютеров на предприятии. Участи в организации работ по защищенности локальных сетей на предприятии. Выявление каналов утечки информации в информационно-коммуникационных сетях. Анализ защищенности беспроводной сети передачи данных. Анализ защищенности проводной сети передачи данных. Участие в выявлении возможных атак на автоматизированные системы. Участие в проверке защищенности автоматизированных систем, информационно-коммуникационных сетей, баз данных.
Уметь: - классифицировать угрозы информационной безопасности - определять возможные виды атак - применять криптографические	Тематика практических занятий Классифицирования угроз информационной безопасности. Проведение оценки степени вероятности реализации угроз Проведение выборки средств защиты и нейтрализации угроз в соответствии с выявленными угрозами Определение возможных видов атак Моделирование схемы технических каналов утечки информации Применение криптографических методов защиты информации

методы защиты информации	
Знать: - каналы утечки информации; - возможные способы несанкционированного доступа; - способы и методы шифрования информации;	**Перечень тем:** Возможные способы несанкционированного доступа Каналы утечки информации Способы и методы шифрования информации
Самостоятельная работа студента	**Тематика самостоятельной работы** Самостоятельная проработка конспектов занятий, учебной и специальной 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.
ПК 3.3. Обеспечивать безопасное администрирование телекоммуникационных систем и сетей электросвязи.	
Иметь практический опыт: - проведения аттестации объекта защиты (проверки уровня защищенности) - разработки политики безопасности для объекта защиты	**Виды работ на практике** Администрирование программных средств шифрования Администрирование аппаратных средств шифрования Администрирование систем контроля доступа Администрирование межсетевого экрана Администрирование систем антивирусной защиты Администрирование проводной защищенной сети Администрирование беспроводной защищенной сети
Уметь: - осуществлять мероприятия по проведению аттестационных работ - разрабатывать политику безопасности объекта - выполнять тестирование систем с целью определения уровня защищенности.	**Тематика практических занятий** «Конфигурирование автоматизированных систем и информационно-коммуникационных сетей в соответствии с политикой информационной безопасности» «Осуществление мероприятий по проведению аттестационных работ» «Выполнение тестирования систем с целью определения уровня защищенности»
Знать: - принципы построения информационно-коммуникационных сетей - правила проведения возможных проверок - нормативно-правовые и законодательные акты в области	**Перечень тем:** Конфигурирование защищаемых сетей Нормативно-правовые акты в области информационной безопасности. Этапы определения конфиденциальности документов объекта защиты Правила проведения возможных проверок Алгоритмы работы тестовых программ.

информационной безопасности - этапы определения конфиденциальности документов объекта защиты - конфигурации защищаемых сетей - алгоритмы работы тестовых программ	
Самостоятельная работа студента	**Тематика самостоятельной работы** Самостоятельная проработка конспектов занятий, учебной и специальной 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.

Приложение 2
Обязательное

ТЕХНОЛОГИИ ФОРМИРОВАНИЯ ОК

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.	- выполняет профессиональные задачи - проявляет творческую инициативу, демонстрирует профессиональную подготовку	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 2 Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- планирует деятельность, применяя технологию с учетом изменения параметров объекта, к объекту того же класса, сложному объекту(комбинирует несколько алгоритмов последовательно или параллельно); -выбирает способ достижения цели в соответствии с заданными критериями качества и эффективности.	
ОК 3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- проводит анализ причин существования проблемы -предлагает способ коррекции деятельности на основе результатов оценки продукта -определяет эффективные показатели результативности деятельности в соответствии с поставленной профессиональной задачей - задает критерии для определения способа разрешения проблемы - прогнозирует последствия принятых решений - называет риски на основе самостоятельно проведенного анализа ситуации - предлагает способы предотвращения и способы нейтрализации рисков.	
ОК 4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных	-предлагает и анализирует источник информации определенного типа/ конкретный источник для получения	

задач, профессионального и личностного развития.	недостающей информации и обосновывает свое предложение -характеризует произвольно заданный источник информации в соответствии с задачей деятельности, принимает решения о завершении/ продолжении информационного поиска на основе оценки достоверности/непротиворечивости полученной информации -извлекает и оценивает информацию по самостоятельным сформулированным основаниям, исходя из понимания цели выполняемой работы, систематизирует информацию в рамках самостоятельно выбранной структуры - делает вывод о причинах событий и явлений на основе причинно следственного анализа информации о них, делает общения на основе предоставленных эмпирических или статистических данных	
ОК 5 Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- применяет ИКТ при выполнении профессиональных задач	
ОК 6 Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- фиксирует особые мнения; использует приемы выхода из ситуации, когда дискуссия зашла в тупик, или резюмирует причины, по которым группа не смогла добиться результатов обсуждения - дает сравнительную оценку идей, высказанных участниками группы, относительно цели групповой работы - самостоятельно готовит средства наглядности; самостоятельно выбирает жанр монологического высказывания в зависимости от его цели и цели аудитории - работает с вопросами в развитии	

	темы и/ или на дискредитации позиции - выделяет и соотносит точки зрения, представленные в диалоге или дискуссии - самостоятельно определяет жанр продукта письменной коммуникации в зависимости от цели, содержания и адресата	
ОК 7 Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	-мотивирует членов команды с целью организации эффективной работы - умеет представить результаты выполненной работы -оценивает работу и контролирует работу группы - отвечает за результат выполнения заданий - мотивирует членов команды с целью организации эффективной работы - умеет представить результаты выполненной работы - оценивает работу и контролирует работу группы	
ОК 8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- анализирует собственные мотивы и внешнюю ситуацию при принятии решений, касающихся своего продвижения	
ОК 9 Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- применяет современные технологии в профессиональной деятельности	