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

УТВЕРЖДАЮ
Директор
_____ И.В. Нуйкин
«___»_____2021 г.

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ03 *ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ*

СОГЛАСОВАНО
Зав. кафедрой
_____ Кабирова Э.Р.

РАЗРАБОТАЛИ:
Преподаватели
Кислицин Н.А.
Кабирова Э.Р.

Уфа, 2021 г.

Составитель:
Кислицин Никита Алексеевич, преподаватель ГБПОУ УКРТБ
Кабирова Эльмира Ринатовна, преподаватель высшей категории ГБПОУ УКРТБ

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

название профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ» и соответствующие ему профессиональные компетенции и общие компетенции:

Перечень общих компетенций

Код	*Наименование общих компетенций*
ОК 01	*Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.*
ОК 02	*Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.*
ОК 03	*Планировать и реализовывать собственное профессиональное и личностное развитие.*
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

Перечень профессиональных компетенций

Код	*Наименование видов деятельности и профессиональных компетенций*
ВД 1	Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи
ПК 3.1.	**Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.**
ПК 3.2.	**Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.**
ПК 3.3.	**Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием** специализированного программного обеспечения и оборудования.

В результате освоения профессионального модуля студент должен:

Иметь практический опыт в:	- анализе сетевой инфраструктуры; выявлении угроз и уязвимости в сетевой инфраструктуре; разработке комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи; использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.
Уметь:	классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; определять оптимальные способы обеспечения информационной безопасности; осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; защищать базы данных при помощи специализированных программных продуктов.
Знать:	принципы построения информационно-коммуникационных сетей; международные стандарты информационной безопасности; акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия; технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия; классификацию угроз сетевой безопасности; методы и способы защиты информации, передаваемой по кабельным направляющим системам; правила проведения возможных проверок согласно нормативным документам Федеральной службы по техническому и экспортному контролю; средства защиты различных операционных систем и среды передачи информации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов – 482 часа, в том числе:

- 122 часа вариативной части, направленных на усиление обязательной части программы профессионального модуля.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ»

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.					Самостоятельная работа[1]
			Обучение по МДК			*Практики*		
			Всего	*В том числе*				
				Лабораторных и практических занятий	Курсовых работ (проектов)	Учебная	Производственная	
ПК 3.1, 3.3 ОК 01-10	**Раздел 1.** Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	**166**	**142**	70	-	-	-	14
ПК 3.1-3.3 ОК 01-10	**Раздел 2.** Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	**164**	**140**	70		-	-	14
ПК 3.1-3.3 ОК 01-10	Учебная практика *(по профилю специальности), часов (концентрированно)*	**72**				72	-	
ПК 3.1-3.3 ОК 01-10	Производственная практика *(по профилю специальности), часов (Концентрированная) практика)*	**72**					72	
	Промежуточная аттестация (экзамен)		8					
	Всего:	**482**	**282**	**140**	**-**	**72**	**72**	**28**

[1]*Самостоятельная работа в рамках образовательной программы планируется образовательной организацией в соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием профессионального модуля.*

2.2. Тематический план и содержание профессионального модуля (ПМ) ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

IV семестр

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов
1	**2**		**3**
Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи			**166**
МДК 03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи			**166**
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание**		**12**
	1	**Проблемы обеспечения безопасности операционных систем**. Полностью контролируемые системы. Частично-контролируемые системы. Windows XP. Windows 7. Windows8. Linux. QNX и другие операционные системы.	2
	2	**Технологии аутентификации** Аутентификация, авторизация и администрирование действий пользователя.	2
	3	**Архитектура подсистемы защиты операционной системы Windows7** Особенности ОС Windows7. Возможности администратора.	2
	4	**Файловые системы** Структура, файлы, права	2
	5	**Загрузка ОС, Технологии виртуализации** BIOS, Виртуализация	2
	6	**Надежное хранение информации** RAID массивы	2
	Практические занятия		**18**
	1-2	Штатные средства защиты Windows	4
	3-4	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя. Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	4

	5-6	Программы надежного удаления информации. Восстановление информации типовыми средствами Программы восстановление информации	4
	7-8	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	4
	9	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация	2
Тема 1.2 Обеспечение безопасности информационных технологий	**Содержание**		**16**
	1	**Разграничение доступа к объектам операционной системы** Модели доступа. Дискреционная модель. Мандатная модель. Роли.	2
	2	**Протоколы сети, домены** IPv4, IPv6, DHCP, DNS	2
	3	**Active Directory** Комплексная система организации управления доступом. Инсталляция. Настройка	2
	4	**Групповые политики безопасности** GPO	2
	5	**Почта** SMTP, POP3, IMAP	2
	6	**Протоколы аутентификации и доступа** LDAP, SAMBA, Kerberos	2
	7	**Функции межсетевых экранов** Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня.	2
	8	**Проблемы информационной безопасности сетей** Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP.	2
	Практические занятия		**18**
	9	Базовая настройка сервера	2
	10-11	Поднятие контроллера домена	4
	12	Создание и настройка роли DHCP на основном контроллере домена	2
	13	Создание и настройка роли DNS на основном контроллере домена	2
	14	Ввод машины в домен	2

	15-16	Добавление дополнительного контроллера домена в существующий домен ActiveDirectory	4
	17	Поднятие и настройка Web-сервера IIS	2
	18	Настройка межсетевого экрана.	2
Тема 1.3 Средства защиты информации от несанкционированного доступа Основы технологии виртуальных защищенных сетей VPN	**Содержание**		**26**
	1, 2	**Проблемы информационной безопасности сетей** Защита информации на физическом и канальном уровне	4
	3, 4	**Проблемы информационной безопасности сетей** Защита информации на сетевом и транспортном уровне IPSec, AH, ESP.	4
	5, 6	**Проблемы информационной безопасности сетей** Защита информации на сеансовом, прикладном и уровне представления Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	4
	7, 8	**Проблемы информационной безопасности сетей** Основные протоколы модели ISO/OSI и стека протоколов TCP/IP. IP, DHCP, DNS, LDAP.	4
	9, 10	**Проблемы информационной безопасности сетей** Основные протоколы модели ISO/OSI и стека протоколов TCP/IP. FTP, HTTP, SMTP.	4
	11, 12	**Концепция построения виртуальных защищенных сетей** Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование.	4
	13	**VPN – решения для построения защищенных сетей** Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация.	2
	Практические занятия		**24**
	19	Работа с локальным хранилищем сертификатов в ОС WINDOWS	2
	20	Установка и настройка ПО eToken PKI Client	2
	21	Настройка ПО eToken PKI Client с помощью групповых политик	2
	22	Развертывание TMS в среде Active Directory	2
	23	Настройка TMS в среде Active Directory. Настройка политик TMS	2
	24	Настройка использования виртуального токена	2
	25	Использование токена на рабочем месте администратора	2
	26	Установка и настройка СКЗИ «КриптоПро CSP»	2
	27	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	2

	28	Применение SecretDisk4. Применение SecretDisk Server NG	2
	29	Изучение основных возможностей ПО VipNet Client Изучение настроек ПОVipNet Client	2
	30	Изучение возможностей ПО Деловая почта	2
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей. Технологии Data Leakage Prevention (DLP).	**Содержание**		**18**
	1	**Защита информации от внутренних угроз информационной безопасности.** Выявление утечек с использованием технологии Data Leakage Prevention (DLP). Теория и практика применения DLP-систем.	**2**
	2	**Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.**	**2**
	3	**Установка DLP IWTM в виртуальном окружении. Режимы port mirroring и proxy.**	**2**
	4	Конфигурирование DLP IWTM Исправление типовых неисправностей.	**2**
	5	**Технологии агентского мониторинга** Назначение агентского мониторинга. Установка и настройка агентского мониторинга. Интерфейс консоли DLP IWDM. Работа в консоли управления агентом	**2**
	6	**Политики агентского мониторинга, особенности их настройки.** Создание и проверка политик. Создание политик защиты на агентах; Фильтрация событий; Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата.	**2**
	7	**Разработка политик безопасности, анализ выявленных инцидентов**	**2**
	8	**Разработка и тестирование политик в системе DLP IWTM.** Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; Работа со сводками, виджетами, сводками; Работа с персонами; Работа с объектами защиты; Провести имитацию процесса утечки конфиденциальной информации в системе; Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. Работа с категориями и терминами; Использование регулярных выражений; Использование морфологического поиска; • Работа с графическими объектами; Работа с выгрузками и баз данных; Работа с печатями и бланками; Работа с файловыми типами;	**2**
	9	**Мониторинг трафика.** Проверка применения политик 4-х видов: трафик, персоны, буфер обмена, движение файлов. Работа с краулером.	**2**

	Практические занятия		**20**
	31-32	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	**4**
	33-34	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	**4**
	35-36	Поиск и предотвращение инцидентов. Технологии анализа сетевого трафика в системе корпоративной защиты информации от внутренних угроз	**4**
	37-38	Технологии агентского мониторинга	**4**
	39-40	Анализ выявленных инцидентов	**4**
Самостоятельная работа при изучении раздела 1 ПМ 03. - Дополнительное конспектирование материала по темам из рекомендуемой преподавателем литературы. - Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации. - Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности. - Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации. **Примерная тематика внеаудиторной самостоятельной работы:** 1. Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре. 2. Практическое применение антивирусных программ для защиты информации от несанкционированного доступа. 3. Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа. 4. Применение различных программ для оперативного и гарантированного восстановления информации на ПК.2 5. Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации. 6. Разработка комплекса организационно-административной защиты от вредоносных программ. 7. Самостоятельная разработка предложений по программно-аппаратной защите информации на определенном объекте. 8. Применение подсистемы безопасности WINDOWS XP/Vista/7 для предотвращения несанкционированного доступа к защищаемой информации.			**14**
Промежуточная аттестация (зачет)			**10**

Раздел 2. **Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи**		**164**
МДК 03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи		**164**
Тема 2.1. Основы информационной безопасности	**Содержание**	**33**
	1. Основные понятия информационной безопасности. Сущность и понятия защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности.	20
	2. Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.	
	3. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	
	4. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.	
	Тематика практических занятий и лабораторных работ	**10**
	1. Требования к безопасности информационных систем	2
	2. Требования к безопасности информационных систем в России	4
	3. Определение требований к защите информации	4
	Самостоятельная работа	**3**
	1. Изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере.	3
Тема 2.2. Организационно-правовые аспекты защиты информации	**Содержание**	**44**
	1. Структура правовой защиты информации. Система документов в области защиты информации.	30
	2. Организационные основы защиты информации. Принципы организационной защиты информации.	
	3. Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации.	
	4. Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности. Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере.	
	Тематика практических занятий и лабораторных работ	**10**
	1. Правовое регулирование в информационной сфере	2

	2. Исследование принципов работы индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	2
	3. Исследование возможностей работы фильтров сетевых помехоподавляющих	2
	4. Исследование работы генератора шума для защиты от ПЭМИН	4
	Самостоятельная работа	**4**
	1. Подготовка презентации по заданной теме с последующим представлением преподавателю в электронном виде.	4
Тема 2.3.Комплексная система защиты информации	**Содержание**	**45**
	1. Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации.	30
	2. Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна.	
	3. Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны. Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.	
	4. Способы и средства обнаружения угроз. Комплексное обследование защищенности информационной системы. Средства нейтрализации угроз.	
	Тематика практических занятий и лабораторных работ	**12**
	1. Исследование уязвимостей и построение модели угроз объекта защиты.	4
	2. Разработка комплексной системы инженерно-технической защиты информации на объекте.	4
	3. Исследование возможностей устройства для защиты объектов информатизации	4
	Самостоятельная работа	**3**
	1. Составление доклада по перспективе и направлению развития комплексных средств защиты информации на основе публикаций в периодической литературе.	3
Тема 2.4. Инженерно-техническая защита информации	**Содержание**	**68**
	1. Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.	44
	2. Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации. Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.	
	3. Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации. Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.	

	4. Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению. Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи. Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания.	
	5. Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок. Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания. Контроль слаботочных цепей. Принципы контроля линий заземления.	
	6. Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации. Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники.	
	Тематика практических занятий и лабораторных работ	**20**
	1. Анализ источников, каналов распространения и каналов утечки информации	2
	2. Измерение параметров ВОСП с помощью системы оценки защищенности оптических линий связи	2
	3. Оценка защищенности оптических линий связи с помощью системы оценки защищенности оптических линий связи	2
	4. Оценка защищённости с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН	4
	5. Исследование возможностей системы оценки защищенности выделенных помещений	2
	6. Измерение уровня виброускорения в ограждающих конструкциях	4
	7. Расчет и оценка защищенности помещения по акустическому каналу	2
	8. Расчет и оценка защищенности помещения по виброакустическому каналу	2
	Самостоятельная работа	**4**
	1. Разработка предложений по инженерно-технической защите информации на определенном объекте.	4
Тема 2.5.Криптографическая защита информации	**Содержание**	**36**
	1. Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	26
	2. Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования. Криптосистемы с открытым ключом. Основы	

	шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	
	3. Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа.	
	Тематика практических занятий и лабораторных работ	**10**
	1. Поиск и локализация скрытых видеокамер	4
	2. Исследование методов защиты сотовых телефонов от несанкционированного прослушивания	4
	3. Создание скрытой информации. Установка паролей.	2
Тема 2.6.Аттестация и лицензирование объектов защиты	**Содержание**	**22**
	1. Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ. Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний.	14
	2. Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании.	
	Тематика практических занятий и лабораторных работ	**8**
	1. Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля	4
	2. Поиск и обнаружение радиоизлучающих средств	4
Промежуточная аттестация (экзамен)		**10**
Самостоятельная работа при изучении раздела 2 ПМ 03.: - изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере; - ознакомление с нормативными документами по ИБ; - изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности; - составление доклада по перспективным направлениям развития средств комплексной защиты информации; - разработка пакета документации по инженерно-технической защите информации на объекте; - изучение возможностей инженерно-технических средств защиты информации; - изучение технических характеристик инженерно-технических средств защиты информации; - разработка предложений по инженерно-технической защите информации на определенном объекте;		**14**
Учебная практика(по профилю специальности) по ПМ 03 **Виды работ:**		**72**

- установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов; - установка и настройка типовых программно-аппаратных средств защиты информации; - использование программно-аппаратных и инженерно-технических средств. - настройка, регулировка и ремонт оборудования средств защиты; - выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой; - проведение типовых операции настройки средств защиты операционных систем; - проведение аттестации объектов защиты; - определение источников несанкционированного доступа, исходя из модели угроз; - определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта; - обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств; - защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК; - защита информации организационными методами в соответствии с инструкциями на объекте.	
Производственная практика (по профилю специальности) по ПМ **Виды работ:** 1. Участие в создании комплексной системы защиты на предприятии. 2. Применение программно-аппаратных средств защиты информации на предприятии 3. Применение инженерно-технических средств защиты информации на предприятии. 4. Применение криптографических средств защиты информации на предприятии.	**72**
Промежуточная аттестация (экзамен)	**8**
Всего	**482**

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие учебной лаборатории программно-аппаратных средств обеспечения информационной безопасности.

Оборудование учебного кабинета и рабочих мест кабинета:
- 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»
- мультимедиапроектор, компьютер преподавателя;

Оборудование лаборатории программно-аппаратных средств обеспечения информационной безопасности:

Технические средства обучения:

- персональные компьютеры (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i5, оперативная память DDR4 объемом не менее 16 Гб; HD 1000 Gb видеокарта, БП 650 Ватт), объединенные в учебную локально-вычислительную сеть с выходом в сеть Интернет, по количеству обучающихся с лицензионным программным обеспечением: ОС Windows 10, Windows Server 2012, ОС Unix;
- система InfoWatch;
- монитор с возможностью поворота экрана не менее 90 градусов, не менее 23,8 дюйма, HDMI, USB;
- криптошлюз ПАК ViPNet Coordinator HW100;
- коммутатор L2 уровень, 16 портов Ethernet стандарта 1000BASE-T;
- маршрутизатор 4 порта Ethernet стандарта 1000BASE-T;
- АПМДЗ Соболь PCI-E.
- 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.;
- паяльная станция – 2 шт.;
- демонтажная станция -1 шт.;
- анализатор поля – 1 шт.;
- измеритель электромагнитного поля – 1 шт.;
- детектор излучений -1 шт.;
- индикатор СВЧ -1шт;
- тестер кабельных линий -1 шт.;
- лабораторные стенды:
- «Изучение системы видеонаблюдения»;
- «Изучение систем контроля доступа»;
-«Изучение беспроводной системы охранно-пожарной сигнализации»;
- «Светочувствительная сигнализация»
- «Микроконтроллерное устройство управления исполнительными блоками для режимных объектов»
- «Микропроцессорное автоматическое устройство управления системой принудительного охлаждения телекоммуникационной стойкой аппаратуры по 4 каналам измерения в реальном масштабе времени»
- «Изучение биометрических систем контроля доступа»
- «Структурированные кабельные системы NIKOMAX»

Реализация программы модуля предполагает обязательную учебную практику.

3.2. Информационное обеспечение обучения
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:
1. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие/ Фороузан Б.А.; пер. с англ. Под ред.А.Н. Берлина. - М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2015.-784с.:ил.,табл.-(Основы информационных технологий).
2. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи/ Под ред. доктора техн. Наук, профессора О.Б. Макаревича. – М.: Горячая линия – Телеком, 2014. -360с.: ил.
3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства –М.: ДМК Пресс, 2016. – 544с.:ил.

4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2016.-272с.:ил.
5. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2017.-528с.-(Профессиональное образование)
6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для вузов -5-е изд., перераб. и доп. – М.: - Горячая линия – Телеком, 2015. – 616с:ил.
7.Романов О.А. Организационное обеспечение информационной безопасности: учебник для студентов высш. учеб. заведений –М.: Издательский центр «Академия», 2015. – 192с.
8. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябов Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2016. – 363 с.
9. InfoWatch Traffic Monitor Руководство пользователя – М.: ЗАО "ИнфоВотч", 2017. – 178 с.: ил..

Дополнительные источники:
1 Руководство администратора Криптон-замок
2. Руководство администратора ППКОП «Астра»
3. Руководство администратора КТМ-256
4. Учебное пособие Структурированная кабельная система NIKOMAX»

Интернет ресурсы:
1. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http:// www.znanium.com/ (2019).
2. http://www.fstec.ru сайт ФСТЭК РФ
3. http://www.ancad.ru сайт компании АНКАД
4. https://www.cryptopro.ru/ сайт компании КриптоПро
5. https://infotecs.ru/ сайт ОАО «ИнфоТеКС»
6. Центр оказания образовательных услуг и подготовки специалистов в области информационной безопасности и эксплуатации средств защиты информации ViPNet. [Электронный ресурс] – режим доступа: https://edu.infotecs.ru/learning/ (2019)

4. .КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ПО РАЗДЕЛАМ)

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.		тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.		тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать	- эффективность выполнения правил ТБ во время учебных занятий, при	

сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	