Воронежский колледж робототехники и компьютерных технологий

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D72D329BBD7B20000000072C4B0002
Владелец: Лукина Виктория Борисовна
Действителен: с 09.04.2021 до 09.04.2022

УТВЕРЖДАЮ
Директор колледжа
_____ Лукина В.Б.
«_____» _____ 2019 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ»

для специальности среднего профессионального образования **11.02.15 "Инфокоммуникационные сети и системы связи"**

Квалификация выпускника: **специалист по обслуживанию телекоммуникаций**

Воронеж
2019

Рабочая программа составлена на основании требований:

— Федерального государственного образовательного стандарта среднего профессионального образования № 1584, утвержденного приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г.;

— учебного плана Воронежского колледжа робототехники и компьютерных технологий по специальности 11.02.15 — "Инфокоммуникационные сети и системы связи", утвержденного Педагогическим советом от 16.12.2019 г. протокол №1

Индекс — 11.02.15 ИТС

Составитель: преподаватель _____ М.О. Маркин

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему общие компетенции и профессиональные компетенции:

1.1.1. 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.

1.1.2. 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.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт:	- выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности; - разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; - осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.
Уметь:	классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей; определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи; осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выполнять тестирование систем с целью определения уровня защищенности; определять оптимальные способы обеспечения информационной безопасности; проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях; проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации; разрабатывать политику безопасности сетевых элементов и логических сетей; выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;

	конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; защищать базы данных при помощи специализированных программных продуктов; защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.
Знать:	принципы построения информационно-коммуникационных сетей; международные стандарты информационной безопасности для проводных и беспроводных сетей; нормативно - правовые и законодательные акты в области 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; способы и методы обнаружения средств съёма информации в радиоканале; классификацию угроз сетевой безопасности; характерные особенности сетевых атак; возможные способы несанкционированного доступа к системам связи; правила проведения возможных проверок согласно нормативных документов ФСТЭК; этапы определения конфиденциальности документов объекта защиты; назначение, классификацию и принципы работы специализированного оборудования; методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2; методы и средства защиты информации в телекоммуникациях от вредоносных программ; технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов; методы и способы защиты информации, передаваемой по кабельным направляющим системам; конфигурации защищаемых сетей; алгоритмы работы тестовых программ; средства защиты различных операционных систем и среды передачи информации;

	способы и методы шифрования (кодирование и декодирование) информации.

1.3. Количество часов, отводимое на освоение профессионального модуля

Всего часов - 523

Из них на освоение МДК- 279,

на практики - 144, в том числе учебную - 36 и производственную - 108

самостоятельная работа – 76.

2. Структура и содержание профессионального модуля

2.1. Структура профессионального модуля

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*		Учебная	Производственная	
				Лабораторных и практических занятий	Курсовых работ (проектов)			
ПК 3.1, 3.3 ОК 01-10	**Раздел 1.** Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	**177**	**151**	66	-	-	-	14
ПК 3.1-3.3 ОК 01-10	**Раздел 2.** Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	**190**	**128**	64		-	-	62

[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.

ПК 3.1-3.3 ОК 01-10	Учебная практика *(по профилю специальности), часов (концентрированно)*	**36**				36	-	
ПК 3.1-3.3 ОК 01-10	Производственная практика *(по профилю специальности), часов (Концентрированная) практика)*	**108**					108	
	Промежуточная аттестация (экзамен)	**12**						
	Всего:	**523**	**279**	**130**	**-**	**36**	**108**	**76**

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	**Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)**	**Объем часов**
1	**2**	**3**
Раздел 1. **Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи**		**177**
МДК 03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		**177**

Тема 1.1.Основы безопасности информационных технологий	**Содержание**	**46**
	1. Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	17
	2. Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.	
	3. Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности	
	4. Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	
	5. Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.	
	6. Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.	
	7. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности.	
	Тематика практических занятий и лабораторных работ	**14**
	1. Сканирование логических дисков с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
	2. Получение списка пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
	3. Создание отчетов на базе СПО ЗИ (например, РЕВИЗОР-1XP)	2
	4. Установка прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2

	5. Считывание прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
	6. Сканирования дерева ресурсов с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
	7. Регистрация пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
	Самостоятельная работа	**4**
	1. Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации.	4
	2. Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.	
Тема 1.2. Обеспечение безопасности информационных технологий	**Содержание**	**60**
	1. Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ.	25
	2. Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации.	
	3. Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты.	
	4. Документы, регламетирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. Правила именования пользователей. Процедур авторизации сотрудников.	
	5. Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация.	
	6. Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем.	
	7. Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов.	

	8. Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы. Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы.	
	9. Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации.	
	10. Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции.	
	Тематика практических занятий и лабораторных работ	**20**
	1. Установка и снятие СЗИ с помощью программы СЗИ НСД (например, Страж NT)	2
	2. Исследование программной среды с помощью СЗИ НСД (например, Страж NT)	2
	3. Исследование возможностей управления пользователями с помощью СЗИ НСД (например, Страж NT)	2
	4. Исследование учета пользователей и контроля устройств с помощью СЗИ НСД (например, Страж NT)	2
	5. Исследование избирательного управления с помощью СЗИ НСД (например, Страж NT)	2
	6. Исследование сортировки и поиска с помощью СЗИ НСД (например, Страж NT)	2
	7. Исследование возможности редактирования пользователей с помощью СЗИ НСД (например, Страж NT)	2
	8. Исследование изменения настроек СЗИ с помощью СЗИ НСД (например, Страж NT)	2
	9. Исследование механизма защиты съемных носителей с помощью СЗИ НСД (например, Страж NT)	2
	10. Исследование настройки маркировки документов с помощью СЗИ НСД (например, Страж NT)	2
	Самостоятельная работа	**8**
	1. Дополнительное конспектирование материала по темам из рекомендуемой преподавателем литературы.	8
	2. Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.	

Тема 1.3. Средства защиты информации от несанкционированного доступа	**Содержание**	**48**
	1. Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов.	22
	2. Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к средствам защиты информации.	
	3. Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, DALLASLOCK)	
	4. Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть».)	
	5. Назначение и особенности применения СЗИ НСД (например, «Страж NT»)	
	6. Назначение и специфика применения комплекса ЗИ (например, «Соболь»)	
	7. Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей.	
	8. Назначение и функциональные возможности eToken и Рутокен. Алгоритм генерации одноразовых паролей. Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи-Хеллмана.	
	9. Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа. Полномочное разграничение доступа. Регистрация событий, имеющих отношение к безопасности	
	Тематика практических занятий и лабораторных работ	**18**
	1. Ввод информации в САПР СЗИ (например, «Гроза-К»)	2
	2. Расчет радиуса контролируемой зоны с помощью САПР СЗИ (например, «Гроза-К»)	2
	3. Исследование защищенности с помощью САПР СЗИ (например, «Гроза-К»)	2
	4. Формирование и вывод проекта протокола в САПР СЗИ (например, «Гроза-К»)	2
	5. Исследование плана тестирования при помощи СПО ЗИ (например, «Ревизор-2XP»)	2
	6. Исследование режима тестирования при помощи СПО ЗИ (например, «Ревизор-2XP»)	2
	7. Исследование содержимого текущего диска с помощью СПО ЗИ (например, «Terrier»)	2
	8. Исследование механизма доступа в систему с использованием СПО ЗИ и УП	2

	(например, «SecretNet»)	
	9. Исследование механизма разграничения доступа с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	Самостоятельная работа	**2**
	1. Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации.	2
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей	**Содержание**	**24**
	1. Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уязвимости и их классификация.	15
	2. Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов.	
	3. Анализ содержимого почтового и WEB-трафика. HTTP-трафик.	
	4. Виртуальные частные сети. Решение на базе ОС Windows 2003. VPN на основе криптошлюза (например, «Континент-К»)	
	5. Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности.	
	6. Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.	
	Тематика практических занятий и лабораторных работ	**9**
	1. Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	2. Исследование функции отслеживания событий НСД с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	3. Исследование возможности обновления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	4. Исследование порядка удаления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	5. Исследование проблемных ситуаций с использованием СПО ЗИ и УП (например,	1

	«SecretNet»)	
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. 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**
Раздел 2. **Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи**		**190**
МДК 03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи		**190**
Тема 2.1. Основы информационной	**Содержание**	**30**
	1. Основные понятия информационной безопасности. Сущность и понятия защиты	12

безопасности	информации.	
	2. Значение информационной безопасности и ее место в системе национальной безопасности.	
	3. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	
	4. Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.	
	5. Состояние информационной безопасности РФ и основные задачи по ее обеспечению.	
	6. Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.	
	Тематика практических занятий и лабораторных работ	**9**
	1. Исследование возможностей профессионального нелинейного радиолокатора (например, NR-900EMS)	2
	2. Исследование возможностей многофункционального поискового прибора (например, ST 033P Пиранья)	2
	3. Исследование возможностей анализатора спектра (например, OSCORGreen-8)	2
	4. Исследование возможностей имитатора источника радиосигналов с различными видами модуляции (например, АВРОРА-3)	2
	5. Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга (например, КРОНА-ПРО)	1
	Самостоятельная работа	**9**
	1. Изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере.	9
	2. Ознакомление с нормативными документами.	
Тема 2.2. Организационно-правовые аспекты защиты информации	**Содержание**	**22**
	1. Структура правовой защиты информации. Система документов в области защиты информации.	10
	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.	
	5. Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере.	
	Тематика практических занятий и лабораторных работ	**7**
	1. Исследование возможностей скоростного приемника сигналов (например, СКОРПИОН-XL)	2
	2. Исследование принципов работы индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	2
	3. Исследование возможностей работы фильтров сетевых помехоподавляющих (например, ЛФС-10-1Ф и ФСП-1Ф-10А)	2
	4. Исследование работы генератора шума для защиты от ПЭМИН (например, ЛГШ-501)	1
	Самостоятельная работа	**5**
	1. Подготовка презентации по заданной теме с последующим представлением преподавателю в электронном виде.	5
Тема 2.3.Комплексная система защиты информации	**Содержание**	**26**
	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.	10
	2. Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна.	
	3. Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.	
	4. Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.	
	5. Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.	

	Тематика практических занятий и лабораторных работ	**7**
	1. Исследование уязвимостей и построение модели угроз объекта защиты.	1
	2. Разработка комплексной системы инженерно-технической защиты информации на объекте.	2
	3. Исследование возможностей устройства для защиты объектов информатизации (например, СОНАТА-Р2, САЛЮТ 2000Б)	2
	4. Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств (например, ПРОКРУСТ-2000)	2
	Самостоятельная работа	**9**
	1. Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности.	9
	2. Составление доклада по перспективе и направлению развития комплексных средств защиты информации на основе публикаций в периодической литературе.	
Тема 2.4. Инженерно-техническая защита информации	**Содержание**	**67**
	1. Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.	26
	2. Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации.	
	3. Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации.	
	4. Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.	
	5. Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.	
	6. Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению.	
	7. Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи.	
	8. Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания.	

	9. Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок.	
	10. Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания.	
	11. Контроль слаботочных цепей. Принципы контроля линий заземления.	
	12. Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации.	
	13. Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники.	
	Тематика практических занятий и лабораторных работ	**20**
	1. Исследование возможностей автоматизированной системы изменений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ)	2
	2. Исследование технических средств и отходящих от них линий с помощью системы измерений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ)	2
	3. Исследование возможностей системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ)	2
	4. Измерение параметров ВОСП с помощью системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ)	1
	5. Оценка защищенности оптических линий связи с помощью системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ)	2
	6. Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН (например, СИГУРД-М19)	2
	7. Оценка защищённости с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН (например, СИГУРД-М19)	1
	8. Измерение параметров ПЭМИН и расчет показателей защищенности технического средства (например, с помощью комплекса СИГУРД-М19)	1
	9. Исследование возможностей системы оценки защищенности выделенных помещений (например, ШЕПОТ)	1

	10. Измерение уровня звукового давления вблизи и на удалении от источника с помощью комплекса оценки защищенности выделенных помещений (например, ШЕПОТ)	1
	11. Измерение уровня виброускорения в ограждающих конструкциях (например, с помощью комплекса ШЕПОТ)	1
	12. Расчет и оценка защищенности помещения по акустическому каналу (например, с помощью комплекса ШЕПОТ)	2
	13. Расчет и оценка защищенности помещения по виброакустическому каналу (например, с помощью комплекса ШЕПОТ)	2
	Самостоятельная работа	**21**
	1. Разработка пакета документации по инженерно-технической защите информации на объекте.	21
	2. Изучение возможностей инженерно-технических средств защиты информации.	
	3. Изучение технических характеристик инженерно-технических средств защиты информации.	
	4. Разработка предложений по инженерно-технической защите информации на определенном объекте.	
	5. Составление доклада по перспективе и направлению развития инженерно-технических средств защиты информации на основе публикаций в периодической специализированной аппаратуре.	
Тема 2.5.Криптографическая защита информации	**Содержание**	**28**
	1. Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	8
	2. Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования	
	3. Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	
	4. 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	**11**
	1. Поиск и локализация скрытых видеокамер (например, с помощью прибора ОПТИК-2)	1
	2. Исследование методов защиты сотовых телефонов от несанкционированного прослушивания (например с помощью изделия Ладья-ИВТ)	2
	3. Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов (например, с помощью устройства КЕДР-1М)	2
	4. Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора (например, с помощью NR-900EMS)	2
	5. Поиск устройств негласного съема информации с помощью многофункционального поискового прибора (например, с помощью ST 033P Пиранья)	2
	6. Оценка защищенности помещения с помощью многофункционального поискового прибора (например, ST 033P Пиранья)	2
	Самостоятельная работа	**12**
	1. Разработка предложений по комплексу технических мероприятий по защите линий связи объекта.	12
	2. Разработка предложений по защите информации от несанкционированного доступа по акустическому каналу в помещении.	
Тема 2.6.Аттестация и лицензирование объектов защиты	**Содержание**	**6**
	1. Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ.	6
	2. Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний.	
	3. 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	**6**
	1. Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	2

	2. Исследование работы генератора шума по сети электропитания и линиям заземления (например, ЛГШ-221)	2
	3. Поиск и обнаружение радиоизлучающих средств (например, с помощью комплекса КРОНА-ПРО)	2
	Самостоятельная работа	**6**
	1. Составление списка уязвимостей предложенного объекта. Самостоятельная разработка комплекта документации на объекте информатизации.	6
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;		**62**
Учебная практика (по профилю специальности) по ПМ 03 **Виды работ:** - 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;		**36**

- 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.	**108**
Промежуточная аттестация (экзамен)	**12**
Всего	**523**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:
Кабинет «Компьютерного моделирования», оснащенный оборудованием:

- компьютеры в комплекте (системный блок, монитор, клавиатура, манипулятор «мышь») или ноутбуки (моноблоки),
- локальная сеть с выходом в Интернет,
- комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном)
- программное обеспечение (системы электротехнического моделирования).
-

Лаборатории «Информационной безопасности телекоммуникационных систем», «Телекоммуникационных систем», оснащенные в соответствии с п. 6.2.1. Примерной программы по специальности 11.02.15.

Оснащенные базы практики, в соответствии с п 6.2.3 Примерной программы по специальности 11.02.15.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1. Партыка Т.Л. Вычислительная техника : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 3-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 445 с. : ил. — (Среднее профессиональное образование). ISBN: 978-5-91134-646-1

2.. Арутюнов, В. В. Защита информации : учебно-методическое пособие / В. В. Арутюнов. - Москва : Либерея-Бибинформ, 2008. - 55, [1] с. : рис. ; 21 см. - (Библиотекарь и время. XXI век ; № 99). - ISBN 5-85129-175-3

4. Васильков А. В., Васильков А. А., Васильков И. А. Информационные системы и их безопасность: Учебное пособие. - М.: Форум, 2015. - 528 с.: 60х90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-289-0

5. **Мельников, В.П.** Информационная безопасность [Текст] : учебное пособие для студентов образовательных учреждений среднего профессионального образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 7-е изд., стер. - Москва : Академия, 2013. - 331, [1] с. : ил., табл.; - (Среднее профессиональное образование. Информатика и вычислительная техника).; ISBN 978-5-7695-9954-5
6.Эксплуатация объектов сетевой инфраструктуры: учебник/А.В.Назаров.-М.: Академия, 2014.- 368с. ISBN 978-5-44680347-7

3.2.3Дополнительные источники

Научно-технические и реферативные журналы:

1. Электросвязь
2. Вестник связи
3. Сети и системы связи
4. Мобильные системы
5. Цифровая обработка сигналов
6. Сводный реферативный журнал "Связь".

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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	классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно; анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный; возможные сетевые атаки и способы несанкционированного доступа в конвергентных	тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач,

	системах связи определены верно; мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме; недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме, тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно;	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.	для обеспечения информационной безопасности выбраны оптимальные способы; выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях;	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	мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации	тестирование, экзамен, экспертное наблюдение выполнения

сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	являются оптимальными и достаточными; политика безопасности сетевых элементов и логических сетей разработана в полном объеме; расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами; установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами; конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами; базы данных максимально защищены при помощи специализированных программных продуктов; ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами;	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	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и	Интерпретация результатов наблюдений за деятельностью обучающегося в

различным контекстам.	самооценка эффективности и качества выполнения профессиональных задач	процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен
ОП 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	

сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	правил ТБ во время учебных занятий, при 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.	

ПРИЛОЖЕНИЕ 1

Воронежский колледж робототехники и компьютерных технологий

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D72D329BBD7B20000000072C4B0002
Владелец: Лукина Виктория Борисовна
Действителен: с 09.04.2021 до 09.04.2022

УТВЕРЖДАЮ

Директор колледжа

_____ Лукина В.Б.

«_____» _____ 2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

дисциплины

«ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ»

для специальности среднего профессионального образования

11.02.15 "Инфокоммуникационные сети и системы связи"

Квалификация выпускника: **специалист по обслуживанию телекоммуникаций**

Воронеж
2019

Цель фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи». Перечень видов оценочных средств соответствует Рабочей программе дисциплины.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля в форме индивидуальных заданий при выполнении цикла лабораторных работ и промежуточной аттестации в форме вопросов и заданий (могут быть заданы как в форме билета, так и экзаменационного теста) к экзамену.

Структура и содержание заданий - задания разработаны в соответствии с рабочей программой дисциплины «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи».

1. Паспорт фонда оценочных средств

Результатом освоения учебной дисциплины являются предусмотренные ФГОС по специальности умения и знания, направленные на формирование общих и профессиональных компетенций.

Таблица 1

№ п/п	Код компетенции	Содержание компетенции	Планируемые результаты обучения	Наименование оценочного средства
1	ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий **Знания:** актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач	**Задание** на выполнение индивидуального варианта лабораторной работы
2	ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска **Знания:** номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации	**Задание** на выполнение индивидуального варианта лабораторной работы
3	ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования **Знания:** содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования	**Задание** на выполнение индивидуального варианта лабораторной работы

4	ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности **Знания:** психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы
5	ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе **Знания:** особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.	**Задание** на выполнение индивидуального варианта лабораторной работы
6	ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	**Умения:** описывать значимость своей специальности **Знания:** сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности	**Задание** на выполнение индивидуального варианта лабораторной работы
7	ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности **Знания:** правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения	**Задание** на выполнение индивидуального варианта лабораторной работы
8	ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	**Умения:** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности **Знания:** роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения	**Задание** на выполнение индивидуального варианта лабораторной работы
9	ОК 09	Использовать информационные технологии в профессиональной деятельности.	**Умения:** применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение **Знания:** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы

10	ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	**Задание** на выполнение индивидуального варианта лабораторной работы
			Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности	
11	ПК 3.1.	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.	**Умения:** - классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; - проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей; - определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи; - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты - выполнять тестирование систем с целью определения уровня защищенности.	**Задание** на выполнение индивидуального варианта лабораторной работы
			Знания: - принципы построения информационно-коммуникационных сетей; - международные стандарты информационной безопасности для проводных и беспроводных сетей; - нормативно - правовые и законодательные акты в области 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; - способы и методы обнаружения средств съёма информации в радиоканале; - классификацию угроз сетевой безопасности;	

			- характерные особенности сетевых атак; - возможные способы несанкционированного доступа к системам связи.	
12	ПК 3.2.	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.	**Умения:** - определять оптимальные способы обеспечения информационной безопасности; - проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях	**Задание** на выполнение индивидуального варианта лабораторной работы
			Знания: - правила проведения возможных проверок согласно нормативных документов ФСТЭК; - этапы определения конфиденциальности документов объекта защиты; назначение, классификацию и принципы работы специализированного оборудования; - методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP. WPA и WPA 2; - методы и средства защиты информации в телекоммуникациях от вредоносных программ; - технологии применения программных продуктов; - возможные способы, места установки и настройки программных продуктов	
13	ПК 3.3.	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	**Умения:** - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации; - разрабатывать политику безопасности сетевых элементов и логических сетей; - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи; - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; - защищать базы данных при помощи специализированных программных продуктов; - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.	**Задание** на выполнение индивидуального варианта лабораторной работы
			Знания: - методы и способы защиты информации, передаваемой по кабельным направляющим системам; конфигурации защищаемых сетей; - алгоритмы работы тестовых программ; - средства защиты различных операционных систем и среды передачи информации;	

			- способы и методы шифрования (кодирование и декодирование) информации.	

Формой промежуточной аттестации по учебной дисциплине является

экзамен

указать форму аттестации, предусмотренную учебным планом

2. Формы контроля и оценивания элементов учебной дисциплины

В результате текущей аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих и профессиональных компетенций.

Таблица 2

Раздел / тема дисциплины	**Проверяемые У, З, ОК, ПК**	**Форма текущего контроля и оценивания**
Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	ОК 01 - 10 ПК 3.1, 3.3	Самостоятельная работа
Тема 1.1. Основы безопасности информационных технологий	ОК 01 - 10 ПК 3.1, 3.3	Практическое занятие №№ 1-7
Тема 1.2. Обеспечение безопасности информационных технологий	ОК 01 - 10 ПК 3.1, 3.3	Практическое занятие №№ 8-18

Тема 1.3. Средства защиты информации от несанкционированного доступа	ОК 01 - 10 ПК 3.1, 3.3	Практическое занятие №№ 18-27
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей	ОК 01 - 10 ПК 3.1, 3.3	Практическое занятие №№ 27-32
Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	ОК 01 - 10 ПК 3.1-3.3	Самостоятельная работа
Тема 2.1. Основы информационной	ОК 01 - 10 ПК 3.1, 3.3	Практическое занятие №№ 1-5
Тема 2.2. Организационно-правовые аспекты защиты информации	ОК 01 - 10 ПК 3.1- 3.3	Практическое занятие №№ 6-9

Тема 2.3. Комплексная система защиты информации	ОК 01 - 10 ПК 3.1- 3.3	Практическое занятие №№ 10-14
Тема 2.4. Инженерно-техническая защита информации	ОК 01 - 10 ПК 3.1, 3.3	Практическое занятие №№ 15-28
Тема 2.5. Криптографическая защита информации	ОК 01 - 10 ПК 3.1, 3.3	Практическое занятие №№ 29-35
Тема 2.6. Аттестация и лицензирование объектов защиты	ОК 01 - 10 ПК 3.1, 3.3	Практическое занятие №№ 36-39

3. Оценка освоения учебной дисциплины

4. Контрольно-оценочные материалы для промежуточной аттестации по учебной дисциплине

Оценка освоения дисциплины предусматривает проведение экзамена

указать форму аттестации, предусмотренную учебным планом

4.1. Вопросы (задания) к экзамену по дисциплине:

1. Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.

2. Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.
3. Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности.
4. Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
5. Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация.
6. Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.
7. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности.
8. Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ.
9. Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации.
10. Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты.
11. Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация.
12. Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем.
13. Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов.
14. Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы. Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы.

15. Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации.
16. Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции.
17. Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов.
18. Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к средствам защиты информации.
19. Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, DALLASLOCK).
20. Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть».)
21. Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей.

5. Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Индикаторы компетенции	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**отлично**
Полнота знаний	Уровень знаний ниже минимальных требований. Лабораторные работы выполнены не в полном объеме	Минимально допустимый уровень знаний. Лабораторные работы выполнены в полном объеме	Уровень знаний в объеме, соответствующем программе подготовки. Лабораторные работы выполнены в полном объеме	Уровень знаний в объеме, соответствующем программе подготовки, лабораторные работы выполнены в полном объеме
Наличие умений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи. Индивидуальные задачи решены по типовому шаблону.	Продемонстрированы все основные умения. Решены типовые задачи. Выполнены индивидуальные задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи, выполнены все индивидуальные задания в полном объеме.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач.	Сформированность компетенции в целом соответствует требованиям, но есть недочеты. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по некоторым профессиональным задачам.	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий	Ниже среднего	Средний	Высокий