Приложение к рабочей программе
по профессиональному модулю
ПМ.03 Обеспечение информационной
безопасности инфокоммуникационных
сетей и систем связи

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«01» 06 2022 г.

Оценочные средства текущего контроля и промежуточной аттестации
по профессиональному модулю

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

для специальности:
11.02.15 Инфокоммуникационные сети и системы связи

Квалификация: специалист по обслуживанию
телекоммуникаций

Екатеринбург
2022

Приложение к рабочей программе
по профессиональному модулю
ПМ.03 Обеспечение информационной
безопасности инфокоммуникационных
сетей и систем связи

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«___» _____ 2022 г.

Оценочные средства текущего контроля и промежуточной аттестации
по профессиональному модулю

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

для специальности:
11.02.15 Инфокоммуникационные сети и системы связи

Квалификация: специалист по обслуживанию
телекоммуникаций

Екатеринбург
2022

Оценочные средства составил:
Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС,

Одобрено цикловой комиссией
Многоканальных
телекоммуникационных систем
кафедры Многоканальной
электрической связи.
Протокол 10 от 31.05.2022
Председатель цикловой комиссии
_____ Е.Б. Пермяков

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

Оценочные средства составил:
Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС,

Одобрено цикловой комиссией
Многоканальных
телекоммуникационных систем
кафедры Многоканальной
электрической связи.
Протокол ___ от _____
Председатель цикловой комиссии
_____ Е.Б. Пермяков

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

1 Общие положения

Комплект оценочных средств предназначен для проверки результатов освоения профессионального модуля основной образовательной программы среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи в части овладения основным видом деятельности ВД 3 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи».

Форма аттестации по профессиональному модулю - экзамен. Итогом экзамена является однозначное решение: «Вид профессиональной деятельности освоен/не освоен».

Экзамен предусматривает выполнение практических заданий.

2 Формы контроля и оценивания элементов профессионального модуля

Таблица 1

Элемент модуля	Форма контроля и оценивания	
	Промежуточная аттестация	Текущий контроль
МДК.03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях электросвязи	Дифференцированный зачет	- проверка отчетов по практическим занятиям; - проверка выполнения самостоятельных работ; - проверка теоретических знаний по междисциплинарному курсу в форме тестирования.
МДК.03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях электросвязи	Дифференцированный зачет	- проверка отчетов по практическим занятиям; - проверка выполнения самостоятельных работ; - проверка теоретических знаний по междисциплинарному курсу в форме тестирования.
УП.03.01 Учебная практика	Дифференцированный зачет	Наблюдения во время выполнения заданий.
ПП.03.01 Производственная практика	Комплексный дифференцированный зачет	Наблюдения во время выполнения заданий.
ПМ.03.ЭК Экзамен по модулю	Экзамен	Наблюдения во время выполнения заданий.

Перечень зачетных тем по всем МДК

Таблица 2

Название МДК	Зачетные темы МДК	Форма контроля
МДК.03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях электросвязи.	Тема 1 Основы безопасности информационных технологий.	Защита практических работ, проверка конспекта.
	Тема 2 Обеспечение безопасности информационных технологий.	Защита практических работ, проверка конспекта.
	Тема 3 Средства защиты информации от несанкционированного доступа.	Защита практических работ, проверка конспекта.
	Тема 4 Обеспечение безопасности компьютерных систем и сетей.	Защита практических работ, проверка конспекта.
МДК.03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных систе-	Тема 1 Основы информационной безопасности	Защита практических работ, проверка конспекта.
	Тема 2 Организационно-правовые аспекты защиты информации.	Защита практических работ, проверка конспекта.

мах и сетях электросвязи.	Тема 3 Комплексная система защиты информации.	Защита практических работ, проверка конспекта.
	Тема 4 Инженерно-техническая защита информации.	Защита практических работ, проверка конспекта.
	Тема 5 Криптографическая защита информации.	Защита практических работ, проверка конспекта.
	Тема 6 Аттестация и лицензирование объектов защиты.	Защита практических работ, проверка конспекта.

3 Результаты освоения модуля, подлежащие проверке на экзамене

В результате аттестации по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций (Таблица 3):

Таблица 3

Код ПК, ОК	Профессиональные и общие компетенции, которые возможно сгруппировать для проверки	Показатели оценки результата
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.	**Практический опыт:** - анализировать сетевую инфраструктуру; - выявлять угрозы и уязвимости в сетевой инфраструктуре. **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. **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.
ПК 3.2	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.	**Практический опыт:** - 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. **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.
ПК 3.3	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	**Практический опыт:** - осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи; - использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи. **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. **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.
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 (самостоятельно или с помощью наставника). **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 профессиональной деятельности.
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.
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.
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.
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.
ОК 06	Проявлять гражданско- патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	**Умения**: описывать значимость своей специальности. **Знания**: сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности.
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.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подго-	**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 специально-

	товленности.	сти. **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.
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.
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. **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.

4 Комплект материалов для оценки сформированности общих и профессиональных компетенций по основному виду деятельности

В состав комплекта оценочных средств входят задания для экзаменующихся и критерии оценки выполненных заданий.

4.1 Задания для экзаменующихся

Количество вариантов - 10.

Оцениваемые компетенции: ПК 3.1 - ПК 3.3, ОК 01 - ОК 10.

Условия выполнения задания: учебная лаборатория.

Вариант 1

Задание 1

Выполнить расчеты для определения класса информационной системы передачи данных (ИСПДн).

Инструкция:

1) Выбрать населенный пункт (поселение) - Город Курган областной.

2) Используя ресурсы поисковой системы определить численность населения.

3) Определить объем данных, основываясь на численности населения.

4) Определить класс ИСПДн.

5) Выбрать средства защиты персональных данных (ПДн).

Перечень раздаточных и дополнительных материалов:

1) Классификация информационных систем персональных данных (ИСПДн).

2) *http://weta.ru/kalkulyator_klassa_ispdn.php*.

3) *https://www.yandex.ru/*

Задание 2

Настроить параметры локальной политики безопасности операционной системы *Windows* 7 (*XP*).

Инструкция:

1) Активизировать и настроить панель управления операционной системы *Windows* 7/*XP*.

2) Настроить политику паролей.

3) Настроить политику блокировки учетной записи.

4) Изменить пароль своей учетной записи.

Перечень раздаточных и дополнительных материалов:

1) Настройка параметров аутентификации *Windows* 7 (*XP*).

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный //

Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 2

Задание 1

Разработать комплекс мероприятий на получение лицензии на определенный вид деятельности в области информационной безопасности.

Вид деятельности: Разработка и (или) производство средств защиты конфиденциальной информации (в пределах компетенции ФСБ).

Инструкция:

1) Использовать раздаточный материал.

2) Определить нормативные и правовые документы для лицензированного вида деятельности.

3) Определить степень секретности и виды конфиденциальной информации.

Перечень раздаточных и дополнительных материалов:

1) Виды деятельности, при которых необходима лицензия ФСБ.

2) Перечень документов для получения лицензии на деятельность по технической защите конфиденциальной информации.

3) Лицензирование деятельности по технической защите конфиденциальной информации.

4) *https://www.yandex.ru*/

5) *http://www.consultant.ru*/

Задание 2

1) Создать учетную запись пользователя.

2) Создать локальную группу пользователей.

3) Выполнить временную блокировку учетной записи.

Инструкция:

1) Создать учетную запись пользователя, локальную группу пользователей, используя раздаточный и дополнительный материал.

2) Изменить состав пользователей в локальной группе, используя раздаточный и дополнительный материал.

3) Выполнить временную блокировку учетной записи, используя раздаточный и дополнительный материал.

4) Записать в отчет последовательность команд (операций).

Перечень раздаточных и дополнительных материалов:

1) Назначение прав пользователей при произвольном управлении доступом.

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 3

Задание 1

Разработать комплекс мероприятий на получение лицензии на определенный вид деятельности в области информационной безопасности.

Вид деятельности: Деятельность по технической защите конфиденциальной информации. Разработка и (или) производство средств защиты конфиденциальной информации.

Инструкция:

1) Использовать раздаточный материал.

2) Определить нормативные и правовые документы для лицензированного вида деятельности.

3) Определить степень секретности и виды конфиденциальной информации.

Перечень раздаточных и дополнительных материалов:

1) Виды деятельности, при которых необходима лицензия ФСБ.

2) Перечень документов для получения лицензии на деятельность по технической защите конфиденциальной информации.

3) Лицензирование деятельности по технической защите конфиденциальной информации.

4) *https://www.yandex.ru/*

Задание 2

Разработать систему видеонаблюдения, входящую в комплексную систему информационной безопасности.

Объект: Периметр одноэтажного здания.

Инструкция:

1) Составить описание и техническое задание на установку системы видеонаблюдения.

2) Составить план размещения видеокамер.

3) Выбрать видеооборудование по техническим характеристикам с учетом особенностей объекта контроля.

4) Составить схему подключения оборудования.

Перечень раздаточных и дополнительных материалов:

1) Принцип построения систем видеонаблюдения.

2) Проектирование системы видеонаблюдения.

3) Видеокамеры *Arman*.

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 4

Задание 1

Разработать комплекс необходимых мероприятий по защите информации.

Объект: Помещение с компьютерным оборудованием (классом).

Инструкция:

1) Использовать перечень раздаточных и дополнительных материалов для составления технического задания на аттестацию объекта.

2) Выполнить последовательность действий для получения аттестата соответствия.

3) Составить отчетную документацию в виде протокола аттестационных испытаний (аттестата соответствия).

Перечень раздаточных и дополнительных материалов:

1) Положение об аттестации.

2) Техническое задание на аттестацию.

3) *https://www.yandex.ru/*

Задание 2

1) Выполнить установку антивирусного сервера и антивирусной консоли.

2) Выполнить установку антивирусного агента на компьютер.

Инструкция:

1) Установить антивирусный сервер и антивирусную консоль.

2) Установить антивирусный агент на компьютер.

3) Выполнить удаление отдельных компонентов комплекса.

Перечень раздаточных и дополнительных материалов:

1) Установка программного антивирусного комплекса *Dr WEB.*

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 5

Задание 1

Составить техническое задание на аттестацию помещения. Разработать комплекс необходимой документации по защите информационной защите помещений.

Объект: Жилое помещение – квартиры, коттеджи.

Инструкция:

1) Пояснить методику составления технического задания на аттестацию помещения, используя раздаточный и дополнительный материал.

2) Выполнить последовательность действий для получения аттестата соответствия.

3) Составить отчетную документацию в виде протокола аттестационных испытаний (аттестата соответствия).

Перечень раздаточных и дополнительных материалов:

1) Аттестация защищаемых помещений.

2) Положение об аттестации Р_1994.11.25.

3) Требования к помещениям.

4) *https://www.yandex.ru/*

Задание 2

1) Установить на компьютер антивирусную программу *KFA*16.0.1.445 *ru* в стандартном режиме.

2) Установить на компьютер антивирусную программу *KFA*16.0.1.445ru из командной строки.

3) Выполнить выборочную проверку файлов/папок антивирусной программой *KFA*.

Инструкция:

1) Изучить функциональные возможности антивирусной программы *KFA*, используя раздаточный и дополнительный материал.

2) Выполнить пошаговую установку антивирусной программы.

3) Выполнить установку антивирусной программы из командной строки.

Перечень раздаточных и дополнительных материалов:

1) Описание антивирусной программы *Kaspersky Free Anti-Virus*.

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 6

Задание 1

Провести аудит информационной системы предприятия.

Объект: Отдел материально-технического обеспечения организации.

Инструкция:

1) Пояснить методику проведения анализа информационных ресурсов в организации, используя раздаточный и дополнительный материал.

2) Определить основные угрозы безопасности и их источники.

3) Сформировать неформальную модель возможных нарушителей и составить план мероприятий по нейтрализации угроз.

Перечень раздаточных и дополнительных материалов:

1) Модель системы информационной безопасности (ИБ) на предприятии.

2) Мероприятия по защите автоматизированных систем (АС).

3) *https://www.yandex.ru/*

Задание 2

1) Настроить межсетевой экран операционной системы *Windows* 7 (*XP*).

2) Установить межсетевой экран (*Firewall*) *Comodo Firewall* на компьютер.

Инструкция:

1) Активизировать и настроить встроенный брандмауэр операционной системы *Windows* 7 *XP*, используя раздаточный и дополнительный материал.

2) Установить и настроить межсетевой экран *Comodo Firewall*, используя раздаточный и дополнительный материал.

Перечень раздаточных и дополнительных материалов:

1) Активизизация встроенного брандмауэра операционной системы *Windows* 7 *XP* и настройка его параметров.

2) Установка и настройка межсетевого экрана *Comodo Firewall*.

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 7

Задание 1

Провести аудит программно-технических средств организации. Выполнить анализ и определить основные угрозы. Разработать модель системы информационной безопасности.

Объект: Отдел материально-технического обеспечения организации.

Инструкция:

1) Определить основные угрозы безопасности и их источники.

2) Составить неформальную модель возможных нарушителей.

3) Разработать план мероприятий по формированию режима безопасности информации в организации.

Перечень раздаточных и дополнительных материалов:

1) Программные и технические средства.

2) Программные и технические методы защиты.

3) *https://www.yandex.ru/*

Задание 2

1) Выполнить шифрование исходного текста из таблицы 1 методом перестановки.

2) Выполнить шифрование исходного текста из таблицы 3 методом гаммирования.

Инструкция:

1) Записать исходные данные для шифрования, используя раздаточный и дополнительный материал.

2) Изучить задания к выполнению работы.

3) Выполнить задания, используя раздаточный и дополнительный материал.

Перечень раздаточных и дополнительных материалов:

1) Таблица 1 – Исходные данные в виде открытого текста.

2) Таблица 2 – Открытый ключ.

3) Таблица 3 – Открытый текст для преобразования гаммированием.

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 8

Задание 1

Провести аудит программно-технических средств предприятия. Выполнить анализ и разработать модель угроз. Разработать политику системы информационной безопасности.

Объект: Больницы, поликлиники, амбулатории, диспансеры.

Инструкция:

1) Изучить порядок проведения анализа программно-технических ресурсов предприятия, используя раздаточный и дополнительный материал.

2) Определить состав программно-технического оборудования и возможные основные угрозы безопасности.

3) Сформулировать рекомендации и план мероприятий по нейтрализации угроз.

4) Описание политики безопасности предприятия.

Перечень раздаточных и дополнительных материалов:

1) Безопасность предприятия.

2) Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи._Политики информационной безопасности.

3) *https://www.yandex.ru/*

Задание 2

1) Выполнить шифрование/расшифрование системой *EFS*.

2) Сгенерировать ключи шифрования (открытый и закрытый) и поместить их в сертификат для экспорта.

Инструкция:

1) Изучить основные сведения о шифрующей системе *EFS,* , используя раздаточный и дополнительный материал.

2) Выбрать файл (папку с файлами) для шифрования.

3) Выполнить шифрование выбранных файлов, используя команды и диалоговые окна.

4) Выполнить расшифрование, используя диалоговые окна и соответствующие команды.

5) Получить сертификат для экспорта ключей для расшифрования данных на другом компьютере.

Перечень раздаточных и дополнительных материалов:

1) Основные сведения о *EFS*.

2) Шифрование файлов.

3) Сертификаты.

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 9

Задание 1

Определить текущее состояние помещения с точки зрения технической защищенности объекта информатизации. Составить поэтапный план мероприятий по защите информации: 1) подготовительный, предпроектный; 2) проектирование системы технической защиты информации; 3) этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации.

Объект: Архив организации.

Инструкция:

1) Изучить порядок проведения анализа, используя раздаточный и дополнительный материал.

2) Провести обследование защищаемых объектов, определить категорию помещения, как объекта защиты.

3) Разработать аналитическое обоснование необходимости создания системы технической защиты информации и техническое задание на ее создание.

Перечень раздаточных и дополнительных материалов:

1) Анализ защищаемых помещений и каналов утечки.

2) защищаемые помещения.

3) ЗИ от утечек по техническим каналам.

Задание 2

1) Провести анализ функциональных возможностей программных продуктов для защиты информационной системы.

2) Установить и проанализировать работу программы *ViPNet Registration Point*.

3) Изучить возможности программы *Sentinel HASP*.

4) Протестировать ключи *Guardant SP*.

Инструкция:

1) Изучить состав линейки программных продуктов компании «Инфо-ТеКС», используя раздаточный и дополнительный материал.

2) Изучить назначение, технические возможности электронных ключей защиты, используя раздаточный и дополнительный материал.

3) Установить программы *Sentinel HASP* и *Guardant SP*, изучить интерфейс и защитные функции.

Перечень раздаточных и дополнительных материалов:

1) Продуктовая линейка *CUSTOM*.

2) Электронные ключи защиты.

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 10

Задание 1

Разработать систему видеонаблюдения, входящую в комплексную систему информационной безопасности.

Объект: Периметр одноэтажного здания.

Инструкция:

1) Составить описание и техническое задание на установку системы видеонаблюдения.

2) Составить план размещения видеокамер.

3) Выбрать видеооборудование по техническим характеристикам с учетом особенностей объекта контроля.

4) Составить схему подключения оборудования.

Перечень раздаточных и дополнительных материалов:

1) Принцип построения систем видеонаблюдения.

2) Проектирование системы видеонаблюдения.

Задание 2

1) Изучить принципы действия, конструкцию и характеристики датчиков.

2) Изучить принцип контроля линейно-кабельных сооружений оператора связи МАКС ЛКС.

3) Изучить применение датчиков на сайте ТехноТроникс.

4) Составить схему размещения различных датчиков контроля состояния линейного оборудования на местной сети связи.

Инструкция:

1) Рассмотреть принцип работы системы контроля линейно-кабельных сооружений, используя раздаточный и дополнительный материал.

2) Рассмотреть применение датчиков ТехноТроникс в системе контроля линейно-кабельных сооружений.

Перечень раздаточных и дополнительных материалов:

1) Датчик вскрытия и запыленности.

2) Контроль линейно-кабельных сооружений.

3) Руководство пользователя Мираж_*GE_RX*4_01.

Возможно использование литературы:

1 Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - *ISBN* 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/118458.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 с. - *ISBN* 978-5-4488-0070-2. - Текст : электронный // Цифровой образовательный ресурс *IPR SMART* : [сайт]. - *URL: https://www.iprbookshop.ru*/87995.*html* (дата обращения: 25.02.2022). - Режим доступа: для авторизир. пользователей.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

4.2 Критерии оценки выполненных заданий

Выполнение задания (Таблица 4)*:*

- самостоятельность выполнения задания;

- рациональное распределение времени на выполнение задания (обязательно наличие следующих этапов выполнения задания: ознакомление с заданием и планирование работы; получение информации; подготовка продукта; рефлексия выполнения задания и коррекция подготовленного продукта перед сдачей);

- обращение в ходе выполнения задания к информационным источникам;

- своевременность выполнения заданий в соответствии с установленным лимитом времени;

- грамотность представления выполненного задания.

Таблица 4 - *Подготовленный продукт*.

Код ПК, ОК	Наименование компетенции	Выполнил	Не выполнил
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.		
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, применять стандарты антикоррупционного поведения.		
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 под-		

	держания необходимого уровня физической подготовленности.		
ОК 09	Использовать информационные технологии в профессиональной деятельности.		
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.		