МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН

«КИЗЛЯРСКИЙ ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»

ФОНД ОЦЕНОЧНЫХСРЕДСТВ
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ
код и название по ФГОС

10.02.05 «Обеспечение информационной безопасности автоматизированных систем»
код и наименование специальности

Кизляр, 2024 г.

Фонд оценочных средств профессионального модуля ПМ.03 «Защита информации техническими средствами», составлен на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО) 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного Приказом Министерства образования и науки от 09.12.2016 № 1553.

Фонд оценочных средств соответствует требованиям к содержанию, структуре, оформлению.

Организация-разработчик: ГБПОУ РД «Кизлярский профессионально-педагогический колледж».

Разработчики:

- Искандырова А.А.
- Раджабова А.Н.

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Цель фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу ПМ.03 «Защита информации техническими средствами».

Перечень видов оценочных средств соответствует Рабочей программе профессионального модуля.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля в форме тестовых заданий и промежуточной аттестации в форме тестовых заданий и практических заданий.

Структура и содержание заданий – задания разработаны в соответствии с рабочей программой ПМ.03 «Защита информации техническими средствами».

Освоение содержания ПМ.03 «Защита информации техническими средствами» обеспечивает достижение студентами следующих **результатов**:

Таблица 1 Перечень общих компетенций и личностных результатов:

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
ОК 2	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

ЛР 15	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации техническими средствами
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	– установки, монтажа и настройки технических средств защиты информации; технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

Уметь	– применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации
Знать	– порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации.

3. ФОРМЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ ЭЛЕМЕНТОВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

В результате текущей аттестации по ПМ.03 «Защита информации техническими средствами» осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих и профессиональных компетенций.

Таблица 2

Элемент модуля	**Форма контроля и оценивания**		
	Промежуточная аттестация	**Рубежный контроль**	**Текущий контроль**
МДК.03.01. Техническая защита информации	Дифференцированный зачет (6,7 семестр) Экзамен (8 семестр)	Тестирование Контрольная работа	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Тестирование; Контроль выполнения самостоятельной
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	Дифференцированный зачет (6,7 семестр) Экзамен (8 семестр)	Тестирование	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Контроль выполнения самостоятельной
УП. 03	Дифференцированный зачет (7 семестры)	------	Оценка результатов выполнения заданий и оформления отчетной документации по учебной практике
ПП 03	Дифференцированный зачет (7 семестр)	------	Оценка выполнения работ и оформления отчетной документации на производственной практике
Профессиональный модуль ПМ.03	Экзамен по модулю 8 семестр		

Контроль и оценка освоения учебной дисциплины «МДК.03.01 Техническая защита информации» по темам (разделам)

Элемент учебной дисциплины	Формы и методы контроля			
	Текущий контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые ОК, ПК, У, З	Форма контроля	Проверяемые ОК, ПК, У, З
Тема 1.1. Предмет и задачи технической защиты информации	Устный опрос. Практические занятие №1, №2.	ОК 1 – ОК 5 ПК.3.4 У, З	Экзамен	ОК 1 – ОК 5 ПК.3.4 У, З
Тема 1.2. Общие положения защиты информации техническими средствами	Устный опрос. Практическое занятие №3.	ОК 1 – ОК 5 ПК 3.1 ПК 3.2 У, З	Экзамен	ОК 1 – ОК 5 ПК 3.1 ПК 3.2 У, З
Тема 1.3. Информация как предмет защиты	Устный опрос. Практические занятия №4, №5, №6.	ОК 1 – ОК 6 ПК 3.1 ПК 3.2 У, З	Экзамен	ОК 1 – ОК 6 ПК 3.1 ПК 3.2 У, З
Тема 1.4. Технические каналы утечки информации	Устный опрос. Практические занятия №7, №8, №9.	ОК 01-ОК 9 ПК 3.1 ПК 3.2 У, З	Экзамен	ОК 01-ОК 9 ПК 3.1 ПК 3.2 У, З
Тема 1.5. Методы и средства технической разведки	Устный опрос. Практическое занятие №10.	ОК 01-ОК 9 ПК 3.1- ПК.3.4 У,З	Экзамен	ОК 01-ОК 9 ПК 3.1- ПК.3.4 У,З
Тема 2.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Устный опрос. Практические занятия №11-№15.	ОК 5 – ОК ПК 3.1-ПК.3.4 9, З	Экзамен	ОК 5 – ОК 9 ПК 3.1-ПК.3.4 У, З

Тема 2.2. Физические процессы при подавлении опасных сигналов	Устный опрос. Практическое занятие №16.	ОК 5 – ОК 9 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 5 – ОК 9 ПК 3.1-ПК.3.4 У, З
Тема 3.1. Системы защиты от утечки информации по акустическому каналу	Устный опрос. Практическое занятие №17.	ОК 1 – ОК 6 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 1 – ОК 6 ПК 3.1-ПК.3.4 У, З
Тема 3.2. Системы защиты от утечки информации по проводному каналу	Устный опрос. Практическое занятие №18.	ОК 6 – ОК 9 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 6 – ОК 9 ПК 3.1-ПК.3.4 У, З
Тема 3.3. Системы защиты от утечки информации по вибрационному каналу	Устный опрос. Практические занятия №19, №20.	ОК 1 ОК-2 ОК-8 ОК-9 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 1 ОК-2 ОК-8 ОК-9 ПК 3.1-ПК.3.4 У, З
Тема 3.4. Системы защиты от утечки информации по электромагнитному каналу	Устный опрос. Практические занятия №21, №22.	ОК 4 – ОК 9 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 4 – ОК 9 ПК 3.1-ПК.3.4 У, З
Тема 3.5. Системы защиты от утечки информации по телефонному каналу	Устный опрос. Практические занятия №23- №26.	ОК 01-ОК 9 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 01-ОК 9 ПК 3.1-ПК.3.4 У, З
Тема 3.6. Системы защиты от утечки информации по электросетевому каналу	Устный опрос. Практическое занятие №27.	ОК 01-ОК 9 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 01-ОК 9 ПК 3.1-ПК.3.4 У, З

Тема 4.1. Применение технических средств защиты информации	Устный опрос. Практические занятия №28, №29.	ОК 01-ОК 9 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 01-ОК 9 ПК 3.1-ПК.3.4 У, З
Тема 4.2. Эксплуатация технических средств защиты информации	Устный опрос. Практическое занятие №30.	ОК 01-ОК 9 ПК 3.1-ПК.3.4 У, З	Экзамен	ОК 01-ОК 9 ПК 3.1-ПК.3.4 У, З

Контроль и оценка освоения учебной дисциплины «МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации» по темам (разделам)

Элемент учебной дисциплины	**Формы и методы контроля**			
	Текущий контроль		**Промежуточная аттестация**	
	Форма контроля	**Проверяемые ОК, ПК, У, З**	**Форма контроля**	**Проверяемые ОК, ПК, У, З**
Тема 1.1. Построение и основные характеристики инженерно-технических средств физической защиты	Устный опрос. Практические занятия №1-№10.	ОК 01-ОК 9 ПК.3.5 У, З	Экзамен	ОК 01-ОК 9 ПК.3.5 У, З
Тема 1.2. Применение инженерно-технических средств физической защиты	Устный опрос. Практические занятия №11-№14.	ОК 1 – ОК 5 ПК.3.5 У, З	Экзамен	ОК 1 – ОК 5 ПК.3.5 У, З

Тема 1.3. Эксплуатация инженерно-технических средств физической защиты	Устный опрос. Практические занятия №15-№24.	ОК 1 ОК-2 ОК-3 ОК-7 ОК-8 ОК-9 ПК.3.5 У, З	Экзамен	ОК 1 ОК-2 ОК-3 ОК-7 ОК-8 ОК-9 ПК.3.5 У, З

Общие положения

1. Формы контроля и оценивания элементов профессионального модуля

2. Результаты освоения модуля, подлежащие проверке на экзамене по модулю

2.1. Общие/профессиональные компетенции, проверяемые дополнительно

2.2. Требования к портфолио

3. Оценка освоения профессионального модуля

3.1. Типовые задания для текущего контроля по МДК.03.01. Техническая защита информации

3.2. Типовые задания для рубежного контроля по МДК.03.01. Техническая защита информации

3.3. Типовые задания для промежуточного контроля по МДК.03.01. Техническая защита информации

3.4. Типовые задания для текущего контроля по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

3.5. Типовые задания для рубежного контроля по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

3.6. Типовые задания для промежуточного контроля по МДК.03. 02 Инженерно-технические средства физической защиты объектов информатизации

4. Требования к дифференцированному зачету по учебной и (или) производственной практике

4.1. Оценочные материалы

4.2. Форма аттестационного листа (из дневника по практике)

5. Структура контрольно-оценочных материалов для экзамена по модулю

6. Ведомость к экзамену по модулю

Общие положения

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности Защита информации техническими средствами и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения основной образовательной программы в целом. Формой аттестации по профессиональному модулю. Итогом экзамена является профессиональной деятельности освоен/не освоен». модулю является экзамен однозначное решение: Экзамен по модулю проводится в форме выполнения практико-ориентированных заданий.

1. Формы контроля и оценивания элементов профессионального модуля

Элемент модуля	Форма контроля и оценивания		
	Промежуточная аттестация	**Рубежный контроль**	**Текущий контроль**
МДК.03.01. Техническая защита информации	Дифференцированный зачет (6,7 семестр) Экзамен (8 семестр)	Тестирование Контрольная работа	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Тестирование; Контроль выполнения самостоятельной
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	Дифференцированный зачет (6,7 семестр) Экзамен (8 семестр)	Тестирование	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Контроль выполнения самостоятельной
УП. 03	Дифференцированный зачет (7 семестры)	------	Оценка результатов выполнения заданий и оформления отчетной документации по учебной практике
ПП 03	Дифференцированный зачет (8 семестр)	------	Оценка выполнения работ и оформления отчетной документации на производственной практике
Профессиональный модуль ПМ.03	Экзамен по модулю 8 семестр		

2. Результаты освоения модуля, подлежащие проверке на экзамене (квалификационном)

В результате аттестации по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Профессиональные и общие компетенции	Показатели оценки результата
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	распознает задачу и/или проблему в профессиональном контексте; анализирует задачу и/или проблему и выделяет её составные части; определяет этапы решения задачи; выявляет и осуществляет поиск

	решения задачи и/или проблемы; составляет план действия; определяет необходимые ресурсы; владеет актуальными методами работы в профессиональной и смежных сферах; реализует составленный план; оценивает результат и последствия своих действий, выделяет в нём сильные и слабые стороны
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;	определяет задачи поиска информации; определяет необходимые источники информации; планирует процесс поиска; структурирует получаемую информацию в соответствии с параметрами поиска; выделяет наиболее значимое в перечне информации; оценивает практическую значимость результатов поиска; интерпретирует полученную информацию в контексте профессиональной деятельности;
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;	использует актуальную нормативно-правовую документацию по специальности; применяет современную научно профессиональную терминологию; определяет актуальность нормативно-правовой документации в профессиональной деятельности; выстраивает траектории профессионального и личностного развития; участвует в конкурсах профессионального мастерства; участвует в мероприятиях профессиональной направленности (вебинары, семинары, конференции,
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;	участвует в деловом общении для эффективного решения деловых задач; планирует профессиональную деятельность; организует работу коллектива и команды; взаимодействует с коллегами, руководством, клиентами;

	при групповом обсуждении задает вопросы для понимания идей других; при групповом обсуждении: убеждается, что коллеги по группе поняли предложенную идею; участвует в деятельности по выявлению ресурсов команды; анализирует работу членов группы; анализирует результаты выполненного задания; презентует результаты работы группы; защищает полученные командой
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;	грамотно (устно и письменно) излагает свои мысли по профессиональной тематике на государственном языке; проявляет толерантность в рабочем коллективе; извлекает из устной речи (монолог, диалог, дискуссия) нужную информацию и логические связи, организующие эту информацию; грамотно оформляет документы на государственном языке; корректно общается с преподавателями и одногруппниками; соблюдает заданный жанр высказывания (служебный доклад, выступление на совещании / собрании, презентация товара / услуг); корректно отвечает на вопросы, направленные на выяснение мнения (позиции); задает четко сформулированные вопросы, направленные на получение необходимой
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;	соблюдает нормы поведения во время учебных занятий и прохождения учебной и производственной практик; понимать значимость своей специальности; демонстрирует поведение на основе общечеловеческих ценностей

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;	эффективность выполнения правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик; использует ресурсосберегающие технологии в профессиональной деятельности, на рабочем месте.
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик участие в спортивных мероприятиях и/или мероприятиях направленных на формирование здорового образа жизни
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языке	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); понимает тексты на базовые профессиональные темы; применяет в профессиональной деятельности инструкции на государственном и иностранном языке; строит простые высказывания о себе и о своей профессиональной деятельности; пишет простые связные сообщения на знакомые или интересующие профессиональные темы

2.1. Общие/профессиональные компетенции, проверяемые дополнительно:

ОК	Основные показатели результата	Дополнительные формы контроля		
		Портфо-лио	Курсовое проектирование	Промежуточная аттестация по практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	выбранный способ решения задачи аргументирован; доказана оптимальность выбранного способа решения применительно к контексту тематики курсового проекта	-	+	-
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;	наличие дипломов, грамот и сертификатов участия в мероприятиях по специальности; наличие дипломов, грамот и сертификатов участия в мероприятиях по формированию SoftSkills; положительный отзыв руководителя	+	-	+
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;	пояснительная записка оформлена грамотно на государственном языке; выдержан научный стиль изложения материала;	-	+	-

ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языке	~ список литературы содержит источники как на русском, так и на иностранных языках.	-	+	-

2.2. Требования к портфолио

Тип портфолио: смешанный.

Состав портфолио:

- ~ дипломы, грамоты и сертификаты участия в мероприятиях профессиональной направленности;
- ~ дипломы, грамоты и сертификаты участия в мероприятиях по формированию SoftSkills;
- ~ отзывы, характеристики с производственных практик;
- ~ разработанные проекты.

3. Оценка освоения профессионального модуля

3.1. Типовые задания для текущего контроля по **МДК.03.01. Техническая защита информации**

1)Вопросы для устного опроса по темам

Критерии оценки

«Отлично» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;

- доказательно раскрыты основные понятия, термины и др.;

- в ответе отслеживается четкая структура, выстроенная в логической последовательности;

- ответ изложен грамотным языком;

- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

«Хорошо» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять

существенные и несущественные моменты материала;

- ответ четко структурирован, выстроен в логической последовательности; - изложен грамотным языком;

- однако были допущены неточности в определении понятий, терминов и др.

«Удовлетворительно» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют некоторые нарушения;

- допущены несущественные ошибки в изложении теоретического материала и употреблении терминов;

- знания показаны слабо, речь неграмотная.

«Неудовлетворительно» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;

- допущены существенные ошибки в теоретическом материале (понятиях, терминах); - знания отсутствуют, речь неграмотная

Тема 1.1 Предмет и задачи технической защиты информации

1. Предмет и задачи технической защиты информации.

2. Характеристика инженерно-технической защиты информации как области информационной безопасности.

3. Системный подход при решении задач инженерно-технической защиты информации.

4. Основные параметры системы защиты информации.

Тема 1.2 Общие положения защиты информации техническими средствами

1. Задачи и требования к способам и средствам защиты информации техническими средствами.

2. Принципы системного анализа проблем инженерно-технической защиты информации.

3. Классификация способов и средств защиты информации.

Тема 2.1 Информация как предмет защиты

1. Особенности информации как предмета защиты. Свойства информации. 2. Виды, источники и носители защищаемой информации.

3. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

4. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы.

5. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке

Тема 2.2 Технические каналы утечки информации 1. Понятие и особенности утечки информации.

2. Структура канала утечки информации.

3. Классификация существующих физических полей и технических каналов утечки информации.

4. Характеристика каналов утечки информации.

5. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.

Тема 2.3 Методы и средства технической разведки 1. Классификация технических средств разведки. 2. Методы и средства технической разведки.

3. Средства несанкционированного доступа к информации. 4. Средства и возможности оптической разведки.

5. Средства дистанционного съема информации.

Тема 3.1 Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок

1. Физические основы побочных электромагнитных излучений и наводок. 2. Акустоэлектрические преобразования.

3. Паразитная генерация радиоэлектронных средств. 4. Виды паразитных связей и наводок.

5. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.

6. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей

Тема 3.2 Физические процессы при подавлении опасных сигналов 1. Скрытие речевой информации в каналах связи.

2. Подавление опасных сигналов акустоэлектрических преобразований. 3. Экранирование.

4. Зашумление

Тема 4.1 Системы защиты от утечки информации по акустическому каналу 1. Технические средства акустической разведки.

2. Непосредственное подслушивание звуковой информации.

3. Прослушивание информации направленными микрофонами. 4. Система защиты от утечки по акустическому каналу.

5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу

Тема 4.2 Системы защиты от утечки информации по проводному каналу 1. Принцип работы микрофона и телефона.

2. Использование коммуникаций в качестве соединительных проводов. 3. Негласная запись информации на диктофоны.

4. Системы защиты от диктофонов.

5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.

Тема 4.3 Системы защиты от утечки информации по вибрационному каналу 1. Электронные стетоскопы.

2. Лазерные системы подслушивания. 3. Гидроакустические преобразователи.

4. Системы защиты информации от утечки по вибрационному каналу.

5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу

Тема 4.4 Системы защиты от утечки информации по электромагнитному каналу 1. Прослушивание информации от радиотелефонов.

2. Прослушивание информации от работающей аппаратуры. 3. Прослушивание информации от радиозакладок.

4. Приемники информации с радиозакладок.

5. Прослушивание информации о пассивных закладок.

6. Системы защиты от утечки по электромагнитному каналу.

7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу

Тема 4.5 Системы защиты от утечки информации по телефонному каналу 1. Контактный и бесконтактный методы съема информации за счет

непосредственного подключения к телефонной линии.

2. Использование микрофона телефонного аппарата при положенной телефонной трубке.
3. Утечка информации по сотовым цепям связи.
4. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.

Тема 4.6 Системы защиты от утечки информации по электросетевому каналу 1. Низкочастотное устройство съема информации.

2. Высокочастотное устройство съема информации.

3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу

Тема 4.7 Системы защиты от утечки информации по оптическому каналу 1. Телевизионные системы наблюдения.

2. Приборы ночного видения.

3. Системы защиты информации по оптическому каналу

Тема 5.1 Применение технических средств защиты информации

1. Технические средства для уничтожения информации и носителей информации, порядок применения.

2. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.

3. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.

4. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

Тема 5.2 Эксплуатация технических средств защиты информации 1. Этапы эксплуатации технических средств защиты информации.

2. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.

3. Установка и настройка технических средств защиты информации.

4. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.

5. Организация ремонта технических средств защиты информации. 6. Проведение аттестации объектов информатизации

3.2. Типовые задания для рубежного контроля по МДК.03.01. Техническая защита информации

1)Типовая контрольная работа. Тема «Технические каналы утечки информации»

Задание. Ответить письменно на поставленные вопросы

Вариант 1

1. Задачи и требования к способам и средствам защиты информации техническими средствами.

2. Структура канала утечки информации.

3. Методы и средства технической разведки.

Вариант 2

1. Принципы системного анализа проблем инженерно-технической защиты информации. 2. Характеристика каналов утечки информации.

3. Средства дистанционного съема информации.

Критерии оценки

Отметкой «отлично» оцениваются ответы, которые показывают прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, давать аргументированные ответы, приводить примеры. *Отметкой «хорошо»* оцениваются ответы, обнаруживающие прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения,

приводить примеры. Однако допускаются две-три неточности в ответах. *Отметкой «удовлетворительно»* оцениваются ответы, свидетельствующие в основном о знании материалов, их свойств, технологий, но отличающиеся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа тем изучаемой дисциплины, недостаточным умением давать

аргументированные ответы и приводить примеры. Допускается несколько ошибок в содержании ответа.

Отметкой «неудовлетворительно» оцениваются ответы, обнаруживающие незнание материалов, их свойств, технологий изучаемой предметной области, отличающиеся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа тем изучаемой дисциплины; неумением давать аргументированные ответы. Допускаются серьезные ошибки в содержании ответов.

3.3. Типовые задания для промежуточного контроля по **МДК.03.01. Техническая защита информации**

1)Вопросы для подготовки к экзамену

1. Понятие информации. Проблема обеспечения безопасности в информационных системах, политика информационной безопасности.
2. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
3. Физические средства
4. Аппаратные средства
5. Программные средства
6. Криптографические средства
7. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля.
8. Генераторы шума.
9. Особенности работы и основные характеристики сканирующих радиоприемников.
10. Блок-схема типового сканирующего радиоприемника.
11. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения локализации в пространстве закладных устройств.
12. Виды модуляции и кодирования передаваемой информации.
13. Амплитудная модуляция. Амплитудная модуляция с подавлением верхней или нижней боковой частоты. Частотная модуляция. Фазовая модуляция.
14. Кодово-импульсная модуляция. Специальные виды модуляции. Основные требования к специальным системам связи.
15. Использование ШПС и ППРЧ сигналов. Основные характеристики.
16. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
17. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений.

18. . Концепции инженерно-технической защиты информации.
19. Системный подход к защите информации.

20. Основные проблемы инженерно-технической защиты информации.
21. Основные концептуальные положения инженерно-технической защиты информации.
22. Направления инженерно-технической защиты информации.
23. Показатели эффективности инженерно-технической защиты информации.
24. Теоретические основы инженерно-технической защиты информации.
25. Источники опасных сигналов.
26. Виды побочных опасных электромагнитных излучений.
27. Характеристика технической разведки.
28. Технические каналы утечки информации.
29. Методы инженерно-технической защиты информации.
30. Методы инженерной защиты и технической охраны объекта.
31. Методы скрытия информации и ее носителей.
32. Физические основы защиты информации.
33. Физические основы побочных электромагнитных излучений и наводок.
34. Распространение сигналов в технических каналах утечки информации.
35. Физические процессы подавления опасных сигналов.
36. Технические средства добывания и инженерно-технической защиты.
37. Средства технической разведки.
38. Средства инженерной защиты и технической охраны.
39. Средства предотвращения утечки информации по техническим каналам.
40. Организационные основы инженерно-технической защиты информации.
41. Государственная система защиты информации.
42. Контроль эффективности инженерно-технической защиты информации.
43. Методическое обеспечение инженерно-технической защиты автоматизированных систем от вредоносных программных воздействий.
44. Моделирование инженерно-технической защиты информации.
45. Методические рекомендации по оценке эффективности защиты информации.

3.5. Итоговое тестовое задание

по МДК. 03.01 «Техническая защита информации»

(ОК 1-ОК 9, ПК 3.1-3.4)

Вариант № 1 (ОК 1-ОК 9, ПК 3.1-3.2)

1. Какие из перечисленных мер относятся к техническим аспектам защиты информации? **(ПК 3.1) (ОК 1, ОК 2)**

A) Установка антивируса

B) Регламентированная процедура увольнения сотрудника

C) Контроль доступа к рабочим станциям

D) Организация курсов повышения квалификации работников

E) Монтаж ограждений территории объекта

2. Назовите документ, устанавливающий требования к охране коммерческой тайны. **(ПК 3.2) (ОК 2, ОК 3)**

_____

3. Соотнесите типы защиты информации с соответствующими методами **(ПК 3.3) (ОК 1, ОК 6):**

I: Законодательные и правовые меры

II: Организационные меры

III: Технические меры

Методы:

A) Лицензирование видов деятельности

B) Использование брандмауэра

C) Режим допуска к информации

D) Нормативные акты и инструкции

E) Криптоалгоритмы

4. Какой уровень конфиденциальности информации является наивысшим? **(ПК 3.4) (ОК 1, ОК 3)**

A) Конфиденциальная

B) Особой важности

C) Совершенно секретная

D) Ограниченная распространенность

5. Какой элемент не входит в перечень стандартных критериев классификации информационных ресурсов по уровням секретности? **(ПК 3.4) (ОК 1, ОК 3)**

A) Общая доступность

B) Секретная информация

C) Ограниченный доступ

D) Государственная тайна

6. Определите основное назначение СКЗИ (средств криптографической защиты информации). **(ПК 3.1) (ОК 2, ОК 6)**

---

7. Установите соответствие между видами защиты информации и примерами реализации **(ПК 3.5) (ОК 1, ОК 4):**

Виды защиты:

I: Физическая защита

II: Организационная защита

III: Техническая защита

Примеры реализации:

A) Ограждение периметра здания

B) Контроль доступа к информации через ACL (списки контроля доступа)

C) Регламентация порядка работы с конфиденциальной информацией

D) Использование экранирования и фильтрации электрических цепей

E) Установка сигнализаций и видеонаблюдения

8. Какие из указанных факторов влияют на уровень защиты информации? **(ПК 3.3) (ОК 2, ОК 5)**

A) Качество исполнения программных средств

B) Особенности архитектуры информационной системы

C) Уровень осведомленности сотрудников

D) Географическое расположение объекта

E) Внешняя среда (климатические условия)

9. Дайте определение понятию «контроль доступа». **(ПК 3.2) (ОК 1, ОК 4)**

---

10. Какая из нижеперечисленных мер защиты относится к физической защите информации? **(ПК 3.5) (ОК 1, ОК 7)**

A) Использование антивирусных программ

B) Кодирование данных

C) Установка пожарных извещателей

D) Организация раздельного рабочего пространства

11. Перечислите три элемента, входящие в состав единого комплексного подхода к защите информации. **(ПК 3.1) (ОК 2, ОК 3**

12. Сопоставьте механизмы защиты с целями их применения **(ПК 3.2) (ОК 1, ОК 4)**

Механизмы защиты:

I: Авторизация

II: Аутентификация

III: Шифрование

Цели применения:

A) Подтверждение личности субъекта

B) Допуск к ресурсу после подтверждения личности

C) Защита содержимого информации от просмотра сторонними лицами

13. Какие инструменты позволяют снизить вероятность инсайдерских угроз? **(ПК 3.3) (ОК 2, ОК 6)**

A) Регулярный аудит учетных записей сотрудников

B) Принцип минимально необходимой информированности

C) Повышение заработной платы сотрудников

D) Внутреннее расследование случаев злоупотреблений

E) Искусственное усложнение интерфейса системы

14. Для чего используется система обнаружения вторжений IDS? **(ПК 3.2) (ОК 1, ОК 4)**

A) Блокировка подозрительного трафика в сетях

B) Мониторинг сетевых соединений и выявление попыток атак

C) Создание резервных копий критически важных файлов

D) Автоматизированное восстановление повреждённой операционной системы

15. Для чего предназначен паспорт безопасности объекта? **(ПК 3.5) (ОК 2, ОК 3)**

A) Детализация состава применяемого оборудования

B) Документирование выявленных уязвимостей и мероприятий по их устранению

C) Учёт штатного расписания сотрудников

D) Определение местонахождения инженерных сооружений

16. Какие три параметра характеризуют критерии выбора технических средств защиты информации? **(ПК 3.1) (ОК 1, ОК 6)**

---

17. Что представляет собой протокол TLS? **(ПК 3.1) (ОК 2, ОК 6)**

A) Стандарт цифровой подписи электронной почты

B) Протокол проверки подлинности сообщений электронной почты

C) Методика шифрования беспроводных сетей Wi-Fi

D) Протокол защиты информации при передаче данных по открытым каналам связи

18. Какие показатели определяют качество защиты информации? **(ПК 3.4) (ОК 1, ОК 6)**

A) Сложность обхода защитного механизма

B) Скорость реакции на попытку вторжения

C) Высокая заработная плата администраторов

D) Удобство работы пользователей с системой

E) Скрытые дефекты программного обеспечения

19. Какие угрозы являются наиболее опасными для автоматизированных систем управления технологическими процессами (АСУТП)? **(ПК 3.4) (ОК 2, ОК 5)**

A) Угрозы отказа функционирования

B) Информационные атаки на систему управления

C) Повреждения коммуникаций вследствие аварии

D) Перегрузка серверов из-за роста количества подключенных рабочих станций

20. Какой этап является первым в процедуре аттестации информационной системы? **(ПК 3.2) (ОК 1, ОК 3)**

A) Предпроектное обследование

B) Проведение экспертизы

C) Формирование плана аттестационных мероприятий

D) Приемка результата аттестационных работ

Вариант № 2 (ОК 1-ОК 9, ПК 3.2-3.3)

1. Какие характеристики выделяют качественную систему защиты информации? **(ПК 3.1) (ОК 1, ОК 2)**

A) Масштабируемость

B) Интеграция с различными платформами

C) Высокие затраты на внедрение

D) Легкость адаптации к изменениям окружения

E) Совместимость с устаревшими системами

2. Как называют форму защиты информации, основанную на географической привязанности субъекта? **(ПК 3.5) (ОК 2, ОК 3)**

---

3. Соответствуйте формы защиты информации следующим категориям **(ПК 3.3) (ОК 1, ОК 6):**

Формы защиты:

I: Организационные меры

II: Технические меры

III: Правовые меры

Категории:

A) Регистрационный журнал учета доступа

B) Установленные санкции за нарушение правил безопасности

C) Фильтрация пакетов на межсетевом экране

D) Двухфакторная аутентификация

E) Регламент прохождения гостевых посетителей

4. Методы пассивного зондирования применяются для... **(ПК 3.3) (ОК 2, ОК 6)**

А) Активного воздействия на объект наблюдения

Б) Выполнения скрытых перехватов сигналов

В) Устранения обнаруженных дефектов структуры

Г) Обнаружения активности постороннего оборудования в охраняемой зоне

5. Какой метод защиты предотвращает чтение данных с жёсткого диска даже после его удаления? **(ПК 3.4) (ОК 1, ОК 3)**

A) Хэш-функции

B) Шифрование данных

C) Парольная защита

D) Биометрия

6. Отметьте две главные цели проведения аудита информационной безопасности. **(ПК 3.2) (ОК 2, ОК 6)**

---

7. Укажите правильное соответствие типов угроз кибернетическим атакам **(ПК 3.3) (ОК 1, ОК 4):**

Типы угроз:

I: Случайные события

II: Целевые нападения

III: Преступники-профессионалы

Нападения:

A) Утечка данных через небезопасные соединения

B) Денежный шантаж и вымогательство (ransomware)

C) Промышленный шпионаж

D) Недостаточно продуманная конфигурация настроек

8. Какие факторы повышают риск успешного взлома информационной системы? **(ПК 3.4) (ОК 2, ОК 5)**

A) Недостаточная квалификация персонала

B) Недостаточное финансирование отдела информационной безопасности

C) Низкое число попыток проникновения

D) Отсутствие должного уровня контроля доступа

E) Современные антивирусные продукты

9. Какой метод позволяет определить наличие активных каналов передачи данных в диапазоне низких частот? **(ПК 3.3) (ОК 2, ОК 5)**

A) Временное зондирование

B) Импульсное сканирование

C) Статистическое наблюдение

D) Логическое тестирование

10. Наиболее эффективный способ борьбы с акустическим проникновением информации **(ПК 3.1) (ОК 1, ОК 4)**:

A) Шумоизоляция помещений

B) Применение генераторов шума

C) Установка видеокамер и датчиков движения

D) Регулярная смена кодов ключей доступа

11. Что подразумевают под термином «логическое пространство доступа»? **(ПК 3.1) (ОК 1, ОК 4)**

---

12. Назначение электромагнитного экрана при размещении серверного оборудования включает **(ПК 3.3) (ОК 1, ОК 6)**:

A) Обеспечение равномерного распределения тепла внутри помещения

B) Сокращение потребления электроэнергии оборудованием

C) Надежную защиту от внешнего электромагнитного влияния

D) Облегчение процесса замены комплектующих элементов сервера

13. Какие методики помогают уменьшить угрозу внутреннего нарушителя? **(ПК 3.4) (ОК 1, ОК 6)**

A) Четко прописанные должностные инструкции

B) Регулярные курсы повышения квалификации сотрудников

C) Организация периодического контроля доступа к конфиденциальной информации

D) Психологические тесты для сотрудников

E) Свободный доступ сотрудников к любым частям корпоративной сети

14. Кто несет ответственность за организацию мероприятий по обеспечению безопасности информации? (ПК 3.2) (ОК 1, ОК 4)

A) Руководители подразделений ИТ-служб предприятий

B) Сотрудники службы безопасности

C) Пользователи корпоративной сети

D) Поставщики телекоммуникационного оборудования

15. Какая форма защиты информации предполагает строгий контроль физического доступа к помещениям и технике? **(ПК 3.5) (ОК 1, ОК 7)**

A) Архитектурная защита

B) Компьютерная защита

C) Физическая защита

D) Химическая защита

16. Почему недостаточно полагаться лишь на одну технологию защиты информации? **(ПК 3.1) (ОК 2, ОК 3)**

---

17. Чем отличаются проводные и беспроводные каналы передачи данных с точки зрения риска несанкционированного доступа? **(ПК 3.2) (ОК 2, ОК 3)**

A) Проводные каналы менее подвержены внешним воздействиям

B) Беспроводные каналы проще мониторить и контролировать

C) Передача данных по проводным линиям осуществляется быстрее

D) Проводные каналы требуют меньше энергоресурсов

18. Какие процессы относятся к административным мерам защиты информации? **(ПК 3.4) (ОК 2, ОК 5)**

A) Процедуры санкционирования доступа

B) Разработку и соблюдение политик безопасности

C) Профилирование и сегментирование сети

D) Регулярные тренировки сотрудников по вопросам безопасности

E) Применение биометрии

19. В чем особенность доверенной загрузки операционной системы? **(ПК 3.5) (ОК 1, ОК 7)**

A) Она ускоряет загрузку ОС благодаря кэшированию драйверов

B) Осуществляет проверку неизменности ядра и основных модулей ОС

C) Устанавливает дополнительные программы автоматически

D) Полностью изолирует прикладные приложения от вредоносных программ

20. Какая методика направлена на снижение опасности инсайдеров? **(ПК 3.3) (ОК 2, ОК 6)**

A) Шифрование данных

B) Политики разграничения доступа

C) Использование прокси-серверов

D) Установление межсетевых экранов

Ключи к тесту

№ п/п	Вариант №1	Вариант №2
1.	A, C	A, B, D
2.	Федеральный закон № 98-ФЗ	Территориальная защита.
3.	I: A, D II: C III: B, E	I: A, E II: C, D III: B
4.	C	D
5.	A	B
6.	Обеспечение конфиденциальности, целостности и аутентичности информации посредством криптографических преобразований.	Оценка текущего уровня защищённости и выработка рекомендаций по снижению рисков.
7.	I: A, E II: C III: B, D	I: A, D II: B III: C
8.	A, B, C	A, B, D
9.	Контроль доступа — это совокупность методов и механизмов, обеспечивающих ограничение доступа субъектов к объектам системы в соответствии с установленными правилами.	B
10.	C	B
11.	Правовые, организационные и технические меры.	Часть виртуального ресурса, доступ к которой ограничен набором правил и процедур.
12.	I: B II: A III: C	C
13.	A, B, D	A, B, C
14.	B	A
15.	B	C
16.	Соответствие нормативным требованиям, стоимость,	Одновременное применение нескольких технологий повышает

	надёжность.	общую устойчивость системы к возможным угрозам.
17.	D	A
18.	A, B, D	A, B, D
19.	B	B
20.	A	B

3.6. Типовые задания для текущего контроля по **МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации**:

1) Практические работы, представленные в методических указаниях по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.

2)Вопросы для устного опроса по темам

«Отлично» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;

- доказательно раскрыты основные понятия, термины и др.;

- в ответе отслеживается четкая структура, выстроенная в логической последовательности;

- ответ изложен грамотным языком;

- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

«Хорошо» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала;

- ответ четко структурирован, выстроен в логической последовательности; - изложен грамотным языком;

- однако были допущены неточности в определении понятий, терминов и др.

«Удовлетворительно» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют некоторые нарушения;

- допущены несущественные ошибки в изложении теоретического материала и употреблении терминов;

- знания показаны слабо, речь неграмотная.

«Неудовлетворительно» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;

- допущены существенные ошибки в теоретическом материале (понятиях, терминах); - знания отсутствуют, речь неграмотная

Тема 1.1 Цели и задачи физической защиты объектов информатизации

1. Характеристики потенциально опасных объектов.

2. Содержание и задачи физической защиты объектов информатизации.

3. Основные понятия инженерно-технических средств физической защиты.

4. Категорирование объектов информатизации.

5. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.

6. Особенности задач охраны различных типов объектов.

Тема 1.2 Общие сведения о комплексах инженерно-технических средств физической защиты

1. Общие принципы обеспечения безопасности объектов.

2. Жизненный цикл системы физической защиты.

3. Принципы построения интегрированных систем охраны.

4. Классификация и состав интегрированных систем охраны.

5. Требования к инженерным средствам физической защиты.

6. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.

Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты

1. Информационные основы построения системы охранной сигнализации.

2. Назначение, классификация технических средств обнаружения.

3. Построение систем обеспечения безопасности объекта.

4. Периметровые средства обнаружения: назначение, устройство, принцип действия.

5. Объектовые средства обнаружения: назначение, устройство, принцип действия.

Тема 2.2 Система контроля и управления доступом

1. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности.

2. Особенности построения и размещения СКУД.

3. Структура и состав СКУД.

4. Периферийное оборудование и носители информации в СКУД.

5. Основы построения и принципы функционирования СКУД.

6. Классификация средств управления доступом.

7. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.

8. Обнаружение металлических предметов и радиоактивных веществ.

Тема 2.3 Система телевизионного наблюдения

1. Аналоговые и цифровые системы видеонаблюдения.

2. Назначение системы телевизионного наблюдения.

3. Состав системы телевизионного наблюдения.

4. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.

Тема 2.4 Система сбора, обработки, отображения и документирования информации

1. Классификация системы сбора и обработки информации.

2. Схема функционирования системы сбора и обработки информации.

3. Варианты структур построения системы сбора и обработки информации.

4. Устройства отображения и документирования информации.

Тема 2.5 Система воздействия

1. Назначение и классификация технических средств воздействия.

2. Основные показатели технических средств воздействия.

Тема 3.1 Применение инженерно-технических средств физической защиты

1. Периметровые и объектовые средства обнаружения, порядок применения.

2. Работа с периферийным оборудованием системы контроля и управления доступом.

3. Особенности организации пропускного режима на КПП.

4. Управление системой телевизионного наблюдения с автоматизированного рабочего места.

5. Порядок применения устройств отображения и документирования информации.

6. Управление системой воздействия.

Тема 3.2 Эксплуатация инженерно-технических средств физической защиты

1. Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.

2. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.

3. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.

4. Организация ремонта технических средств физической защиты.

3.6. Задания по разделам дисциплины МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты.

ОК-01, ОК-02, ОК-09

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Что такое процедура? а. Правила использования программного и аппаратного обеспечения в компании б. Пошаговая инструкция по выполнению задачи в. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах г. Обязательные действия	б
Задание 2. *Прочитайте текст, выберите один правильный ответ* Что такое IDS? а. Система обнаружения вторжений б. Система межсетевого экранирования в. Система тактического планирования г. Система протоколирования и аудита	а
Задание 3. *Прочитайте текст, выберите один правильный ответ* Достоинством дискретных моделей политики безопасности является а. простой механизм реализации б. числовая вероятностная оценка надежности а.высокая степень надежности г. динамичность	а
Задание 4. *Прочитайте текст, выберите один правильный ответ* Для решения проблемы правильности выбора и надежности функционирования средств защиты в «Европейских критериях» вводится понятие а.адекватности средств защиты б.унификации средств защиты в.надежности защиты информации г.оптимизации средств защиты	а
Задания открытого типа	

Задание 5. *Прочитайте текст и ответьте на вопрос* Наукой, изучающей математические методы защиты информации путем ее	Криптология
Задание 6. *Прочитайте текст и ответьте на вопрос* Основу политики безопасности составляет?	Способ управления доступом
Задание 7. *Прочитайте текст и ответьте на вопрос* С точки зрения ГТК основной задачей средств безопасности является обеспечение?	Защиты от НСД
Задание 8. *Прочитайте текст и дополните ответ* Класс F-DC согласно «Европейским критериям» характеризуется повышенными требованиями к _____	Конфиденциальности
Задание 9. *Прочитайте текст и ответьте на вопрос* Какая длина исходного ключа у алгоритма шифрования DES(бит)?	56
Задание 10. *Прочитайте текст и дополните ответ* В многоуровневой модели, если субъект доступа формирует запрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен _____	Доминировать
Задание 11. *Прочитайте текст и дополните ответ* В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен _____	Быть равен
Задание 12. *Прочитайте текст и дополните ответ* Оконечное устройство канала связи, через которое процесс может передавать или получать данные, называется _____	Сокет
Задание 13. *Прочитайте текст и дополните ответ* Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется _____	Качеством информации

Раздел 2. Основные компоненты комплекса инженерно- технических средств физической защиты

ОК-01, ОК-02, ОК-09

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Что из перечисленного не является целью проведения анализарисков? а. Делегирование полномочий б. Количественная оценка воздействия потенциальных угроз в. Выявление рисков г. Определение баланса между воздействием риска и стоимостью необходимых контрмер д.	а
Задание 2. *Прочитайте текст, выберите один правильный ответ* Перехват, который основан на фиксации электромагнитныхизлучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется: а .активный перехват; б.пассивный перехват; в.аудиоперехват; г.видеоперехват;	б
Задание 3. *Прочитайте текст, выберите один правильный ответ* Под replay-атакой понимается: а. модификация передаваемого сообщения б. повторное использование переданного ранее сообщения в. невозможность получения сервиса законным пользователем	б
Задание 4. *Прочитайте текст, выберите один правильный ответ* Выделения пользователем и администраторам только тех правдоступа, которые им необходимы это а.принцип минимазации привилегий б.принцип простоты и управляемости ИС в.принцип многоуровневой защиты г.принцип максимизации привилегий	а
Задания открытого типа	

Задание 5. *Прочитайте текст и ответьте на вопрос* Достоинствами программной реализации криптографического закрытия данных являются?	Практичность и гибкость
Задание 6. *Прочитайте текст и дополните ответ* Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается _____	Высокой
Задание 7. *Прочитайте текст и дополните ответ* Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается ___	Средней
Задание 8. *Прочитайте текст и дополните ответ* Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается _____	Базовой
Задание 9. *Прочитайте текст и дополните ответ* Длина исходного ключа в ГОСТ 28147-89 (бит) составляет _____	256
Задание 10. *Прочитайте текст и дополните ответ* По документам ГТК количество классов защищенности АСот НСД _____	9
Задание 11. *Прочитайте текст и дополните ответ* С помощью закрытого ключа информация _____	Расшифровывается
Задание 12. *Прочитайте текст и дополните ответ* Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это _____	Аутентификация

Задание 13. *Прочитайте текст и дополните ответ* При полномочной политике безопасности совокупностьметок с одинаковыми значениями образует _____	Уровень безопасности

Раздел 3. Применение и эксплуатация инженерно- технических средств физической защиты

ОК-01, ОК-02, ОК-03, ОК-04, ОК-09

ПК-3.5

Вопрос	Ответ
Задание 1. *Прочитайте текст, выберите один правильный ответ* Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: а.активный перехват; б.пассивный перехват; в.аудиоперехват; г.видеоперехват; д.просмотр мусора.	в
Задание 2. *Прочитайте текст, выберите один правильный ответ* Если используются автоматизированные инструменты для анализарисков, почему все равно требуется так много времени для проведения анализа? а. Много информации нужно собрать и ввести в программу б. Руководство должно одобрить создание группы в. Анализ рисков не может быть автоматизирован, что связано ссамой природой оценки г. Множество людей должно одобрить данные	а
Задание 3. *Прочитайте текст, выберите один правильный ответ* В модели политики безопасности Лендвера ссылка на сущность,если это идентификатор сущности, называется а. прямой б. простой в. циклической г. косвенной	а

Задание 4. *Прочитайте текст, выберите один правильный ответ* Абстрактное описание системы, без связи с ее реализацией, даетмодель политики безопасности а. С полным перекрытием б. Белла-ЛаПадула в. На основе анализа угроз г.Лендвера	б
Задания открытого типа	
Задание 5. *Прочитайте текст и дополните ответ* Для реализации технологии RAID создается _____	Псевдодрайвер
Задание 6. *Прочитайте текст и дополните ответ* Единственный ключ используется в криптосистемах называется _____	Симметричный
Задание 7. *Прочитайте текст и дополните ответ* Запись определенных событий в журнал безопасностисервера называется _____	Аудитом
Задание 8. *Прочитайте текст и дополните ответ* Главным параметром криптосистемы является показатель _____	Криптостойкости
Задание 9. *Прочитайте текст и ответьте на вопрос*	Руководство
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?	
Задание 10. *Прочитайте текст и дополните ответ* Недостатком дискретных моделей политики безопасности является _____	Статичность
Задание 11. *Прочитайте текст и дополните ответ* Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется_____	Профилем защиты
Задание 12. *Прочитайте текст и дополните ответ* Математические методы нарушения конфиденциальности иаутентичности информации без знания ключей объединяет _____	Криптоанализ

Задание 13. *Прочитайте текст и ответьте на вопрос* Какое количество уровней адекватности, которое определяют «Европейские критерии»?	7

Типовые задания для рубежного контроля по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации:

Тестовое задание

Вариант №1

1. **Что представляет собой информация в информатизации?**

а) Смесь цветов
б) Случайные символы
в) Организованные данные смыслового содержания
г) Звуковая волна

2. **Какие объекты могут подвергаться информатизации?**

а) Только природные явления
б) Различные объекты, включая данные, процессы и системы
в) Исключительно химические соединения
г) Только материальные объекты

3. **Что представляет собой информационный сигнал в контексте передачи данных?**

а) Световая волна
б) Звуковая волна
в) Передающее сообщение в виде электрического сигнала
г) Цветовой спектр

4. **Какие физические свойства могут быть характерны для аналоговых сигналов?**

а) Дискретность значений
б) Бесконечное количество значений в диапазоне
в) Ограниченный диапазон частот
г) Цифровое кодирование

5. **Какой документ регулирует вопросы информационной безопасности в Российской Федерации?**

а) Конституция Российской Федерации
б) Закон о защите от вредоносных программ
в) Федеральный закон "Об информации, информационных технологиях и о защите информации"
г) Декларация прав человека и гражданина

6. **Что определяют нормативные акты в области защиты информации?**

а) Лишь рекомендации и советы
б) Методы взлома информационных систем
в) Обязательные требования и правила по обеспечению безопасности информации
г) Программы для шифрования данных

7. **Что включает в себя физическая защита объектов информатизации?**

а) Только программное обеспечение
б) Организационные и технические меры, направленные на предотвращение несанкционированного доступа
в) Электронные пароли

г) Защита
от вирусов

8. Какое значение имеет правовое обеспечение физической защиты объектов информатизации?

а) Только документирование процедур
б) Установление норм и правил обеспечения безопасности, а также ответственности за их нарушение
в) Инвентаризация оборудования
г) Обучение
персонала

9. Что определяет объект как потенциально опасный?

а) Только наличие огнестрельного оружия
б) Возможность причинения вреда здоровью людей и окружающей среде
в) Только размер объекта
г) Отдаленное расположение от населенных пунктов

10. Какие критерии могут указывать на потенциальную опасность объекта в информатизированном обществе?

а) Наличие ценной информации, влияющей на функционирование общества и государства
б) Лишь количество сотрудников компании
в) Только финансовые показатели
г) Уровень образования сотрудников

11. Что включает в себя физическая защита объектов информатизации?

а) Охрана со стороны сотрудников
б) Организационные, технические и меры контроля доступа
в) Установка антивирусного программного
обеспечения
г) Электронные пароли

12. Какие задачи решает физическая защита в области информатизации?

а) Защита от вирусов
б) Предотвращение несанкционированного доступа, обеспечение целостности и конфиденциальности информации, обеспечение работоспособности системы
в) Контроль за содержанием информации
г) Оптимизация работы
компьютеров

13. Что представляют собой инженерно-технические средства физической защиты?

а) Только электрические приборы
б) Совокупность средств и систем, предназначенных для обеспечения безопасности объектов
в) Только строительные конструкции
г) Автомобильные
дороги

14. Какие задачи решают инженерно-технические средства физической защиты?

а) Только охрана от пожаров
б) Предотвращение несанкционированного проникновения, обнаружение и реагирование на инциденты безопасности
в) Только декоративное украшение объекта
г) Улучшение климата в
помещении

15. Какие этапы включает в себя жизненный цикл системы инженерно-технических средств физической защиты?

а) Только проектирование
б) Проектирование, внедрение, эксплуатация, вывод из эксплуатации
в) Только обслуживание
г) Разработка технической документации

16. На каком этапе жизненного цикла происходит разработка технических требований к системе физической защиты?

а) На этапе
проектирования
б) Только на
этапе
внедрения
в) Только на этапе эксплуатации
г) На этапе вывода из эксплуатации

17. Какие методы могут быть использованы при внедрении инженерно-технических средств на объекты информатизации?

а) Только метод проб и ошибок
б) Метод пилотного проекта, этапного внедрения, стратегии
"большого взрыва" в) Только принуждение сотрудников
г) Метод случайного выбора

18. Какой метод предпочтителен при внедрении инженерно-технических средств с минимальными рисками?

а) Метод "большого взрыва"
б) Метод пилотного проекта
в) Метод этапного внедрения
г) Метод случайного выбора

19. Какие требования предъявляются к системам видеонаблюдения с точки зрения информационной безопасности?

а) Только высокая разрешающая способность
б) Шифрование передаваемых видеопотоков, защита от несанкционированного доступа
в) Только цветовое воспроизведение
г) Простота использования

20. Каким образом системы контроля доступа должны обеспечивать информационную безопасность предприятия?

а) Ограничение и регулирование доступа, регистрация действий сотрудников
б) Только обнаружение движения на территории

в) Легкость обхода системы
г) Только визуализацию рабочего времени

Вариант №2

1. Что характеризует информацию в контексте информатизации?

а) Безупречная форма
б) Значимость и организованность данных
в) Непредсказуемость
г) Случайность и случайность

2. Какова цель информатизации объектов?

а) Сокрытие информации
б) Уменьшение доступности данных
в) Эффективное управление информацией и повышение производительности
г) Случайная трансформация данных

3. Какое из перечисленных является примером цифрового сигнала?

а) Синусоидальная волна
б) Битовая последовательность 01010101
в) Амплитудная модуляция
г) Аналоговый ток

4. Что определяет частоту информационного сигнала?

а) Временной интервал между битами
б) Скорость передачи данных
в) Диапазон изменения амплитуды
г) Количество колебаний в секунду

5. Какой орган в России отвечает за контроль и надзор в области защиты информации?

а) Министерство здравоохранения
б) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
в) Министерство образования и науки
г) Федеральная служба безопасности (ФСБ)

6. Какие данные относятся к категории ограниченного доступа согласно законодательству России?

а) Информация о погоде
б) Сведения о подготовке к военным действиям и действиям в чрезвычайных ситуациях
в) Новости о спорте
г) Объявления о продаже недвижимости

7. Какие органы ответственны за контроль за соблюдением правил физической защиты?

а) Только местные органы самоуправления
б) Федеральные органы исполнительной власти и органы местного самоуправления, уполномоченные в сфере информационной безопасности
в) Только представители бизнес-структур
г) Акционеры компании

8. Какое документальное оформление необходимо для обеспечения физической защиты?

а) Только устные инструкции от руководства
б) Письменные объявления на дверях помещений
в) Только устные инструкции от
сотрудников
г) Разработка и утверждение положений о физической защите, планов мероприятий по безопасности

9. Что подразумевается под термином "критерии оценки потенциальной опасности"?

а) Только цвет стен здания
б) Определенные параметры и характеристики, позволяющие оценить степень возможного воздействия объекта на окружающую среду
в) Только наличие забора вокруг объекта
г) Лишь местоположение
объекта

10. Какие объекты могут быть отнесены к потенциально опасным в информационной сфере?

а) Только банковские учреждения
б) Информационные системы, обрабатывающие данные
государственной важности
в) Только склады материалов
г) Культурные учреждения

11. Каким образом реализуется организационная часть физической защиты объектов информатизации?

а) Установка сигнализации
б) Разработкой и внедрением правил и процедур безопасности,
обучением персонала
в) Использование биометрической идентификации
г) Регулярной сменой паролей

12. Какие технические средства могут быть задействованы в физической защите?

а) Огнетушители
б) Системы видеонаблюдения, датчики движения, системы
контроля доступа
в) Оборудование для автоматического восстановления данных
г) Программы антивирусной защиты

13. Какие функции могут выполнять системы видеонаблюдения в инженерно-технических средствах физической защиты?

а) Определение и фиксация движения, визуальное наблюдение за объектом,
детекция нарушений безопасности
б) Только запись звука
в) Только подсветка
территории

г) Предупреждение
об авариях

14. Каким образом датчики движения могут использоваться в инженерно-технических средствах физической защиты?

а) Только для замера
температуры
б) Определение
влажности воздуха
в) Только для измерения уровня освещенности
г) Обнаружение движения и сигнализация о наличии посторонних объектов на охраняемой территории

15. Что включает в себя этап внедрения в жизненном цикле системы физической защиты?

а) Только тестирование оборудования
б) Установка и настройка системы, обучение персонала, внедрение в реальные условия
в) Только разработка технической документации
г) Обслуживание оборудования

16. На каком этапе происходит активное использование системы физической защиты?

а) Только на этапе
проектирования
б) На этапе вывода из
эксплуатации
в) Только на этапе
внедрения
г) На этапе эксплуатации

17. Как осуществляется внедрение по методу "большого взрыва"?

а) Только поэтапно
б) Одновременно на всем объекте
в) Только по одному
элементу в день
г) Случайным образом

18. Что представляет собой метод этапного внедрения?

а) Внедрение на случайно выбранных этапах
б) Постепенное внедрение на различных этапах с последующей проверкой и корректировкой
в) Только внедрение на последних этапах
г) Одновременное внедрение на всех этапах

19. Какие требования к датчикам движения необходимы для обеспечения информационной безопасности?

а) Надежность обнаружения, защита от ложных
срабатываний
б) Только высокая чувствительность
в) Только совместимость с другими
устройствами

г) Простота монтажа

20. Какую роль выполняют системы сигнализации в обеспечении информационной безопасности?
а) Только визуальное оповещение
б) Своевременное обнаружение и сигнализация о возможных инцидентах безопасности в) Только запись видеоматериалов
г) Поддержание микроклимата в помещении

Вариант № 3

1. **Что является основой для объектов информатизации?**

а) Только человеческий фактор
б) Данные и
информационные
технологии
в) Эмоциональные состояния
г) Несистематизированные хаос и беспорядок

2. **Какой процесс непосредственно связан с информатизацией объектов?**

а) Случайное изменение данных
б) Отделение от информационных технологий
в) Внедрение современных технологий для управления
информацией
г) Изоляция данных от доступа

3. **Какова роль шума в передаче данных?**

а) Увеличение скорости передачи
б) Искажение и исключение полезной
информации
в) Снижение частоты сигнала
г) Увеличение амплитуды сигнала

4. **Что характеризует амплитуду информационного сигнала?**

а) Временной интервал
между битами
б) Частоту передачи
данных
в) Максимальное отклонение сигнала от
нулевого уровня
г) Длительность сигнала

5. **Какие меры обеспечения безопасности информации предписаны законодательством?**

а) Только шифрование данных

б) Только установка антивирусного программного обеспечения
в) Комплекс мер, включая шифрование, антивирусную защиту, контроль доступа и т.д.
г) Регулярное копирование данных

6. Какой документ содержит основные положения о защите информации в информационных системах?

а) ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации"
б) Техническое задание на создание сайта
в) Рецепт приготовления кофе
г) Справочник по программированию на языке Python

7. Какова роль технических средств в физической защите объектов информатизации?

а) Обеспечение физической безопасности при помощи видеонаблюдения, контроля доступа и т.д.
б) Исключительно оформление бумажных документов
в) Только защита от вирусов
г) Сокрытие компьютеров от посторонних глаз

8. Какие основные нормативно-правовые акты регулируют физическую защиту объектов информатизации в России?

а) Законы о земле и воде
б) Федеральный закон "Об информации, информационных технологиях и о защите информации"
в) Налоговый кодекс
г) Конституция Российской Федерации

9. Какие характеристики могут быть важны для оценки потенциальной опасности в информатизированных системах?

а) Только год создания компании
б) Уровень заработной платы сотрудников
в) Значимость обрабатываемой информации, уровень защиты данных
г) Цвет фасада здания

10. Какое значение имеет оценка вероятности возникновения опасных ситуаций на объекте?

а) Только для страховых компаний
б) Позволяет определить необходимость и эффективность мер по физической защите
в) Лишь для геологов
г) Применяется только в промышленности

11. Какое значение имеет контроль доступа в физической защите объектов информатизации?

а) Ограничение доступа к печатающим устройствам
б) Предотвращение несанкционированного проникновения, контроль за перемещением людей в помещении
в) Защита от перегрева оборудования
г) Увеличение скорости передачи данных

12. Какие принципы лежат в основе технической части физической защиты информатизированных объектов?

а) Принцип энергосбережения
б) Принципы целесообразности, неотвратимости, комплексности и сочетания с организационными мерами
в) Принцип экономии бумаги
г) Принцип самообслуживания

13. Какую роль могут выполнять системы контроля доступа в инженерно-технических средствах физической защиты?

а) Только регистрация рабочего времени
б) Определение температуры в помещении
в) Только контроль за исправностью оборудования
г) Ограничение и регулирование доступа сотрудников и посетителей на объект

14. Какие преимущества обеспечивает использование биометрической идентификации в системах физической защиты?

а) Только низкая стоимость оборудования
б) Высокий уровень точности идентификации, исключение возможности передачи аутентификационных данных
в) Только дополнительный эффект декоративности
г) Улучшение качества интернет-соединения

15. Какие меры могут быть предприняты на этапе эксплуатации системы физической защиты?

а) Только заключение контрактов с поставщиками оборудования
б) Проведение регулярных технических обслуживаний, мониторинг работы системы, обучение персонала
в) Только разработка новых технических требований
г) Обновление программного обеспечения

16. Какие этапы включают в себя мероприятия по выводу системы физической защиты из эксплуатации?

а) Только разработка технической документации
б) Подготовка к выводу, анализ эффективности, разработка отчетов
в) Только демонтаж оборудования
г) Подписание нового контракта

17. Какова основная идея метода пилотного проекта?

а) Провести внедрение только в
одном отделе
б) Внедрение только на
критических объектах
в) Только обучение персонала на отдельных образцах
г) Выбрать небольшую часть объекта для тестирования и корректировки перед полным внедрением

18. Какие преимущества предоставляет метод проб и ошибок при внедрении инженерно-технических средств?

а) Постепенное выявление недостатков и корректировка,
минимизация рисков б) Только сокращение сроков внедрения
в) Только снижение бюджетных затрат
г) Ускорение процесса внедрения на всех объектах

19. Каким образом технические барьеры должны способствовать обеспечению информационной безопасности предприятия?

а) Только как декоративные элементы
б) Ограничение доступа посетителей, создание зон
контролируемого доступа в) Только для обозначения
территории
г) Снижение энергопотребления

20. Какие требования предъявляются к системам биометрической идентификации для обеспечения информационной безопасности?

а) Высокий уровень точности идентификации, исключение возможности передачи аутентификационных данных
б) Только низкая стоимость оборудования
в) Только дополнительный эффект
декоративности г) Улучшение
качества интернет-соединения

Вариант № 4

1. Как изменяется природа информации при информатизации объектов?

а) Становится менее
структурированной
б) Теряет свою значимость
в) Становится более организованной и
целенаправленной
г) Превращается в случайный набор данных

2. Какое влияние оказывает информатизация на эффективность управления информацией?

а) Снижает эффективность
б) Не влияет на эффективность
в) Делает управление
беспорядочным
г) Повышает
эффективность

3. Как влияет демпфирование на информационный сигнал? а) Уменьшение амплитуды сигнала по мере распространения
б) Увеличение частоты сигнала
в) Искажение формы сигнала
г) Увеличение длительности сигнала

4. Что определяет скорость передачи данных в канале связи?
а) Амплитуду сигнала
б) Количество бит, передаваемых за единицу времени
в) Частоту сигнала
г) Длительность сигнала

5. Какие субъекты относятся к категории субъектов информационных отношений согласно законодательству России?
а) Только физические лица
б) Только юридические лица
в) Физические и юридические лица, осуществляющие обработку информации
г) Информационные технологии

6. Какова ответственность за нарушение законодательства о защите информации в России?
а) Только предупреждение
б) Административная, гражданская и уголовная ответственность
в) Штраф в размере 5000 рублей
г) Ограничение доступа к интернету

7. Что подразумевается под термином "организационные меры" в физической защите?
а) Только установление технических средств защиты
б) Только охрана со стороны правоохранительных органов
в) Система правил и процедур, направленных на обеспечение безопасности г) Только пожарная безопасность

8. Какие документы могут определять порядок физической защиты?
а) Только техническая документация
б) Положения о физической защите и планы мероприятий по обеспечению безопасности
в) Только устав предприятия
г) Протоколы собраний акционеров

9. Какие виды угроз могут быть связаны с потенциально опасными объектами в информационной сфере?

а) Только стихийные бедствия
б) Кибератаки, утечка конфиденциальной информации, нарушение целостности данных
в) Только человеческий фактор
г) Загрязнение окружающей среды

10. Что подразумевается под термином "возможные последствия потенциально опасных объектов"?

а) Только возможные финансовые потери
б) Потенциальные угрозы для здоровья людей, окружающей среды и общества в целом
в) Только временные проблемы с работой объекта
г) Возможность создания новых рабочих мест

11. Какие методы обучения персонала используются в организациях для обеспечения физической безопасности?

а) Чтение статей в интернете
б) Проведение тренингов, семинаров, тестирование сотрудников
в) Самостоятельное изучение литературы по теме
г) Принуждение к выполнению правил

12. Как обеспечивается физическая защита в условиях удаленной работы сотрудников?

а) Применение VPN-соединений
б) Комбинацией технологий, включая шифрование данных, использование защищенных каналов связи и контроль дистанционного доступа
в) Проведение ежегодных тренингов по физической защите
г) Запрет на удаленную работу

13. Каким образом технические барьеры могут применяться в инженерно-технических средствах физической защиты?

а) Только как декоративные элементы
б) Ограничение доступа посетителей, создание зон контролируемого доступа
в) Только для обозначения территории
г) Снижение энергопотребления

14. Какую роль могут играть системы сигнализации в инженерно-технических средствах физической защиты?

а) Своевременное обнаружение и сигнализация о возможных инцидентах безопасности
б) Только визуальное оповещение
в) Только запись видеоматериалов

г) Поддержание микроклимата в помещении

15. На каком этапе возможно проведение модернизации системы физической защиты?

а) Только на этапе
проектирования
б) На этапе внедрения
в) Только на этапе эксплуатации
г) На любом этапе жизненного цикла

16. Какие факторы могут повлиять на принятие решения о модернизации системы физической защиты?

а) Техническое устаревание оборудования, изменение уровня угроз,
появление новых технологий
б) Только изменение
структуры персонала
в) Только финансовые
аспекты
г) Рост числа сотрудников

17. Каким образом может быть реализован метод случайного выбора?

а) Только розыгрышем среди
сотрудников
б) Выбор случайного объекта
для внедрения
в) Только решением
руководства
г) Путем проведения конкурса

18. Какие этапы включает в себя стратегия "большого взрыва"?

а) Только этап обучения персонала
б) Подготовка, внедрение,
обучение персонала
в) Только этап тестирования
г) Этап выбора метода внедрения

19. Какие требования предъявляются к системам датчиков утечки воды для обеспечения информационной безопасности?

а) Быстрое обнаружение утечки,
оповещение персонала б) Только
визуальное отображение информации
в) Только совместимость с другими системами
безопасности г) Простота использования

20. Что необходимо учитывать при выборе технических средств физической защиты для обеспечения информационной безопасности предприятия?

а) Соответствие современным стандартам, возможность интеграции с
другими системами безопасности
б) Только цветовое воспроизведение
в) Наличие красочной инструкции по
эксплуатации
г) Простота монтажа

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	в	б	б	б
2	б	в	в	г
3	в	б	б	г
4	б	г	в	б
5	в	б	в	в
6	в	б	а	б
7	б	б	а	в
8	б	г	б	б
9	б	б	в	б
10	а	б	б	б
11	в	в	в	в
12	в	в	в	в
13	б	а	г	б
14	б	г	б	а
15	б	б	б	г
16	а	г	б	а
17	б	б	г	б
18	а	б	а	б
19	б	а	б	а
20	а	б	а	а

Вопросы ко 2-ой рубежной аттестации

1. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.
2. Общие принципы обеспечения безопасности объектов.
3. Жизненный цикл системы физической защиты.
4. Принципы построения интегрированных систем охраны.
5. Классификация и состав интегрированных систем охраны.
6. Требования к инженерным средствам физической защиты.
7. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.
8. Информационные основы построения системы охранной сигнализации.
9. Назначение, классификация технических средств обнаружения.
10. Построение систем обеспечения безопасности объекта)
11. Периметровые средства обнаружения: назначение, устройство, принцип действия.
12. Назначение объектовых средств обнаружения.

Итоговые тестовые задания по МДК. 03. 02 «Инженерно-технические средства физической защиты объектов информатизации»

(ОК 1-ОК 9, ПК 3.5)

Вариант № 1 (ОК 1-ОК 9, ПК 3.5)

1. Основной функцией инженерно-технических средств физической защиты является...

(ПК 3.5) (ОК 1, ОК 2)

A) мониторинг финансовых операций

B) обеспечение устойчивой работы информационной системы

C) регистрация информации в журнале учета

D) физическая охрана объектов и исключение несанкционированного доступа

2. Какой из перечисленных видов инженерно-технических средств используется для предотвращения проникновения на объект?

(ПК 3.5) (ОК 1, ОК 3)

A) кассовые аппараты

B) молниезащиту

C) ограждения и решетки

D) смартфоны сотрудников

3. Средствами какого класса называются устройства, предназначенные для охраны периметра территории?

(ПК 3.5) (ОК 1, ОК 4)

A) преграды и препятствия

B) видеонаблюдение и аудиозапись

C) датчики движения и звуковые сирены

D) огнетушители и системы пожаротушения

4. Для какой цели устанавливается оборудование мониторинга состояния инженерных систем объекта?

(ПК 3.5) (ОК 1, ОК 5)

A) регистрация перемещения транспортных средств

B) контроль расхода электроэнергии

C) обнаружение отклонений в функционировании инженерных систем и предотвращение аварийных ситуаций

D) визуализация архитектурных решений здания

5. Основное назначение инженерно-технического средства — электромеханического замка:

(ПК 3.5) (ОК 1, ОК 6)

A) задержка открывания двери

B) управление доступом и контроль за открытием дверных проемов

C) включение сигнальной тревоги при попытке взлома

D) хранение и обработка биометрических данных

6. Что из перечисленного не является средством инженерно-технической защиты объекта?

(ПК 3.5) (ОК 1, ОК 7)

A) видеокамеры наружного наблюдения

B) электронные замки с дистанционным управлением

C) подвесные потолки и фальшполы

D) заграждения вдоль периметра территории

7. Основными характеристиками надежного инженерно-технического средства защиты являются:

(ПК 3.5) (ОК 1, ОК 3)

A) эстетика и эргономичность

B) надежность, долговечность и простота эксплуатации

C) большой ассортимент цветов и материалов

D) цена и бренд производителя

8. Зачем используются стационарные металлодетекторы на входе в здание?

(ПК 3.5) (ОК 1, ОК 4)

A) обнаружение металлических предметов, потенциально представляющих опасность

B) запрет курения на территории учреждения

C) открывание автоматических дверей

D) контроль перемещения материальных ценностей

9. Какая категория инженерно-технических средств относится к контролю и управлению доступом?

(ПК 3.5) (ОК 1, ОК 5)

A) освещённость улиц

B) замки и турникеты

C) цветники и клумбы

D) медицинские аптечки первой помощи

10. Основным элементом инженерно-технической защиты помещения служит: **(ПК 3.5) (ОК 1, ОК 6)**

A) декор интерьера и элементы дизайна

B) установка видеокамер и охранной сигнализации

C) система кондиционирования воздуха

D) общедомовая электросеть

11. Назовите основное назначение инженерно-технических средств физической защиты. **(ПК 3.5) (ОК 1, ОК 2)**

---

12. Какие инженерно-технические средства обеспечивают физическую защиту объектов информатизации от стихийных бедствий?
(ПК 3.5) (ОК 1, ОК 7)

---

13. Какие инженерно-технические средства используются для обеспечения физической защиты объектов информатизации?
(ПК 3.5) (ОК 1, ОК 3)

A) камеры видеонаблюдения

B) средства пожаротушения

C) ограждения территории

D) фильтры электромагнитных волн

14. Какие инженерно-технические средства относят к средствам физической защиты информации?
(ПК 3.5) (ОК 1, ОК 4)

A) ограждения и заборы

B) видеонаблюдение и системы сигнализации

C) интеркомы и переговорные устройства

D) замки и турникеты

15. Какие инженерно-технические средства формируют систему защиты периметра объекта? **(ПК 3.5) (ОК 1, ОК 5)**

A) ворота и контрольно-пропускные пункты

B) штативы для камер видеонаблюдения

C) заборы и ограждения

D) электротехнические приспособления

16. Какие инженерно-технические средства обеспечивают охрану периметра объекта? **(ПК 3.5) (ОК 1, ОК 7)**

A) заборы и ограждения

B) видеокамеры

C) датчики движения

D) парковые скамьи

17. Какие инженерно-технические средства могут использоваться для защиты объекта от несанкционированного доступа?
(ПК 3.5) (ОК 1, ОК 3)

A) шлагбаумы

B) ограждения

C) курортные путевки

D) датчики присутствия

18. Соотнесите инженерно-технические средства с их назначением:

(ПК 3.5) (ОК 1, ОК 6)

Средства защиты:

1. Видеокамеры наружного наблюдения
2. Ограждения территории
3. Замки и турникеты
4. Системы пожаротушения

Назначение:

A. контроль доступа и передвижений персонала
B. обнаружение незаявленных лиц и транспорта
C. обеспечение физической неприступности территории
D. быстрое тушение очагов возгорания

19. Расположите инженерно-технические средства в порядке возрастания сложности эксплуатации:
(ПК 3.5) (ОК 1, ОК 7)

Средства защиты:

1. обычные механические замки
2. система видеонаблюдения с распознаванием лиц
3. электронные ключи и карточки доступа
4. средства контроля периметра с датчиками инфракрасного излучения

20. Установите соответствие между видом инженерно-технических средств и их функциями: **(ПК 3.5) (ОК 1, ОК 3)**

Зона защиты:

1. территория объекта
2. входная группа здания

3. внутри помещений
4. внешний периметр территории

Средства защиты:

A. электронные замки и карты доступа
B. видеонаблюдение и контроль доступа
C. ограждения и въездные ворота
D. инфракрасные датчики и тепловизоры

Вариант № 2 (ОК 1-ОК 9, ПК 3.5)

1. Инженерно-техническими средствами физической защиты объектов информатизации являются:
(ПК 3.5) (ОК 1, ОК 2)

A) кабельная продукция и разъёмы для подключения периферийных устройств

B) сигнализации, замки, системы видеонаблюдения и охранные системы

C) рабочие станции и ноутбуки сотрудников

D) сервисы удаленного доступа и подключение к облачным хранилищам

2. Главной целью инженерно-технических средств физической защиты объектов является:
(ПК 3.5) (ОК 1, ОК 3)

A) экономия электроэнергии и оптимизация расходов на содержание объектов

B) повышение комфорта сотрудников и улучшение эргономики рабочей обстановки

C) обеспечение физической безопасности и исключение несанкционированного доступа

D) реклама услуг и продвижение бренда компании

3. Какие инженерно-технические средства предназначены для охраны территории объекта?
(ПК 3.5) (ОК 1, ОК 4)

A) интерьерные украшения и декор помещений

B) средства санитарной гигиены и дезинфекции

C) заборы, ворота и видеонаблюдение

D) температурный контроль и отопление помещений

4. Основные задачи инженерно-технических средств физической защиты заключаются в:
(ПК 3.5) (ОК 1, ОК 5)

A) обеспечении комфортного пребывания на рабочем месте

B) максимальном увеличении продуктивности сотрудников

C) управлении финансовыми потоками и бюджетом организации

D) защите объекта от несанкционированного проникновения и преступных посягательств

5. Какой инженерно-технический инструмент позволяет оперативно реагировать на случаи несанкционированного проникновения?
(ПК 3.5) (ОК 1, ОК 6)

A) кассовый аппарат

B) видеокамеры с распознаванием лиц

C) тачскрин мониторы

D) алкогольный датчик дыхания водителей

6. Какая категория инженерно-технических средств применяется для блокировки доступа на объект?
(ПК 3.5) (ОК 1, ОК 7)

A) живописные картины на стенах офисов

B) парящие скульптуры в холле здания

C) запорные устройства и электрозамки

D) многоуровневые подвалы и подземные переходы

7. Основная цель инженерно-технических средств физической защиты заключается в:
(ПК 3.5) (ОК 1, ОК 3)

A) продвижении инноваций и улучшении имиджа компании

B) защите территории и информации от преступных посягательств

C) организации удобного транспортного сообщения сотрудников

D) обучении сотрудников новым профессиональным компетенциям

8. Какие инженерно-технические средства призваны обеспечить безопасность на объекте?
(ПК 3.5) (ОК 1, ОК 4)

A) системы охраны периметра и видеонаблюдения

B) садово-парковые насаждения и газоны

C) озвучивание и музыкальное сопровождение

D) автомобильные парковки и гаражи

9. Какие инженерно-технические средства физической защиты представляют собой системы предупреждения о нарушении периметра?
(ПК 3.5) (ОК 1, ОК 5)

A) орхидеи и домашние растения

B) декоративные водоемы и фонтаны

C) инфракрасные датчики и видеокамеры

D) семейные альбомы и фотографии на стене

10. Какие инженерно-технические средства применяются для охраны объектов информатизации?
(ПК 3.5) (ОК 1, ОК 6)

A) ограждения, турникеты и видеонаблюдение

B) экскурсионные туры и выставки экспонатов

C) салюты и фейерверки праздничных мероприятий

D) школьные учебники и тетради студентов

11. Назовите хотя бы два примера инженерно-технических средств физической защиты объектов информатизации.
(ПК 3.5) (ОК 1, ОК 2)

---

12. Какое инженерно-техническое средство помогает контролировать движение автотранспорта на территории объекта?
(ПК 3.5) (ОК 1, ОК 7)

---

13. Какие инженерно-технические средства составляют основу физической защиты объекта?
(ПК 3.5) (ОК 1, ОК 3)

A) средства противопожарной защиты

B) видеонаблюдение и охранные сигнализации

C) элементы ландшафтного дизайна и озеленения

D) системы контроля доступа и охранные турникеты

14. Какие инженерно-технические средства отвечают за безопасность объектов информатизации?
(ПК 3.5) (ОК 1, ОК 4)

A) видеокамеры наружные и внутренние

B) заборы и специальные ограждения территории

C) печати и штампы организаций

D) замки механического и электрического типа

15. Какие инженерно-технические средства поддерживают высокий уровень безопасности на объекте?
(ПК 3.5) (ОК 1, ОК 5)

A) тележки и стеллажи для перевозки грузов

B) форменная одежда сотрудников охраны

C) сигнализация и камеры видеонаблюдения

D) средства оперативной связи и связь двусторонняя

16. Соотнесите инженерно-технические средства с областью их применения:
(ПК 3.5) (ОК 1, ОК 6)

Средства защиты:

1. система видеонаблюдения
2. ограждения и ворота
3. встроенные датчики движения

4. запирающие устройства и замок

Область применения:

A. контроль доступа в помещения
B. охрана периметра территории
C. наблюдение за территорией и зданием
D. обнаружение перемещений внутри помещения

17. Распределите инженерно-технические средства по группам сложности эксплуатации: **(ПК 3.5) (ОК 1, ОК 7)**

Средства защиты:

1. механические замки и задвижки
2. умные системы видеонаблюдения с распознаванием лиц
3. электронные карточные системы доступа
4. средства контроля периметра с ИК-датчиками

18. Установите соответствие между инженерно-техническими средствами и их функциями: **(ПК 3.5) (ОК 1, ОК 3)**

Зона защиты:

1. территория объекта
2. входная группа здания
3. внутри помещений
4. внешний периметр территории

Средства защиты:

A. электронные замки и карты доступа
B. видеонаблюдение и контроль доступа
C. ограждения и въездные ворота
D. инфракрасные датчики и тепловизоры

19. Какие инженерно-технические средства применяются для физической защиты объектов информатизации?
(ПК 3.5) (ОК 1, ОК 4)

A) ограждения и системы видеонаблюдения

B) механические и электронные замки

C) гардеробы и вешалки для верхней одежды

D) автоматические шлюзы и турникеты

20. Какие инженерно-технические средства помогают обеспечивать безопасность офисных пространств?

(ПК 3.5) (ОК 1, ОК 5)

A) средства пожаротушения и сигнализации

B) замки с цифровым кодом доступа

C) мероприятия культурно-развлекательного характера

D) видеонаблюдение и системы контроля доступа

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2
1	D	B
2	C	C
3	A	C
4	C	D
5	B	B
6	C	C
7	B	B
8	A	A
9	B	C
10	B	A
11	Обеспечение физической защиты объектов и предотвращение несанкционированного доступа.	Видеокамеры видеонаблюдения, электронные замки, турникеты, системы сигнализации.
12	Ограждения, герметизация помещений, укрепление строительных конструкций, водонепроницаемая изоляция.	Автоматические шлагбаумы, парковочные системы, видеонаблюдение.
13	A, B, C	A, B, D
14	A, B, D	A, B, D
15	A, C	C, D
16	A, B, C	1—C, 2—B, 3—D, 4—A
17	A, B, D	1—3—4—2
18	1—B, 2—C, 3—A, 4—D	1—B, 2—A, 3—A, 4—C
19	1—3—4—2	A, B, D
20	1—B, 2—A, 3—A, 4—C	A, B, D

3.7. Типовые задания для промежуточного контроля по

МДК.03. 02 Инженерно-технические средства физической защиты объектов информатизации

1)Вопросы для подготовки к дифференцированному зачету

1. Инженерно-техническая защита
2. Физические средства
3. Аппаратные средства
4. Программные средства
5. Криптографические средства
6. ПК на предмет определения максимального расстояния, при котором информацию можно снять с ПК, физически не подключаясь к нему;
7. Оценивается система видеонаблюдения помещения, где расположен сервер;
8. Проверяются помещения, предназначенные для переговоров, на предмет наличия различных подслушивающих устройств;
9. Производится установка специального оборудования, призванного распознавать подслушивающие устройства
10. Утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности
11. Детекторы, индикаторы поля и тест-приёмники;
12. Анализаторы проводных коммуникаций;
13. Многофункциональные поисковые приборы;
14. Обнаружители скрытых видеокамер;
15. Нелинейные локаторы;
16. Комплексы радиомониторинга и пеленгования;
17. Средства защиты от утечки акустической информации;
18. Устройства противодействия радиоэлектронным средствам негласной аудиозаписи;
19. Устройства блокирования работы систем проводной, мобильной связи и передачи данных;
20. Устройства защиты от прослушивания телефонных переговоров;
21. Устройства защиты от утечки информации по цепям электропитания (фильтры помехоподавляющие электрические) и заземления;
22. Устройства защиты от утечки информации по каналам ПЭМИН;
23. Устройства хранения, копирования, уничтожения и восстановления информации;
24. Цифровые системы регистрации, звукозаписи и шумоочистки речевых сигналов;
25. Металлодетекторы ручные досмотровые;
26. Металлоискатели поисковые грунтовые, глубинные;
27. Металлодетекторы арочные стационарные досмотровые;
28. Программных средств сбора, анализа и обработки информации;
29. Радиоэкранирующих и радиопоглощающих материалов шумопоглощающих материалов.
30. Комплексное использование технических, программных и организационных средств
31. Информация как объект защиты
32. Требования к защищенности информации
33. Организационные меры защиты информации
34. Оценка вероятного противника
35. Оценка условий решения задачи защиты информации
36. Инженерно-технические меры защиты информации
37. Системы информационной безопасности
38. Принципы построения систем безопасности

39. Защита компьютерной информации
40. Угрозы несанкционированного доступа в сеть
41. Системы информационной безопасности сети
42. Принципы построения систем безопасности сети
43. Аппаратные средства защиты передаваемых данных
44. Разработка системы управления объектом защиты и безопасности
45. Постановка задачи проектирования
46. Анализ объекта защиты
47. Контролируемая зона
48. Возможные каналы утечки информации
49. Разработка политики защиты контролируемой зоны
50. Обеспечение защиты помещения проведения совещаний
51. Обеспечение защиты помещения руководителя
52. Обеспечение защиты помещения серверной
53. Разработка политики безопасности сети и коммуникаций
54. Интернет-шлюз + файерволл как основа системы управления
55. Выбор и конфигурирование аппаратных средств защиты данных
56. Защита данных средствами защиты информации и специального ПО
57. Описание настройки специального программного обеспечения защиты данных
58. Моделирование объектов защиты.

4. Требования к дифференцированному зачету по учебной и (или) производственной практике

Дифференцированный зачет по учебной и (или) производственной практике выставляется с учетом данных аттестационного листа (характеристики профессиональной деятельности обучающегося/студента на практике) с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика.

4.1. Оценочные материалы

Перечень вопросов к собеседованию по производственной практике

1. Краткая характеристика места практики
2. Требования по защите персональных данных
3. Требования по защите конфиденциальных данных предприятия
4. Системы контроля и управления доступом на предприятии
5. Способы ограничения доступа к информации
6. Признаки наличия вредоносного программного обеспечения
7. Средства защиты информации в компьютерных сетях
8. Средства обнаружения компьютерных атак
9. Способы предупреждения компьютерных атак
10. Программно-аппаратные средства уничтожения информации и носителей информации

4.2. Форма аттестационного листа (из дневника по практике)

АТТЕСТАЦИОННЫЙ ЛИСТ ПО УЧЕБНОЙ/ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

_____

ФИО обучающегося

обучающийся (аяся) на ____ курсе по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем успешно прошел(ла) учебную/производственную практику по профессиональному модулю **ПМ.03 «Защита информации техническими средствами»**

в объеме _____с «___» _____20__г. по «___» _____20___г.

в организации /на предприятии _____

наименование организации/предприятии, юридический адрес

Виды и качество выполнения работ

Виды работ, выполненных обучающимся(ейся) во время практики	Объем работ	Качество выполнения работ (оптимальный/средний/ допустимый уровень)
Итого		

Руководитель от предприятия

_____

(должность, фамилия, имя, отчество)

Дата _____ _____ /_____/

(*подпись*) *Расшифровка подписи*

Руководитель практики от ГБПОУ РД «КППК»

_____

(должность, фамилия, имя, отчество)

5. Структура контрольно-оценочных материалов для экзамена (квалификационного) Типовое задание для экзаменующегося

Текст задания:

Научно-внедренческое предприятие «Телесистемы» занимается прокладкой компьютерных сетей и разработкой программных комплексов для организаций нашего города. Численность работников в организации «Телесистемы» – примерно 80 человек. Одновременно находится в разработке до 30 проектов. Один разработчик может участвовать в нескольких проектах одновременно, степень секретности для каждого проекта индивидуальна. Одна организация может заказать в «Телесистемах» несколько разработок. В связи с большой востребованностью создаваемых программных продуктов, а также с появлением новых конкурирующих фирм, предоставляющих аналогичные услуги, охране и защите коммерческих секретов уделено усиленное внимание.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 **Данных о защищаемой информации.**

№ Эл. инф.	Элементы информации	Гриф КИ	Цена инф, руб.	Носитель информации	Местоположение источника информации

Создайте модель защиты в Visio.

3.4 Контрольно-оценочные средства для проведения экзамена (квалификационного)

3.4.1 Общие положения

Экзамен (квалификационный) предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.03 «Защита информации техническими средствами».

Экзамен включает: практический экзамен. Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/ не освоен». Условием положительной аттестации (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемых показателям, а также общих компетенций. Условием допуска к экзамену (квалификационному) является положительная аттестация по текущему контролю (защита контрольных работ, тестирование, защита ЛПЗ, решение ситуационных задач) и по промежуточному (МДК.03.01, МДК.03.02, учебной практике УП.03 и производственной практике (по профилю специальности ПП.03).

ГБПОУ РД «Кизлярский профессионально-педагогический колледж»

Рассмотрено на заседании методического совета протокол №____	**Экзаменационный билет №1** ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ	«УТВЕРЖДАЮ» Зам. директора по УПР « » _____ 202__г.

Инструкция:

1. Внимательно прочитайте задание.
2. Спланируйте вашу работу.
3. Создайте **рабочую папку** с Вашей фамилией и инициалами (например: Ахмедов А.М.) на *Рабочем столе* для размещения в ней работы.

Вы можете воспользоваться:

1. предоставленной литературой, а также справочной системой программного обеспечения.

Время выполнения задания – 60 мин.

Задание №1:

Внимательно прочитайте задание.

Текст задания:

Научно-внедренческого предприятия «Звезда» занимается прокладкой компьютерных сетей и разработкой программных комплексов для организаций нашего города. Численность работников в «Звезда» – примерно 80 человек. Одновременно находится в разработке до 30 проектов. Один разработчик может участвовать в нескольких проектах одновременно, степень секретности для каждого проекта индивидуальна. Одна организация может заказать в «Звезда» несколько разработок. В связи с больший востребованностью создаваемых программных продуктов, а также с появлением новых конкурирующих фирм, предоставляющих аналогичные услуги, охране и защите коммерческих секретов уделено усиленное внимание.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры

, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а nый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

4. Создайте модель защиты в CorelDRAW.

Задание №2:

Внимательно прочитайте задание.Создайте документ в Microsoft Word, напишите номер теста и напротив букву ответа (например, 1-d).

1. Какие основные угрозы могут быть связаны с технической защитой информации?

a) Вирусы и вредоносные программы

b) Физическое повреждение оборудования

c) Несанкционированный доступ к данным

d) Все перечисленное выше

2. Что такое уровень целостности данных?

a) Способность данных быть доступными только для авторизованных пользователей

b) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения

c) Способность данных быть достоверными и точными

d) Способность данных быть сохраненными и доступными в случае сбоя системы

3. Что такое политика безопасности информации?

a) Набор правил и регуляций, определяющих принципы и стратегию защиты информации

b) Программное обеспечение для контроля и мониторинга доступа к информации

c) Способность системы автоматически обнаруживать и предотвращать вторжения d) Все перечисленное выше

4. Какая роль играет обучение пользователей в обеспечении технической защиты информации?

a) Обучение помогает пользователям понять основные принципы безопасности и правила использования информационных систем

b) Обучение не играет роли в обеспечении технической защиты информации

c) Обучение позволяет пользователям настроить системные параметры для повышения безопасности

d) Обучение помогает идентифицировать и предотвращать кибератаки

5. Какие методы технической защиты информации могут использоваться для предотвращения несанкционированного доступа? a) Аутентификация и авторизация

b) Фильтрация сетевого трафика

c) Контроль доступа к системным ресурсам

d) Все перечисленное выше

ГБПОУ РД «Кизлярский профессионально-педагогический колледж»

Рассмотрено на заседании методического совета протокол №____	**Экзаменационный билет №1** ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ	«УТВЕРЖДАЮ» Зам. директора по УПР « » _____ 202__г.

Инструкция:

1. Внимательно прочитайте задание.
2. Спланируйте вашу работу.
3. Создайте **рабочую папку** с Вашей фамилией и инициалами (например: Ахмедов А.М.) на *Рабочем столе* для размещения в ней работы.

Вы можете воспользоваться:

1. предоставленной литературой, а также справочной системой программного обеспечения.

Время выполнения задания – 60 мин.

Задание №1:

Внимательно прочитайте задание.

Текст задания:

Судоходной компании «Балтика» занимается перевозками грузов между континентами. В ее собственности несколько десятков судов различного класса и грузоподъемности. К услугам этой компании обращаются тысячи клиентов из различных стран мира. Судно следует по маршруту. Маршрут разрабатывается главным менеджером компании и проходит через несколько портов. В очередном порту назначения производится лишь частичная погрузка и выгрузка грузов, и судно следует дальше. Компания имеет в своей собственности складские зоны. Все эти зоны разделены между собой. В связи с большим количеством конкурирующих фирм, охране и защите коммерческих секретов, связанных со статусом груза и маршрутом следования, уделено усиленное внимание.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Задание №2:

Внимательно прочитайте задание. Создайте документ в Microsoft Word, напишите номер теста и напротив букву ответа (например, 1-d).

1. Что такое антивирусное программное обеспечение?

a) Программное обеспечение для защиты систем от вирусов

b) Программное обеспечение для шифрования данных

c) Программное обеспечение для контроля доступа

d) Программное обеспечение для аутентификации пользователей

2. Что такое бекапирование (резервное копирование) данных?

a) Процесс сохранения копии данных для их восстановления в случае потери или повреждения

b) Процесс шифрования данных для защиты их от несанкционированного доступа

c) Процесс аутентификации пользователей перед предоставлением им доступа к данным

d) Процесс контроля доступа к системным ресурсам

3. Какие меры безопасности могут быть связаны с физическими преградами?

a) Установка видеонаблюдения и систем контроля доступа

b) Использование мощных шифровальных алгоритмов для защиты данных

c) Усиление физической защиты зданий и помещений

d) Все перечисленное выше

4. Что такое техническая защита информации?

a) Защита информации с использованием криптографических методов

b) Защита информации с использованием технических, программных и программнотехнических средств

c) Защита информации с использованием физических преград

d) Защита информации с использованием социальных мер безопасности

5. **Какие задачи решает техническая защита информации?**

a) Предотвращение утечки информации через технические каналы утечки информации

b) Предотвращение несанкционированного доступа к информации

c) Обеспечение целостности, конфиденциальности и доступности защищаемой информации

d) Все перечисленное выше

ГБПОУ РД «Кизлярский профессионально-педагогический колледж»

Рассмотрено на заседании методического совета протокол №____	**Экзаменационный билет №1** ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ	«УТВЕРЖДАЮ» Зам. директора по УПР « » _____ 202__г.

Инструкция:

1. Внимательно прочитайте задание.
2. Спланируйте вашу работу.
3. Создайте **рабочую папку** с Вашей фамилией и инициалами (например: Ахмедов А.М.) на *Рабочем столе* для размещения в ней работы.

Вы можете воспользоваться:

1. предоставленной литературой, а также справочной системой программного обеспечения.

Время выполнения задания – 60 мин.

Задание №1:

Внимательно прочитайте задание.

Текст задания:

ООО «Киновидеопрокат», является почти полным монополистом относительно посреднических услуг в сфере кинобизнеса. Отдел маркетинга, изучив ситуацию на рынке кинофильмов, принимает решение о покупке тех или иных кинолент. Отдел закупок претворяет эти решения в жизнь, причем лента может быть куплена как у производителя, так и у посредника. Отдел аренды «Киновидеопроката» сдает закупленные фильмы кинотеатрам города в аренду. В 31 связи с возникающей больший конкуренцией охране и защите коммерческих секретов уделено усиленное внимание.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Задание №2:

Внимательно прочитайте задание. Создайте документ в Microsoft Word, напишите номер теста и напротив букву ответа (например, 1-d).

1. Кто является регулятором в области обеспечения технической защиты информации в Российской Федерации?

a) Федеральная служба по техническому и экспортному контролю

b) Федеральная служба безопасности

c) Министерство обороны

d) Министерство связи и массовых коммуникаций

2. Что может являться объектом технической защиты информации?

a) Объект информатизации

b) Информационная система/автоматизированная система

c) Ресурсы информационной системы/автоматизированной системы

d) Все перечисленное выше

3. Какие основные цели имеет техническая защита информации?

a) Обеспечение целостности информации

b) Обеспечение конфиденциальности информации

c) Обеспечение доступности информации

d) Все перечисленное выше

4. Какие методы могут использоваться для обеспечения технической защиты информации?

a) Физические преграды

b) Криптографические методы

c) Технические средства

d) Все перечисленное выше

5. Какие определения информации существуют?

a) Единственное формальное определение информации

b) Множество определений информации в зависимости от контекста

c) Определение информации, основанное на законах информатики

d) Определение информации, основанное на социологии

ГБПОУ РД «Кизлярский профессионально-педагогический колледж»

Рассмотрено на заседании методического совета протокол №____	**Экзаменационный билет №2** ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ	«УТВЕРЖДАЮ» Зам. директора по УПР « » _____ 202__г.

Инструкция:

1. Внимательно прочитайте задание.
2. Спланируйте вашу работу.
3. Создайте **рабочую папку** с Вашей фамилией и инициалами (например: Ахмедов А.М.) на *Рабочем столе* для размещения в ней работы. **Вы можете воспользоваться**:

1. предоставленной литературой, а также справочной системой программного обеспечения.

Время выполнения задания – 60 мин.

Задание №1:

Внимательно прочитайте задание.

Текст задания:

Торгово-посредническая фирма «Столица». Бизнес этого предприятия предельно прост: «покупай дешевле – продавай дороже», или состыкуй продавца и покупателя и получи «комиссионные». Основной упор фирма делает на закупки продуктов питания в других регионах страны и за рубежом – там, где они производятся и стоят дешевле, чем в нашем регионе. Часть продукции может быть закуплена и у местных продавцов. В этом случае фирма получает прибыль за счет того, что крупные партии товара стоят дешевле, чем мелкие. Так как в данной сфере количество фирм на сегодняшний день увеличивается, то маркетинговой политики предприятия охраняется как службой безопасности, так и лично руководством.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Задание №2:

Внимательно прочитайте задание.

Создайте документ в Microsoft Word, напишите номер теста и напротив букву ответа (например, 1-d).

1. Какие принципы включает в себя техническая защита информации?

a) Принцип обязательности

b) Принцип целесообразности

c) Принцип градации мер безопасности

d) Все перечисленное выше

2. Какие основные категории угроз информационной безопасности существуют?

a) Технические угрозы

b) Организационные угрозы

c) Персональные угрозы

d) Все перечисленное выше

3. Какие виды ресурсов информационной системы могут подлежать защите?

a) Аппаратные ресурсы

b) Программные ресурсы

c) Информационные ресурсы

d) Все перечисленное выше

4. Какие преимущества обеспечения безопасности сетевых соединений с помощью виртуальных частных сетей (VPN)?

a) Шифрование данных для защиты конфиденциальности

b) Обеспечение анонимности пользователя

c) Позволяет подключаться к защищенным сетям удаленно

d) Предотвращение перехвата данных в общественных Wi-Fi сетях

5. Что такое защита от атак по сети и почему она важна?

a) Обеспечение безопасности сетевых соединений и защита от несанкционированного доступа

b) Защита от физических угроз и контроль доступа в помещения

c) Шифрование данных и защита от вредоносного программного обеспечения

d) Отслеживание активности пользователей и аудит безопасности

ГБПОУ РД «Кизлярский профессионально-педагогический колледж»

Рассмотрено на заседании методического совета протокол №____	**Экзаменационный билет №3** ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ	«УТВЕРЖДАЮ» Зам. директора по УПР « » _____ 202__г.

Инструкция:

1. Внимательно прочитайте задание.
2. Спланируйте вашу работу.
3. Создайте **рабочую папку** с Вашей фамилией и инициалами (например: Ахмедов А.М.) на *Рабочем столе* для размещения в ней работы.

Вы можете воспользоваться:

1. предоставленной литературой, а также справочной системой программного обеспечения.

Время выполнения задания – 60 мин.

Задание №1:

Внимательно прочитайте задание.

Текст задания:

Рассмотреть работу отдела кадров университета, в которой находятся данные всех сотрудников: от преподавателя до ректора, и их трудовой деятельности. Также в отделе 32 кадров хранится информация о трудовой деятельности сотрудника: о предыдущих местах работы, сроке работы и предприятии. Отдел кадров занимается подготовкой трудовых договоров с преподавателями после избрания их по конкурсу на очередной срок. Также в его ведении находятся сведения о наложении взысканий на сотрудников и их поощрениях, часть данных не имеет общего права доступа. Взыскания в трудовую книжку не заносятся, а хранятся в электронном виде.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Задание №2:

Внимательно прочитайте задание.Создайте документ в Microsoft Word, напишите номер теста и напротив букву ответа (например, 1-d).

1. Какие основные угрозы могут быть связаны с технической защитой информации?

a) Вирусы и вредоносные программы

b) Физическое повреждение оборудования

c) Несанкционированный доступ к данным

d) Все перечисленное выше

2. Что такое уровень целостности данных?

a) Способность данных быть доступными только для авторизованных пользователей

b) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения

c) Способность данных быть достоверными и точными

d) Способность данных быть сохраненными и доступными в случае сбоя системы

3. Что такое политика безопасности информации?

a) Набор правил и регуляций, определяющих принципы и стратегию защиты информации

b) Программное обеспечение для контроля и мониторинга доступа к информации

c) Способность системы автоматически обнаруживать и предотвращать вторжения d) Все перечисленное выше

4. Какая роль играет обучение пользователей в обеспечении технической защиты информации?

a) Обучение помогает пользователям понять основные принципы безопасности и правила использования информационных систем

b) Обучение не играет роли в обеспечении технической защиты информации

c) Обучение позволяет пользователям настроить системные параметры для повышения безопасности

d) Обучение помогает идентифицировать и предотвращать кибератаки

5. Какие методы технической защиты информации могут использоваться для предотвращения несанкционированного доступа? a) Аутентификация и авторизация

b) Фильтрация сетевого трафика

c) Контроль доступа к системным ресурсам

d) Все перечисленное выше

ГБПОУ РД «Кизлярский профессионально-педагогический колледж»

Рассмотрено на заседании методического совета протокол №____	**Экзаменационный билет №3** ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ	«УТВЕРЖДАЮ» Зам. директора по УПР « » _____ 202__г.

Инструкция:

1. Внимательно прочитайте задание.
2. Спланируйте вашу работу.
3. Создайте **рабочую папку** с Вашей фамилией и инициалами (например: Ахмедов А.М.) на *Рабочем столе* для размещения в ней работы.

Вы можете воспользоваться:

1. предоставленной литературой, а также справочной системой программного обеспечения.

Время выполнения задания – 60 мин.

Задание №1:

Внимательно прочитайте задание.

Текст задания:

Фармацевтическая компания занимается производством и оптовой продажей лекарств больницам и аптекам города. В ее ассортименте – тысячи наименований лекарств, а также различных аптечных принадлежностей (градусники, шприцы, бинты и т. д.) Возможна продажа лишь тех лекарств, которые одобрены Минздравом РФ, т. е. имеют регистрационный номер Минздрава РФ. Поступающие лекарства сопровождаются документами – приходными накладными ведомостями. Имеются наркосодержащие лекарства, доступ к работе с ними имеют возможности, только работники, имеющие допуск. Допуск к данным о сроках покупок и доставок такой продукции строго ограничен, склады с такими лекарствами охраняются службой безопасности, также усилено охраняется рецептура производимых лекарств.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Задание №2:

Внимательно прочитайте задание.Создайте документ в Microsoft Word, напишите номер теста и напротив букву ответа (например, 1-d).

1. Какие методы защиты от атак по сети могут использоваться?

a) Файрволлы, сетевые прокси, виртуальные частные сети (VPN)

b) Антивирусное программное обеспечение, межсетевые экраны, IDS/IPS

c) Шифрование данных, аутентификация и контроль доступа

d) Межсетевые экраны, виртуальные частные сети (VPN), IDS/IPS

2. Что такое защита от вредоносного программного обеспечения и какие методы защиты можно применить?

a) Обеспечение безопасности от вирусов, троянов и других вредоносных программ

b) Аутентификация и шифрование данных

c) Контроль доступа и мониторинг активности пользователей

d) Физическая защита и контроль угроз в реальном времени

3. Что такое аудит безопасности и какая роль у него в обеспечении информационной безопасности?

a) Систематическая оценка и проверка безопасности информационных систем

b) Предотвращение хищения и утечек конфиденциальной информации

c) Мониторинг и обнаружение вторжений и несанкционированной активности

d) Определение уязвимостей и предотвращение атак по сети

4. Какие основные меры безопасности могут помочь защитить информацию от угроз в реальном времени?

a) Бэкап данных, контроль доступа и шифрование

b) Межсетевые экраны, IDS/IPS и аутентификация пользователей

c) Антивирусное программное обеспечение, файрволлы и виртуальные частные сети (VPN)

d) Физическая защита, контроль угроз и мониторинг активности **5. Что такое аутентификация и зачем она используется?**

a) Подтверждение подлинности и идентификация пользователей

b) Защита от вредоносного программного обеспечения

c) Шифрование конфиденциальной информации

d) Обеспечение целостности данных

ГБПОУ РД «Кизлярский профессионально-педагогический колледж»

Рассмотрено на заседании методического совета протокол №____	**Экзаменационный билет №4** ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ	«УТВЕРЖДАЮ» Зам. директора по УПР « » _____ 202__г.

Инструкция:

1. Внимательно прочитайте задание.
2. Спланируйте вашу работу.
3. Создайте **рабочую папку** с Вашей фамилией и инициалами (например: Ахмедов А.М.) на *Рабочем столе* для размещения в ней работы.

Вы можете воспользоваться:

1. предоставленной литературой, а также справочной системой программного обеспечения.

Время выполнения задания – 60 мин.

Задание №1:

Внимательно прочитайте задание.

Текст задания:

Туристическая компания «Вояж» формирует туристические группы для заграничных поездок и обеспечивает им полную поддержку на маршруте. Количество туристов в группе заранее известно и ограничено.

Маршрут группы может пролегать через несколько городов страны назначения. Вместе с группой следует представитель компании, который несет полную ответственность за качество услуг, предоставляемых компанией. Так как в данной сфере количество фирм на сегодняшний день увеличивается, то сохранностью и невозможностью легкого доступа к сведениям относительно туристов, а также сведения договоров охраняется как службой безопасности, так и лично руководством.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Задание №2:

Внимательно прочитайте задание.Создайте документ в Microsoft Word, напишите номер теста и напротив букву ответа (например, 1-d).

1. Какие методы аутентификации могут использоваться для проверки подлинности пользователя?

a) Логин и пароль, биометрические данные, одноразовые коды

b) Антивирусное программное обеспечение, файрволлы, VPN

c) Криптографические алгоритмы, сетевые протоколы, защитные меры

d) Контроль доступа, системы мониторинга, физические барьеры

2. Что такое авторизация и почему она важна в контексте информационной безопасности?

a) Проверка прав доступа пользователя к определенным ресурсам

b) Шифрование данных для защиты от несанкционированного доступа

c) Контроль целостности информации и предотвращение ее изменения

d) Анализ угроз и реагирование на них в реальном времени

3. Какие принципы безопасности помогают обеспечить аутентификацию и авторизацию пользователей?

a) Необходимость знания и секретность

b) Принцип наименьших привилегий и разделение обязанностей

c) Отслеживание активности и контроль доступа

d) Физическая безопасность и защита от внутренних угроз

4. Какой вид защиты информации является одним из видов инженерно-технической защиты?

a) Физическая защита

b) Криптографическая защита

c) Компьютерная защита

d) Юридическая защита

5. Что такое информационная безопасность?

a) Защита от хищения информации

b) Защита информационных технологий

c) Обеспечение конфиденциальности информации

d) Комплекс мер по предотвращению угроз информации

ГБПОУ РД «Кизлярский профессионально-педагогический колледж»

Рассмотрено на заседании методического совета протокол №____	**Экзаменационный билет №5** ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ	«УТВЕРЖДАЮ» Зам. директора по УПР _____ « » _____ 202__г.

Инструкция:

1. Внимательно прочитайте задание.
2. Спланируйте вашу работу.
3. Создайте **рабочую папку** с Вашей фамилией и инициалами (например: Ахмедов А.М.) на *Рабочем столе* для размещения в ней работы. **Вы можете воспользоваться**: 1. предоставленной литературой, а также справочной системой программного обеспечения. **Время выполнения задания** – 60 мин.

Задание №1:

Внимательно прочитайте задание.

Текст задания:

В собственности рекламного агентства «Rapid» находится примерно около сотни рекламных щитов, расположенных по всему городу. Установка их согласована с администрацией города, и все необходимые формальности выполнены. На этих щитах может быть размещена реклама по заказу любой организации города. Срок размещения, стоимость аренды щита и стоимость изготовления самой рекламы – договорные, условия договора строго конфиденциальны и индивидуальны для каждого партнера.

Договор размещения рекламы может быть продлен по взаимной договоренности сторон.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).
4. Создайте модель защиты в CorelDRAW.

Задание №2:

Внимательно прочитайте задание.

Создайте документ в Microsoft Word, напишите номер теста и напротив букву ответа (например, 1-d).

1. Какие основные принципы информационной безопасности существуют?

a) Конфиденциальность, целостность, доступность

b) Аутентификация, авторизация, аудит

c) Защита от внешних и внутренних угроз

d) Профилактика, реагирование, восстановление

2. Что представляют собой объекты защиты информации?

a) Физические лица, имеющие доступ к информации

b) Технические средства защиты информации

c) Компьютерные программы и алгоритмы

d) Материальные носители информации и информационные системы

3. Какие виды конфиденциальной информации выделяются в зависимости от области деятельности человека?

a) Служебная, профессиональная, промышленная, коммерческая, государственная, военная

b) Личная, рабочая, техническая, финансовая

c) Секретная, закрытая, открытая, публичная

d) Внутренняя, внешняя, секретная, публичная **4. Какими свойствами обладает информация?**

a) Масса, размеры, энергия

b) Физические параметры

c) Уникальность, отсутствие физических параметров

d) Существование только на материальном носителе

5. Какие объекты защиты информации существуют с точки зрения защиты?

a) Материальные средства

b) Материальные носители информации

c) Физические поля

d) Источники информации

4. КРИТЕРИИ ОЦЕНИВАНИЯ

Критерии оценивания(устный ответ):

«5» «отлично» или «зачтено» - студент показывает глубокое и полное овладение содержанием программного материала по ПМ, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» или «зачтено» - студент в полном объеме освоил программный материал по ПМ, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и

профессиональными компетенциями и готовность к профессиональной деятельности **«3» «удовлетворительно» или «зачтено»** - студент обнаруживает знание и понимание основных положений программного материала по ПМ но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» или «не зачтено» - студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по ПМ, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

Критерии оценивания(тестирование):

Индикаторы компетенции	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**отлично**

Полнота знаний	Уровень знаний ниже Минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.
Наличие умений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественны м недочетами, выполнены все 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	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	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.

		практических задач.	профессиональным задачам.	
Уровень сформирован-ности компетенций	Низкий	Ниже среднего	Средний	Высокий

5 . Критерии оценки промежуточной (итоговой) аттестации

При определении оценки необходимо исходить из следующих критериев:

Задания для дифзачёта обучающихся состоят из тестовых заданий и практической работы на компьютере.

Максимальное количество баллов, которые обучающийся может получить по результатам компьютерного тестирования в рамках промежуточной (итоговой) аттестации, составляет:

- На экзамене – 20 баллов,
- На дифференцированном зачете – 10 баллов.

Шкала оценивания: Экзамен

Количество баллов	**Отметка в 5 бальной системе**	**Качество усвоения предмета**
От 0 до 10	2	менее 50%
От 11 до 14	3	51%-70%
От 15 до 17	4	71%-85%
От 18 до 20	5	86%-100%

Шкала оценивания: Дифференцированный зачет (зачет)

Количество баллов	**Отметка в 5 бальной системе**	**Качество усвоения предмета**
От 0 до 5	2	менее 50%
От 6 до 7	3	51%-70%
От 8	4	71%-85%
От 9 до 10	5	86%-100%

Шкала оценивания: Дифференцированный зачет (зачет)

Количество баллов	**Отметка в 5 бальной системе**	**Качество усвоения предмета**
От 0 до 4	2	менее 40%
От 5 до 6	3	41%-60%
От 7 до 8	4	61%-80%

От 9 до 10	5	81%-100%

Список использованных источников:

Основные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2019.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2020.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018.
4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2018.

Электронные источники:

1. Введение в теоретико-числовые методы криптографии : учебное пособие для спо / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 396 с. — ISBN 978-5-507-45348-1. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/265178
2. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие для спо / Р. Н. Гилязова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 44 с. — ISBN 978-5-8114-9138-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/187645
3. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо

/ О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-47174-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/336200

Дополнительные источники:

1. Котеров Д.В. PHP 5 в подлиннике. – СПб.: БХВ-Петербург, 2018. – 1104 с.
2. Федеральный образовательный портал «Информационно -коммуникационные технологии в образовании». [Электронный ресурс] – Режим доступа: http://window.edu.ru/resource/832/7832.