

**ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»**

*Утвержден решением
Ученого совета ДГУНХ,
протокол № 11
от 30 мая 2024 г*

**КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ
«ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО
ТЕХНИЧЕСКИМ КАНАЛАМ»**

**Специальность 10.02.05 Обеспечение
информационной безопасности автоматизированных
систем**

Квалификация – техник по защите информации

Форма обучения – очная

УДК 65.012.45

ББК 73.73

Составитель – Эмирбеков Эльдар Меликович, старший преподаватель кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, к.ф.-м.н., доцент, зав. кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

Представитель работодателя–Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза».

Фонд оценочных средств разработан в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г., № 1553, в соответствии с приказом Минпросвещения России от 24.08.2022 г., № 762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования».

Фонд оценочных средств по дисциплине «Техническая защита информации» размещены на официальном сайте www.dgunh.ru

Эмирбеков Э.М. Фонд оценочных средств по дисциплине «Техническая защита информации» по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. – Махачкала: ДГУНХ, 2024 г.– 57 с.

Рекомендован к утверждению Учебно-методическим советом ДГУНХ 28 мая 2024 г.

Рекомендован к утверждению руководителем образовательной программы СПО – программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, к.пед.н., Гасановой З.А.

Одобен на заседании кафедры «Информационные технологии и информационная безопасность» 23 мая 2024 г., протокол № 10.

СОДЕРЖАНИЕ

Назначение оценочных материалов.....	4
РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины	5
1.1 Перечень формируемых компетенций.....	5
1.2 Перечень компетенций с указанием видов оценочных средств.....	5
РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине.....	14
РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.....	47
РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций.....	51
Лист актуализации оценочных материалов по дисциплине.....	57

Назначение оценочных материалов

Фонд оценочных средств для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Техническая защита информации» на соответствие их учебных достижений поэтапным требованиям соответствующей образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Фонд оценочных средств по дисциплине «Техническая защита информации» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Фонд оценочных средств сформированы на основе ключевых принципов оценивания:

- валидности: объекты оценки должны соответствовать поставленным целям обучения;
- надежности: использование единообразных стандартов и критериев для оценивания достижений;
- объективности: разные обучающиеся должны иметь равные возможности для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

- предметная направленность (соответствие предмету изучения конкретной дисциплины);
- содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);
- объем (количественный состав оценочных материалов);
- качество оценочных материалов в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины

1.1 Перечень формируемых компетенций

код компетенции	формулировка компетенции
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, создаваемых техническими средствами обработки информации ограниченного доступа
ПК-3.4.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

1.2. Перечень компетенций с указанием видов оценочных средств

<i>Формируемые компетенции</i>	<i>Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций</i>	<i>Уровни освоения компетенций</i>	<i>Критерии оценивания сформированности компетенций</i>	<i>Виды оценочных средств</i>
ПК-3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	<u>Знать:</u> - основные нормативные и методические документы в области технической защиты информации	Пороговый уровень	Обучающийся слабо (частично) знает основные нормативные и методические документы в области технической защиты информации	Блок А — задания репродуктивного уровня — тестовые задания; — вопросы для обсуждения
		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает основные	

<i>Формируемые компетенции</i>	<i>Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций</i>	<i>Уровни освоения компетенций</i>	<i>Критерии оценивания сформированности компетенций</i>	<i>Виды оценочных средств</i>
			нормативные и методические документы в области технической защиты информации	
		Продвину- тый уровень	Обучающийся с требуемой степенью полноты и точности знает основные нормативные и методические документы в области технической защиты информации	
	Уметь: - определять ресурсы и объекты подлежащие защиты, а также требования к системе защиты	Пороговый уровень	Обучающийся слабо (частично) умеет определять ресурсы и объекты подлежащие защиты, а также требования к системе защиты	Блок В – задания реконструктивного уровня – лабораторная работа; - тестирование
		Базовый уровень	Обучающийся с незначительными затруднениями умеет определять ресурсы и объекты подлежащие защиты, а также требования к системе защиты	
		Продвину- тый уровень	Обучающийся умеет определять ресурсы и объекты подлежащие защиты, а также требования к	

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Уровни освоения компетенций	Критерии оценивания сформированности компетенций	Виды оценочных средств
	Владеть: - методами аттестации уровня защищенности объектов, помещений, технических средств и систем		системе защиты	Блок С – задания практико-ориентированного уровня – Кейс задача; - тестирование
		Пороговый уровень	Обучающийся слабо (частично) владеет методами аттестации уровня защищенности объектов, помещений, технических средств и систем	
		Базовый уровень	Обучающийся с небольшими затруднениями владеет методами аттестации уровня защищенности объектов, помещений, технических средств и систем	
		Продвинутый уровень	Обучающийся свободно владеет методами аттестации уровня защищенности объектов, помещений, технических средств и систем	
ПК-3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Знать: - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	Пороговый уровень	Обучающийся слабо (частично) знает технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	Блок А – задания репродуктивного уровня – тестовые задания; – вопросы для обсуждения - тестирование

<i>Формируемые компетенции</i>	<i>Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций</i>	<i>Уровни освоения компетенций</i>	<i>Критерии оценивания сформированности компетенций</i>	<i>Виды оценочных средств</i>
		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	
		Продвину- тый уровень	Обучающийся с требуемой степенью полноты и точности знает технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	
	Уметь: осуществлять меры противодействия утечки информации по техническим каналам	Пороговый уровень	Обучающийся слабо (частично) умеет осуществлять меры противодействия утечки информации по техническим каналам	Блок В – задания реконструктивного уровня – лабораторная работа; - тестирование
		Базовый уровень	Обучающийся с незначительными затруднениями умеет осуществлять	

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Уровни освоения компетенций	Критерии оценивания сформированности компетенций	Виды оценочных средств
			меры противодействия утечки информации по техническим каналам	
		Продвину- тый уровень	Обучающийся умеет осуществлять меры противодействия утечки информации по техническим каналам	
	Владеть: - навыками моделирования технических каналов утечки информации	Пороговый уровень	Обучающийся слабо (частично) владеет навыками моделирования технических каналов утечки информации	Блок С – задания практико-ориентированного уровня – Кейс-задача; - тестирование
		Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками моделирования технических каналов утечки информации	
		Продвину- тый уровень	Обучающийся свободно владеет навыками моделирования технических каналов утечки информации	
ПК-3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок,	Знать: - методы и средства контроля эффективности технической защиты информации	Пороговый уровень	Обучающийся слабо (частично) знает методы и средства контроля эффективности технической защиты информации	Блок А – задания репродуктивного уровня – вопросы для обсуждения

<i>Формируемые компетенции</i>	<i>Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций</i>	<i>Уровни освоения компетенций</i>	<i>Критерии оценивания сформированности компетенций</i>	<i>Виды оценочных средств</i>
создаваемых техническими средствами обработки информации ограниченного доступа		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает методы и средства контроля эффективности технической защиты информации	
		Продвину- тый уровень	Обучающийся с требуемой степенью полноты и точности знает методы и средства контроля эффективности технической защиты информации	
	Уметь: - обслуживать технические средства защиты информации	Пороговый уровень	Обучающийся слабо (частично) умеет обслуживать технические средства защиты информации	Блок В – задания реконструк- тивного уровня – лабораторна- я работа; - тестировани- е
		Базовый уровень	Обучающийся с незначительными затруднениями умеет обслуживать технические средства защиты информации	
		Продвину- тый уровень	Обучающийся умеет обслуживать технические средства защиты информации	
	Владеть: - навыками установки и настройки средств	Пороговый уровень	Обучающийся слабо (частично) владеет навыками	Блок С – задания практико-

<i>Формируемые компетенции</i>	<i>Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций</i>	<i>Уровни освоения компетенций</i>	<i>Критерии оценивания сформированности компетенций</i>	<i>Виды оценочных средств</i>
	технической защиты информации		установки и настройки средств технической защиты информации	ориентированного уровня – практическая работа – тестирование
		Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками установки и настройки средств технической защиты информации	
		Продвинутой уровень	Обучающийся свободно владеет навыками установки и настройки средств технической защиты информации	
ПК-3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	<u>Знать:</u> – методы расчета и инструментального контроля показателей технической защиты информации	Пороговый уровень	Обучающийся слабо (частично) знает методы расчета и инструментального контроля показателей технической защиты информации	Блок А – задания репродуктивного уровня – тестовые задания; – вопросы для обсуждения – тестирование
		Базовый уровень	Обучающийся с не-значительными ошибками и отдельными пробелами знает методы расчета и инструментального контроля показателей технической	

<i>Формируемые компетенции</i>	<i>Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций</i>	<i>Уровни освоения компетенций</i>	<i>Критерии оценивания сформированности компетенций</i>	<i>Виды оценочных средств</i>
			защиты информации	
		Продвину- тый уровень	Обучающийся с требуемой степенью полноты и точности знает методы расчета и инструментального контроля показателей технической защиты информации	
	Уметь: - Рассчитывать показатели технической защиты информации	Пороговый уровень	Обучающийся слабо (частично) умеет рассчитывать показатели технической защиты информации	Блок В – задания реконструк- тивного уровня – лабораторна- я работа; - тестировани- е
		Базовый уровень	Обучающийся с незначительными затруднениями умеет рассчитывать показатели технической защиты информации	
		Продвину- тый уровень	Обучающийся умеет рассчитывать показатели технической защиты информации	
	Владеть: - методами расчета и инструментального контроля показателей технической защиты информации	Пороговый уровень	Обучающийся слабо (частично) владеет навыками методами расчета и инструментального контроля показателей	Блок С – задания практико- ориентиров- анного уровня –

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Уровни освоения компетенций	Критерии оценивания сформированности компетенций	Виды оценочных средств
			технической защиты информации	практическая работа (проект); - тестирование
		Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками методами расчета и инструментального контроля показателей технической защиты информации	
		Продвинутый уровень	Обучающийся свободно владеет навыками методами расчета и инструментального контроля показателей технической защиты информации	

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине

Для проверки сформированности компетенции ПК-3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. Прочтите текст задания и выберите один верный ответ

Что понимается под техническим каналом утечки информации?

Варианты ответов:

- а. Совокупность объекта разведки, технического средства разведки и физической среды распространения сигнала.
- б. Способ хищения информации путем подкупа сотрудников.
- в. Программная уязвимость в операционной системе.
- г. Отсутствие антивирусного программного обеспечения.

2. Прочтите текст задания и выберите один верный ответ

Какой вид информации подлежит технической защите в обязательном порядке согласно законодательству РФ (для госучреждений)?

Варианты ответов:

- а. Общедоступная информация.
- б. Информация, составляющая государственную тайну.
- в. Рекламная информация.
- г. Личная переписка сотрудников в нерабочее время.

3. Прочтите текст задания и выберите один верный ответ

Акустический канал утечки информации возникает за счет:

Варианты ответов:

- а. Электромагнитного излучения монитора.
- б. Распространения звуковых волн в воздушной среде.
- в. Колебаний строительных конструкций.
- г. Отражения лазерного луча от оконного стекла.

4. Прочтите текст задания и выберите один верный ответ

Виброакустический канал утечки информации подразумевает съем информации:

Варианты ответов:

- а. Через микрофон, спрятанный в вентиляции.

- б. Путем считывания вибраций твердых тел (стен, труб, стекол), вызванных звуковой волной.
- в. Путем перехвата радиосигнала от беспроводной клавиатуры.
- г. Через визуальное наблюдение.

5. Прочтите текст задания и выберите один верный ответ

Что такое «микрофонный эффект» в технических средствах?

Варианты ответов:

- а. Использование некачественного микрофона при записи.
- б. Свойство элементов электронных схем преобразовывать акустические колебания в электрический сигнал.
- в. Эффект эха при конференц-связи.
- г. Усиление звука с помощью программных средств.

6. Прочтите текст задания и выберите один верный ответ

Оптико-электронный (лазерный) канал утечки информации основан на:

Варианты ответов:

- а. Использовании скрытых видеокамер.
- б. Модуляции лазерного луча, отраженного от вибрирующей поверхности (например, оконного стекла).
- в. Передаче данных по оптоволоконным линиям связи.
- г. Считывании информации с экрана монитора через бинокль.

7. Прочтите текст задания и выберите один верный ответ

Что такое «контролируемая зона» (КЗ)?

Варианты ответов:

- а. Зона, где установлены камеры видеонаблюдения.
- б. Пространство, в пределах которого исключено неконтролируемое пребывание посторонних лиц и транспортных средств.
- в. Комната для проведения секретных переговоров.
- г. Зона действия сигнала Wi-Fi.

8. Прочтите текст задания и выберите один верный ответ

Развязывающие устройства (например, оптроны) в линиях связи применяются для:

Варианты ответов:

- а. Гальванической изоляции цепей и предотвращения прохождения опасных сигналов.
- б. Увеличения дальности связи.
- в. Шифрования данных.
- г. Ускорения обработки пакетов.

9. Прочтите текст задания и выберите один верный ответ

Для защиты от утечки информации по вентиляционным каналам (акустический канал) применяются:

Варианты ответов:

- а. Акустические ловушки и глушители (лабиринтного типа).
- б. Металлические сетки.
- в. Сетевые фильтры.
- г. Видеонаблюдение внутри шахты.

10. Прочтите текст задания и выберите один верный ответ

Что такое «категорирование» объекта информатизации?

Варианты ответов:

- а. Присвоение инвентарных номеров компьютерам.
- б. Установление градации важности объекта и необходимого уровня его защищенности.
- в. Разделение сотрудников на группы доступа.
- г. Выбор цветовой схемы оформления кабинета.

11. Прочтите текст задания и выберите один верный ответ

Для защиты окон от лазерного съема информации пассивным методом используют:

Варианты ответов:

- а. Жалюзи.
- б. Специальные пленки или стекла с определенными оптическими свойствами.
- в. Открытие окон на проветривание.
- г. Установку решеток.

12. Прочтите текст задания и выберите один верный ответ

Система виброакустической защиты (виброизлучатели) устанавливается на:

Варианты ответов:

- а. Компьютерные мыши и клавиатуры.
- б. Стены, окна, трубы отопления и дверные проемы.
- в. Серверные стойки.
- г. Кабели питания.

A2. Вопросы для обсуждения

1. Порядок организации защиты информации на объектах информатизации.
2. Предварительное специальное обследование объекта информатизации.
3. Лицензирование деятельности по технической защите информации.
4. Сертификация технических средств защиты информации.

5. Назовите законы РФ, являющиеся, законодательной и нормативной базой лицензирования и сертификации в области защиты информации?

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст задания и установите соответствие

Каналы утечки информации и физическая природа

1. Акустический канал	а. Побочные электромагнитные излучения и наводки информативных сигналов
2. Виброакустический канал	б. Распространение звуковых волн в воздушной среде
3. Оптический канал	в. Наблюдение (регистрация) визуально воспринимаемой информации/светового излучения
4. Электромагнитный канал (ПЭМИН)	г. Передача информативных колебаний через твёрдые конструкции (стены, перекрытия, инженерные коммуникации)

Прочтите текст задания и установите соответствие

Методы ТЗИ и их базовый принцип

1. Экранирование	а. Ослабление информативных составляющих за счёт добавления маскирующего сигнала/шума
2. Фильтрация	б. Прерывание электрической связи между цепями при сохранении передачи сигнала (например, через трансформатор/оптопару)
3. Гальваническая развязка	в. Ослабление электромагнитной связи с внешней средой за счёт экрана
4. Зашумление (маскирование)	г. Подавление (ослабление) нежелательных составляющих по частоте в проводных линиях

Прочтите текст задания и установите соответствие

Средства защиты и типовой канал, против которого они применяются

1. Акустический генератор шума	а. Электромагнитный (ПЭМИН)
2. Виброизлучатели (виброакустическое зашумление конструкций)	б. Виброакустический

3. Экранированный шкаф/кожух	в. Акустический
4. Вводной помехоподавляющий фильтр на линии питания	г. Проводной (утечка/наводки по цепям электропитания)

Прочтите текст задания и установите соответствие

Меры против акустической утечки и механизм действия

1. Звукоизоляция ограждающих конструкций	а. Снижение передачи звука через конструкции за счёт повышения изоляции
2. Звукопоглощение (акустическая обработка)	б. Снижение разборчивости речи добавлением маскирующего шума
3. Акустическое зашумление	в. Снижение уровня отражений в помещении (уменьшение реверберации)
4. Увеличение дистанции/организация пространственного разобщения	г. Ослабление уровня речевого сигнала на границе контроля за счёт расстояния

Прочтите текст задания и установите соответствие

Комплексные меры защиты помещения и канал утечки, который они перекрывают в первую очередь

1. Тамбур/двойные двери	а. Виброакустический
2. Виброразвязка инженерных коммуникаций (труб, коробов) и конструкций	б. Электромагнитный/проводной (по вводам коммуникаций)
3. Жалюзи/шторы на окнах	в. Оптический
4. Экранирование и фильтрация кабельных вводов	г. Акустический

В2. Лабораторная работа «Разработка технического паспорта объекта»

При подготовки к занятию необходимо обратить внимание на следующие моменты.

1. Требования к разработке технического паспорта.
2. Необходимая документация для разработки технического паспорта.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Тестовые задания

Прочтите текст задания и выберите один верный ответ

Описание ситуации: В переговорной обсуждаются сведения ограниченного доступа. Стена граничит с коридором, слышимость высокая.

Задание: Какое средство относится к защите информации в акустическом техническом канале утечки?

Варианты ответов:

- а. Сегментация локальной сети VLAN
- б. Зашумление (маскирование) речевого сигнала/акустическое зашумление
- в. Электронная подпись документов
- г. Шифрование диска BitLocker

Прочтите текст задания и выберите один верный ответ

Описание ситуации: Переговоры ведутся в комнате с общей стеной. Предполагается, что утечка возможна не только по воздуху, но и через вибрации в конструкциях.

Задание: Какой вариант соответствует противодействию виброакустическому техническому каналу?

Варианты ответов:

- а. Акустическая/виброизоляция конструкций (применение материалов, снижающих передачу вибраций)
- б. Настройка SIEM для мониторинга событий
- в. Введение политики смены паролей
- г. Контроль целостности ОС

Прочтите текст задания и выберите один верный ответ

Описание ситуации: Рабочие места расположены рядом с окном. Напротив — здание, из которого возможно визуальное наблюдение за экранами.

Задание: Какое решение относится к защите информации по оптическому (визуальному) техническому каналу?

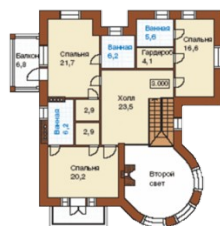
Варианты ответов:

- а. Использование экранов/жалюзи/плёнок, ограничивающих обзор (антишпионские решения), и/или организационное размещение рабочих мест вне прямой видимости
- б. Установка DLP на рабочие станции
- в. Использование VPN для удалённого доступа
- г. Внедрение управления уязвимостями

C2. Практическая работа

Рассчитать требуемое количество оборудования для закрытия речевого канала утечки информации в здании имеющего следующие характеристики

План второго этажа



План первого этажа



План цокольного этажа



объекта защиты

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Нормативные документы в сфере технической защиты информации
2. Требования к защищаемым помещениям

Для проверки сформированности компетенции ПК -3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. Прочтите текст задания и выберите один верный ответ

Подавители сотовой связи (джаммеры) работают по принципу:

Варианты ответов:

- а. Физического уничтожения SIM-карт.
- б. Создания мощной помехи на частотах работы стандартов GSM/3G/4G/5G.
- в. Перехвата SMS-сообщений.
- г. Экранирования телефона свинцом.

2. Прочтите текст задания и выберите один верный ответ

Для защиты телефонных линий от прослушивания используются:

Варианты ответов:

- а. Криптомаршрутизаторы.
- б. Скремблеры (устройства шифрования речи) и анализаторы телефонных линий.
- в. Обычные диктофоны.
- г. Усилители сигнала.

3. Прочтите текст задания и выберите один верный ответ

«Выжигание» входных цепей подслушивающих устройств — это метод:

Варианты ответов:

- а. Пассивной защиты.
- б. Активного функционального подавления (силового воздействия).
- в. Организационной меры.
- г. Криптографической защиты.

4. Прочтите текст задания и выберите один верный ответ

Нелинейный локализатор предназначен для:

Варианты ответов:

- а. Поиска скрытых камер по бликам объектива.
- б. Обнаружения полупроводниковых элементов (электроники) независимо от того, включены они или выключены.
- в. Измерения уровня радиации.
- г. Поиска металлических предметов больших размеров (сейфов).

5. Прочтите текст задания и выберите один верный ответ

Индикатор поля — это прибор для:

Варианты ответов:

- а. Выявления факта работы радиопередающих устройств (жучков) в ближней зоне.
- б. Измерения напряженности магнитного поля Земли.
- в. Определения сторон света.
- г. Измерения влажности воздуха.

6. Прочтите текст задания и выберите один верный ответ

Анализатор спектра используется в ТЗИ для:

Варианты ответов:

- а. Анализа химического состава воздуха.
- б. Исследования радиозэфира на наличие подозрительных сигналов и их характеристик.
- в. Проверки качества звукоизоляции.
- г. Тестирования скорости интернета.

7. Прочтите текст задания и выберите один верный ответ

Оптический обнаружитель скрытых видеокамер работает на принципе:

Варианты ответов:

- а. Эффекта «световозвращения» (отражения света от светочувствительного слоя матрицы камеры).
- б. Улавливания радиосигнала камеры.
- в. Теплового излучения камеры.
- г. Анализа трафика сети.

8. Прочтите текст задания и выберите один верный ответ

Тепловизор может быть полезен при поиске закладных устройств, так как:

Варианты ответов:

- а. Закладные устройства всегда холоднее окружающей среды.
- б. Работающая электроника выделяет тепло, которое может быть заметно на фоне холодных поверхностей (стен, потолков).
- в. Он видит сквозь стены.
- г. Он обнаруживает радиоволны.

9. Прочтите текст задания и выберите один верный ответ

Рентгеновская установка (интроскоп) применяется для:

Варианты ответов:

- а. Проверки входящей корреспонденции, посылок и сумок на наличие вложений.
- б. Сканирования радиоэфира.
- в. Защиты от вирусов.
- г. Проверки биометрических данных.

10. Прочтите текст задания и выберите один верный ответ

Какое устройство используется для проверки проводных линий (электросеть, телефон) на наличие подключений?

Варианты ответов:

- а. Дозиметр.
- б. Рефлектометр или анализатор проводных линий.
- в. Люксметр.
- г. Барометр.

11. Прочтите текст задания и выберите один верный ответ

Специальная проверка (СП) технических средств — это:

Варианты ответов:

- а. Проверка работоспособности компьютера (включается или нет).
- б. Комплекс инженерно-технических мероприятий по поиску возможно внедренных закладных устройств.
- в. Проверка наличия инвентарных номеров.
- г. Протирка оборудования от пыли.

12. Прочтите текст задания и выберите один верный ответ

Специальные исследования (СИ) технических средств проводятся с целью:

Варианты ответов:

- а. Выявления возможных технических каналов утечки информации (например, измерения уровня ПЭМИН).
- б. Ремонта неисправных блоков.
- в. Установки операционной системы.
- г. Модернизации оборудования.

13. Прочтите текст задания и выберите один верный ответ

Биометрические системы контроля доступа (СКУД) относятся к:

Варианты ответов:

- а. Средствам защиты от ПЭМИН.
- б. Средствам защиты от несанкционированного доступа (НСД) к объектам и информации.
- в. Средствам обнаружения радиозакладок.
- г. Средствам пожаротушения.

A2. Вопросы для обсуждения

1. Основные задачи инженерно-технической защиты информации. Факторы, влияющие на эффективность инженерно-технической защиты информации.
2. Базовые принципы инженерно-технической защиты информации (общие, специальные, дополнительные).
3. Объект информатизации (определение). Основные технические средства и системы (ОТСС). Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации
4. Показатели эффективности инженерно-технической защиты информации.
5. Основные направления инженерно-технической защиты информации (остановиться на информационном и энергетическом скрывании)
6. Виды побочных электромагнитных излучений и наводок.
7. Чем отличаются активные акустоэлектрические преобразователи от пассивных?
8. Какие угрозы создают случайные акустоэлектрические преобразователи?
9. Виды паразитных связей. Физические явления, вызывающие емкостные и индуктивные паразитные связи.
10. Физический смысл действующей высоты и действующей длины антенны.
11. Источники побочных низкочастотных и высокочастотных излучений.
12. Причины, вызывающие появление опасных сигналов в цепях электропитания.
13. Физические процессы, приводящие к утечке информации по цепям заземления.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст задания и установите соответствие

Активные и пассивные меры: установите соответствие

1. Экранирование	а. Пассивная мера
2. Фильтрация	б. Активная мера
3. Акустическое зашумление	в. Активная мера
4. Виброакустическое зашумление конструкций	г. Пассивная мера

Прочтите текст задания и установите соответствие

Защита визуальной информации: средство и результат

1. Приватный фильтр (ограничитель угла обзора) на монитор	а. Ограничение угла, под которым читается изображение на экране
2. Размещение монитора с исключением прямой видимости	б. Блокирование линии наблюдения через оконный проём

со стороны проходов/окон	
3. Жалюзи/шторы на окнах	в. Снижение визуальной прозрачности стекла при сохранении освещённости (в пределах свойств плёнки)
4. Матирующая/тонирующая плёнка на стекло	г. Исключение возможности наблюдения экрана из типовых точек доступа наблюдателя

Прочтите текст задания и установите соответствие

Охранные извещатели и тип реагирования

1. Магнитоконтактный извещатель	а. Реагирует на изменение теплового (ИК) излучения в зоне контроля (движение человека)
2. Пассивный инфракрасный (PIR) извещатель	б. Реагирует на открывание двери/окна (размыкание/смыкание контакта)
3. Вибрационный извещатель	в. Реагирует на удар/вибрации конструкций (стены, сейфы, ограждения)
4. Объёмный микроволновый извещатель	г. Реагирует на движение в зоне контроля по изменению параметров СВЧ-поля (доплеровский эффект)

Прочтите текст задания и установите соответствие

Нарушение (угроза) и техническая мера противодействия

1. Проникновение в помещение постороннего лица	а. Охранный сигнализация/СКУД (системы контроля и управления доступом)
2. Внедрение (скрытая установка) закладного устройства	б. Регулярные обследования/поиск специальных технических средств (в т.ч. нелинейным локатором и радиоконтролем)
3. Несанкционированное подключение к кабельной линии	в. Организация защиты визуального канала (жалюзи/плёнки/исключение прямой видимости)
4. Наблюдение конфиденциальной информации через окно	г. Контроль целостности/мониторинг линий и физическая защита трасс прокладки

В2. Лабораторная работа

Лабораторная работа «Исследование акустического и виброакустического каналов утечки информации»

Цель работы:

- Исследовать эффективность пассивного и активного противодействия утечке речевой информации по акустическому и виброакустическому каналу.
- Изучение способов работы с многофункциональным поисковым прибором ST -031 «Пиранья» в области акустических и виброакустических измерений.
- Знакомство с системой виброакустической защиты (СВАЗ) путем постановки маскирующей помехи «Соната» и пассивным экранированием акустического и виброакустического каналов утечки конфиденциальной информации.

Лабораторная работа 1 «Выбор объекта и определение информационных ресурсов»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Основные понятия и сущность информационных ресурсов.
2. Информационное описание объекта и формирование информационных ресурсов.
3. Классификация информационных ресурсов

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Тестовые задания

Прочтите текст задания и выберите один верный ответ

Описание ситуации: Организация вводит контролируемую зону вокруг помещения, где обрабатывается конфиденциальная информация, из-за рисков утечки по техническим каналам.

Задание: Для какого класса угроз такое решение является типичным с точки зрения технической защиты информации?

Варианты ответов:

- а. Утечки через фишинговые письма
- б. Утечки через ошибки в веб-приложении
- в. Утечки по техническим каналам (например, ПЭМИН/акустика/оптика), когда необходимо исключить возможность съёма сигналов за пределами зоны

г. Утечки через компрометацию облачного провайдера

Прочтите текст задания и выберите один верный ответ

Описание ситуации: В офисе есть стеклянные перегородки и окна; экран сотрудника может быть виден под углом через отражение в стекле.

Задание: Какая мера относится к защите по оптическому каналу утечки?

Варианты ответов:

- а. Использование антибликовых/антишпионских экранов и изменение расстановки рабочих мест для исключения прямой/отражённой видимости
- б. Настройка DNSSEC
- в. Контейнеризация приложений
- г. Управление патчами

C2. Кейс задача

«В поисках источника утечки информации»

Задача :

- 1. Составить логическую схему базы знаний по содержанию блока.
- 2. Составить терминологический словарь.
- 3. Выполнить все пункты, перечисленные в разделе подготовительного этапа к занятию.

Цели: 1. Закрепить и углубить изучаемый материал студентами.

2. Уметь изложить свою точку зрения по проблемным вопросам инженерно-технической защиты информации.

Участники: Студенты распределены на 3 подгруппы:

- 1-я подгруппа – сотрудники технической группы службы безопасности;
- 2-я подгруппа – специалисты по добыванию информации различными способами (в том числе и незаконными);
- 3-я подгруппа – экспертная группа.

Время: 90 минут.

1. Подготовительный этап (домашняя работа):

- 1. Подготовить материал по ранее выданной преподавателем проблеме:
 - составить план блока;
 - составить терминологический словарь: выписать встречаемые в тексте блока термины и дать им расшифровку;
 - выбрать одно из предприятий (хранилища и депозитарии банков; предприятия по производству или хранилища химически опасных, наркотических и взрывчатых веществ, боеприпасов ядерных материалов; предприятия оборонного профиля; правительственные учреждения; энергетические комплексы, кассовые залы банков; подъезды инкассаторских машин; помещения для хранения и работы с важной защищаемой информацией; торговые центры по

продаже ценных товаров; производственные помещения для изготовления ценной продукции, торговые залы магазинов; служебные помещения учреждений; офисы среднего и малого бизнеса; производственные помещения общего назначения; жилые помещения и т.д.);

2. Исходя из содержания блока, составить применительно к выбранному объекту до десяти вопросов:

а) сотрудникам технической группы службы безопасности, касающиеся обеспечения безопасности объекта;

б) специалистам по добыванию информации различными способами (в том числе и незаконными), касающиеся способов несанкционированного вторжения на объект, подслушивания, перехвата и т.п.

3. Быть готовыми ответить на любые поставленные вопросы со стороны подгруппы сотрудников технической группы службы безопасности, подгруппы специалистов по добыванию информации различными способами (в том числе и незаконными). Уметь оценить вопросы и ответы участников будучи в подгруппе экспертов.

4. Быть готовыми ответить на вопросы помещенные в конце блока.

5. Оформить работу в виде отчета.

2. Порядок проведения занятия

1. Организация занятия (проверка присутствующих и готовности к занятиям, объявление темы исходя из содержания текущего занятия). (5 минут.)

2. Распределение на подгруппы и доведение порядка проведения занятия. (5 минут.)

3. Присвоение подгруппам первоначальных ролей (сотрудники технической группы службы безопасности, специалисты по добыванию информации различными способами (в том числе и незаконными), экспертная группа). (5 минут.)

4. Обсуждение студентами подгрупп вопросов, вынесенных на практическое занятие с целью выработки общих позиций:

4.1. Вопросы со стороны подгруппы выступающих в роли сотрудников технической группы службы безопасности. (15 минут.)

4.2. Вопросы со стороны подгруппы выступающих в роли специалистов по добыванию информации. (15 минут.)

4.3. Вопросы со стороны подгруппы экспертов. (15 минут.)

4.4. Ответы и дискуссии. (10 минут.)

4.5. Выработка общей позиции и общего подхода к вопросам рассматриваемым на текущем занятии согласно его теме. (5 минут.)

5. Обсуждение преподавателем и старшими групп оценок участников занятия. (5 минут.)

6. Подведение итогов занятия с объявлением окончательных оценок участников занятия. (5 минут.)

7. Объявление проблемы и содержания следующего занятия. (5 минут.)

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации.
2. Принципы защиты информации техническими средствами.
3. Основные направления инженерно-технической защиты информации.
4. Показатели эффективности инженерно-технической защиты информации.
5. Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты.
6. Характеристики технических каналов утечки информации.
7. Физические принципы технических каналов передачи информации.
8. Структурирование информации.
9. Классификация демаскирующих признаков.
10. Оознавательные признаки и признаки деятельности.
11. Видовые демаскирующие признаки.
12. Демаскирующие признаки сигналов.
13. Демаскирующие признаки веществ. Именные, прямые и косвенные демаскирующие признаки.
14. Виды источников и носителей информации.
15. Прямые и косвенные источники семантической информации.
16. Принципы записи и съема информации с её носителя.
17. Источники функциональных сигналов. Понятие модуляции, манипуляции, демодуляции.
18. Побочные электромагнитные излучения и наводки Угрозы утечки информации. Угрозы преднамеренных воздействий. Угрозы случайных воздействий.
19. Технические каналы утечки информации: наблюдение, подслушивание, перехват.
20. Источники угроз безопасности информации.
21. Опасные сигналы и их источники.

Для проверки сформированности компетенции ПК-3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа

Блок А. Задания репродуктивного уровня («знать»)

А1. Тестовые задания

1. Прочтите текст задания и выберите один верный ответ

Что означает аббревиатура ПЭМИН?

Варианты ответов:

- а. Побочные электромагнитные излучения и наводки.
- б. Первичные электронные методы измерения напряжения.
- в. Программные элементы мониторинга информационной нагрузки.
- г. Пороговые эталоны магнитных импульсных напряжений.

2. Прочтите текст задания и выберите один верный ответ

Какой материал лучше всего подходит для экранирования низкочастотных магнитных полей?

Варианты ответов:

- а. Сухое дерево.
- б. Пластик.
- в. Пермаллой (магнитомягкий материал).
- г. Алюминий.

3. Прочтите текст задания и выберите один верный ответ

Сетевые помехоподавляющие фильтры устанавливаются в цепях электропитания для:

Варианты ответов:

- а. Экономии электроэнергии.
- б. Предотвращения утечки информации через провода электросети за счет наводок.
- в. Защиты от короткого замыкания (как основная функция).
- г. Усиления сигнала процессора.

4. Прочтите текст задания и выберите один верный ответ

Какая мера является организационно-технической при защите от ПЭМИН?

Варианты ответов:

- а. Размещение ОТСС (основных технических средств и систем) на максимальном удалении от граница контролируемой зоны.
- б. Установка антивируса Касперского.
- в. Обучение сотрудников основам криптографии.
- г. Использование только бумажных носителей.

5. Прочтите текст задания и выберите один верный ответ

Генераторы электромагнитного шума (ГШ) применяются для:

Варианты ответов:

- а. Защиты от перепадов напряжения.
- б. Подавления приемников, пытающихся перехватить ПЭМИН, путем создания широкополосной помехи.
- в. Усиления сигнала Wi-Fi.
- г. Зарядки беспроводных устройств.

6. Прочтите текст задания и выберите один верный ответ

Что такое «пространственное зашумление»?

Варианты ответов:

- а. Создание электромагнитного поля помех в пространстве вокруг защищаемого объекта.
- б. Загромождение комнаты мебелью.
- в. Использование нескольких слоев гипсокартона.
- г. Хаотичное движение сотрудников по офису.

7. Прочтите текст задания и выберите один верный ответ

Активная защита от ПЭМИН методом «синфазной помехи» в цепях питания и заземления эффективна, если:

Варианты ответов:

- а. Помеха создается в слышимом диапазоне.
- б. Уровень помехи значительно превышает уровень информативного сигнала в проводнике.
- в. Используется батарейное питание.
- г. Оборудование выключено.

8. Прочтите текст задания и выберите один верный ответ

Система защиты информации от утечки по каналу ПЭМИН должна быть сертифицирована:

Варианты ответов:

- а. Роспотребнадзором.
- б. ФСТЭК России (или аналогичным регулятором в зависимости от страны).
- в. Министерством образования.
- г. Местным провайдером интернета.

A2. Вопросы для обсуждения

1. Принципы защиты информации в технических каналах утечки информации.
2. Способы защиты информации в акустическом техническом канале утечки.
3. Способы и средства защиты информации от специальных закладных

- устройств (общие вопросы).
4. Способы и средства защиты информации от специальных закладных устройств (методы выявления, индикаторы поля).
 5. Способы и средства защиты информации от специальных закладных устройств (методы выявления, специальные приемники).
 6. Способы и средства защиты информации от специальных закладных устройств (методы выявления, комплексы радиоконтроля).
 7. Способы и средства защиты информации от специальных закладных устройств (методы выявления, нелинейные локаторы).
 8. Методы и средства защиты информации в электромагнитном техническом канале утечки информации (общие вопросы).
 9. Методы и средства защиты информации в электрическом канале утечки информации (контроль линий связи).
 10. Технические средства защиты информации в электрическом техническом канале утечки информации (предотвращение использования эффекта акустоэлектронного преобразования и эффекта ВЧ-навязывания).
 11. Методы защиты информации в телефонных каналах связи (исключая криптографию).
 12. Методы защиты информации от несанкционированной аудиозаписи.
 13. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
 14. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля.
 15. Генераторы шума.
 16. Особенности работы и основные характеристики сканирующих радиоприемников.
 17. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения и локализации в пространстве закладных устройств.
 18. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
 19. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений
 20. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных наводок.
 21. Схема перехвата речевой информации по акустовибрационному каналу утечки речевой информации. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.
 22. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.
 23. Основные требования к заземлению технических средств. Схемы заземлителей. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.

24. Основные требования к системе пространственного электромагнитного зашумления. Схема установки системы пространственного зашумления на объекте информатизации. Основные требования по установке системы пространственного зашумления на объекте информатизации. Основные характеристики генераторов шума.
25. Основные требования к системе электропитания технических средств. Способы защиты цепей электропитания технических средств от утечки информации, возникающей за счет побочных электромагнитных излучений.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст задания и установите соответствие

Защита кабельных линий: технические решения и принцип

1. Экранированный кабель	а. Гальваническая развязка цепей при передаче сигнала через оптический канал
2. Витая пара	б. Снижение влияния внешних наводок за счёт симметрии и скрутки проводников
3. Оптронная (оптическая) развязка	в. Ослабление высокочастотных помех (общего режима) на проводнике
4. Ферритовый фильтр (ферритовое кольцо/защёлка)	г. Снижение излучений/наводок за счёт экрана при корректном подключении (заземлении) экрана

Прочтите текст задания и установите соответствие

Типовые источники ПЭМИН и вид информативного сигнала

1. Видеоподсистема (монитор/видеокабель)	а. Сигналы, соответствующие выводимому изображению
2. Клавиатура	б. Сигналы, соответствующие событиям ввода (нажатиям клавиш)
3. Принтер	в. Сигналы, соответствующие передаваемым по сети данным
4. Сетевой интерфейс/кабель	г. Сигналы, соответствующие формированию печати (работе печатающего узла)

Прочтите текст задания и установите соответствие

Вводы в экранированное помещение: элемент и его роль

1. Вводной фильтр на линии питания	а. Снижение прохождения помех/информативных составляющих по цепи электропитания
2. Фильтр на сигнальной линии (вводной/проходной)	б. Снижение прохождения высокочастотных составляющих по информационному кабелю
3. Экранированный ввод/муфта с обеспечением непрерывности экрана	в. Сохранение целостности экранирующей оболочки при вводе кабеля
4. Оптический ввод (передача по волокну)	г. Исключение электрической связи по проводнику между зонами (электрическая изоляция канала)

В2. Лабораторная работа

Лабораторная работа 1 «Ознакомление со средствами добывания информации в оптическом диапазоне волн»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Оптические каналы утечки информации.
2. Структура оптического канала утечки информации.
3. Среда распространения в оптическом канале утечки информации.

Лабораторная работа 2 «Ознакомление со средствами добывания информации в акустическом диапазоне волн»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Акустические (речевые) каналы утечки информации.
2. Характеристики речевого сигнала.
3. Средства акустической разведки и их технические характеристики.

Лабораторная работа 3 «Ознакомление со средствами добывания информации в радиоэлектронном канале утечки»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Особенности радиоэлектронных каналов утечки информации.
2. Виды и структура радиоэлектронных каналов утечки информации.
3. Направляющие линии связи, их характеристики.

Лабораторная работа 4 «Ознакомление со средствами добывания информации в электромагнитном канале утечки»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Электромагнитные каналы утечки информации.
2. Электрические каналы утечки информации.
3. Параметрический канал утечки информации.

Лабораторная работа 5 «Изучение способов утечки информации по материально-вещественному каналу»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Структура материально-вещественного канала утечки информации и характеристики ее элементов.
2. Способы утечки демаскирующих веществ в твердом, жидком и газообразном виде.
3. Особенности утечки информации о радиоактивных веществах.

Лабораторная работа 6 «Способы и средства защиты информации от наблюдения»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Объект наблюдения в оптическом канале утечки информации.
2. Электромагнитные излучения объекта наблюдения.
3. Оптический приемник.

Лабораторная работа 7 «Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Классификация способов и средств защиты объектов информатизации.
2. Экранирование технических средств их соединительных линий.
Экранированные помещения. Заземление технических средств.
3. Требования к системам электропитания и заземления основных технических средств и систем.

Лабораторная работа 8 «Методы и средства выявления электронных устройств негласного получения информации»

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Анализа изменений параметров полей.
2. Способы выявления изменений параметров полей.

Лабораторная работа 9 «Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам»
При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звука и виброизоляции.
2. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Тестовые задания

Прочтите текст задания и выберите один верный ответ

Описание ситуации: В помещении обрабатывается конфиденциальная информация на ПК с обычным монитором. Есть риск утечки по каналу побочных электромагнитных излучений и наводок (ПЭМИН) на расстояние за пределы контролируемой зоны. Требуется снизить риск утечки.

Задание: Какое решение относится к методам/средствам защиты информации именно в техническом канале ПЭМИН?

Варианты ответов:

- а. Установить антивирус и включить контроль внешних носителей
- б. Перевести документы в формат PDF и поставить пароль
- в. Применить экранирование/фильтрацию (например, экранированные конструкции и/или фильтры на линиях питания/сигнальных линиях)
- г. Ограничить права пользователей в домене

Прочтите текст задания и выберите один верный ответ

Описание ситуации: В здании разные арендаторы используют общую электрическую сеть. В защищаемом кабинете стоят средства обработки информации. Подозревается возможность утечки за счёт наводок по цепям электропитания.

Задание: Какой из вариантов является типичной мерой защиты от утечки по цепям электропитания как техническому каналу?

Варианты ответов:

- а. Настроить резервное копирование на NAS
- б. Установить сетевой экран (firewall) на периметре сети

- в. Применить фильтры/развязку по питанию для подавления высокочастотных составляющих/наводок
- г. Включить двухфакторную аутентификацию

С2. Практическое задание - Кейс задача

Моделирование схемы технических каналов утечки информации

Цель работы: Приобрести практические навыки в определении степени защищенности объекта *информатизации* путем моделирования возможных схем технических каналов утечки информации.

Научиться определять потенциальные и реальные каналы утечки информации.

Теоретическая часть

Для того чтобы построить эффективную систему информационной безопасности, необходимо в первую очередь определить потенциальные и реальные угрозы технического проникновения на защищаемый объект, возможные каналы для несанкционированного доступа и утечки защищаемой информации.

Данная работа базируется на знании природы возникновения технических каналов утечки информации и методов ведения технической разведки. Правильное определение потенциальных угроз на предпроектном этапе построения системы защиты позволит в дальнейшем выбрать наиболее оптимальные меры и средства защиты.

При выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное оборудование технических средств обработки информации, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы вентиляции и т.п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др. Наибольшее внимание следует уделить вспомогательным средствам, имеющие линии, выходящие за пределы контролируемой зоны.

В качестве каналов утечки больше внимания следует уделить вспомогательным средствам, имеющим линии, выходящие за пределы контролируемой зоны, а также посторонним проводам и кабелям, проходящим через помещения, где

установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При оценке защищенности помещений от утечки речевой информации необходимо учитывать возможность ее прослушивания как из соседних помещений, так и с улицы. Следует проводить оценку возможности ведения разведки с использованием *лазерных микрофонов*. Интерес могут вызывать каналы утечки за счет вибраций, возникающих под давлением *акустических волн*, в твердых телах (ограждениях, трубах и т.п.).

Оценка защищенности объекта включает в себя анализ режима работы и охраны объекта, с *целью моделирования* действий по скрытному проникновению на них (неконтролируемому пребыванию) посторонних лиц. Режим работы специалистов сторонних организаций, приобретение, установка и ремонт мебели, оргтехники и т.п. Т.е. всю совокупность условий, позволяющих внедрить на объект специальные закладные устройства перехвата информации (микропередатчики, возможность установки миниатюрных микрофонов с подключением к внешним линиям и т.д.). А также определение наиболее эффективных, для использования на разных уровнях проникновения, средств технической разведки.

Большое, а иногда решающее, значение при оценке угрозы может иметь знание наиболее вероятного противника, его финансовых и оперативных возможностей, знание личностных качеств постоянного персонала, временных работников и другая дополнительная информация

Легенда

1. Защищаемое помещение расположено на четвертом этаже 7-этажного здания. Все здание принадлежит одной организации:

- Сверху расположены служебные помещения.
- Снизу расположены технические помещения (туалет, электрощитовая).
- Со стороны стены Б расположена приемная.
- Со стороны стены Г расположен общий коридор.

Стороны А и В выходят на улицы с интенсивным пешеходным и транспортным движением.

Окна помещения оборудованы шторами, смотрят на жилой дом расположенный на расстоянии 30 метров.

2. Из мебели в помещении установлены рабочий и журнальный столы, стулья, подставки под: телефоны, ПЭВМ и *телевизор*.

3. Из основных технических средств в помещении установлен телефон внутренней конфиденциальной связи, ПЭВМ включенная в локальную сеть.

4. Из вспомогательных технических средств в помещении установлен телефон ГТС, *телевизор*, радиотрансляционный приемник. Помещение оборудовано системой пожарной и охранной сигнализации, линии которых

выходят на пульт дежурного охранника. Помещение электрифицировано (освещение, питание оборудования).

5. Помещение оборудовано системой вытяжной вентиляции, короб которой проложен вдоль коридора и поднимается на крышу здания. Радиаторы отопления установлены вдоль стены А. Трубы отопления спускаются в подвал.

6. Режим работы учреждения предусматривает свободное передвижение сотрудников и посетителей в рабочее время. В ночное время помещение закрывается на ключ, сдается под охрану дежурному. Системы связи обслуживаются штатным сотрудником. Системы жизнеобеспечения (отопление, канализация) обслуживаются по заявке приходящим сотрудником.

7. Доступ штатных сотрудников к служебной информации не ограничен.

Схема объекта представлена на рисунке.

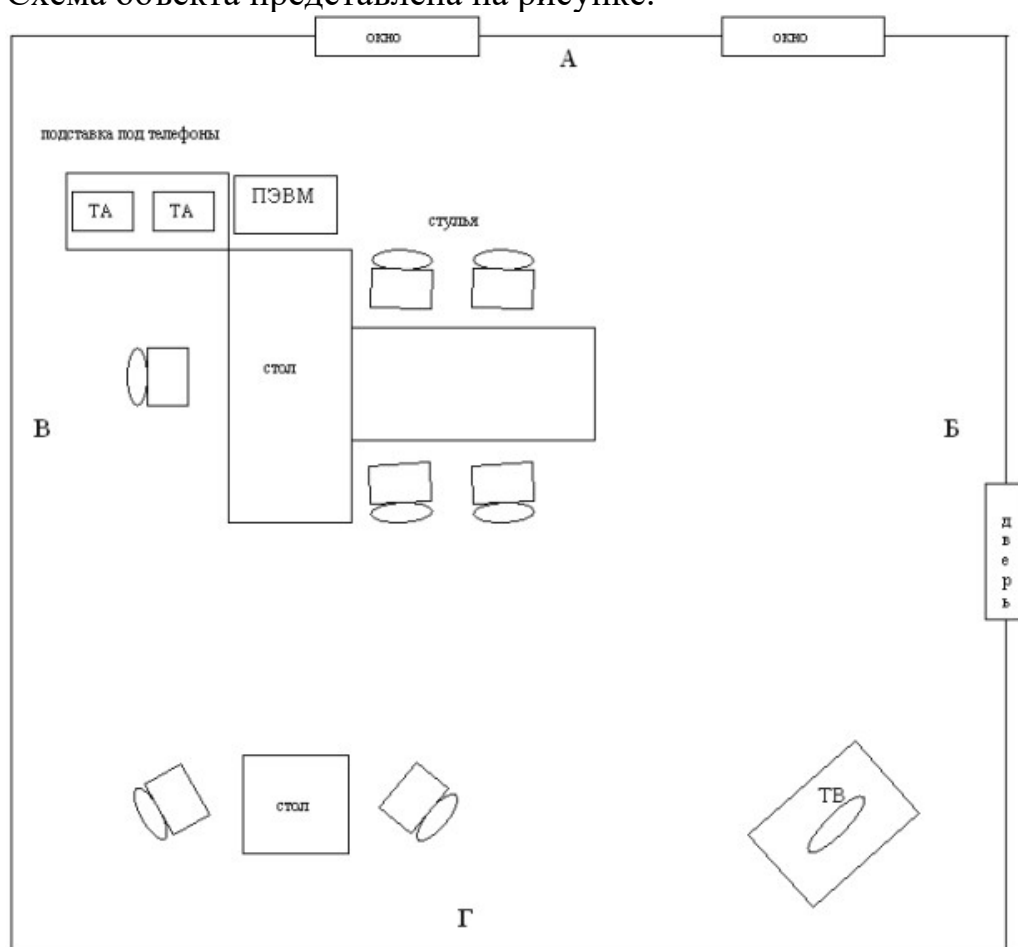


Рис. 1.

Задача

1. Изучить методическую литературу по составлению таблицы утечки информации
2. Разработать таблицу каналов утечки информации.

Содержание отчета

1. Цель работы
2. Задание

3. Ответы на контрольные вопросы
4. Результаты выполнения практической части
5. Вывод по результатам работы

Контрольные вопросы к работе

Что такое структурная модель каналов утечки информации

Что такое динамические показатели каналов утечки информации

Перечислить существующие каналы утечки информации

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Понятие технической защиты информации. Виды, источники и носители защищаемой информации.
2. Классификация способов и средств иностранной технической разведки. Технические каналы утечки информации.
3. Основные этапы и процедуры добывания информации технической разведкой. Пассивные и активные средства технической защиты информации.
4. Принципы оценки эффективности систем технической защиты информации. Технический контроль эффективности принимаемых мер защиты;
5. Концепция защиты объекта информатизации. Содержание, принципы, рекомендации.
6. Компоненты системы видеонаблюдения. Этапы выбора телевизионной камеры.
7. Инженерно-техническая укрепленность. Требования, цели и задачи.
8. Охранные извещатели. Классификация, выбор из учета помеховой обстановки.
9. Оборудование, формирующее структуру системы контроля и управления доступом
- 10.(СКУД) современной интегрированной системы физической защиты. Уровни, состав,назначение и размещение.

Для проверки сформированности компетенции ПК-3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. Прочтите текст задания и выберите один верный ответ

Канал утечки за счет высокочастотного навязывания (ВЧ-навязывания) предполагает:

Варианты ответов:

- а. Воздействие на телефонную линию высокочастотным сигналом для активации микрофона трубки при положенной трубке.
- б. Взлом Wi-Fi сети методом перебора паролей.
- в. Установку радиомаяка на автомобиль.
- г. Использование мощного генератора помех.

2. Прочтите текст задания и выберите один верный ответ

Параметрический канал утечки информации связан с:

Варианты ответов:

- а. Изменением параметров (индуктивности, емкости) элементов схем под воздействием акустического поля и последующим переизлучением ВЧ-сигнала.
- б. Ошибками в параметрах настройки межсетевого экрана.
- в. Утечкой паролей администратора.
- г. Физической кражей жестких дисков.

3. Прочтите текст задания и выберите один верный ответ

Основной целью экранирования является:

Варианты ответов:

- а. Усиление полезного сигнала.
- б. Локализация электромагнитной энергии в определенном пространстве или защита от внешних полей.
- в. Создание акустических помех.
- г. Охлаждение оборудования.

4. Прочтите текст задания и выберите один верный ответ

Заземление технических средств используется для:

Варианты ответов:

- а. Увеличения скорости передачи данных.
- б. Отвода наведенных опасных токов и зарядов в землю.
- в. Защиты от акустической прослушки.
- г. Улучшения качества изображения на мониторе.

5. Прочтите текст задания и выберите один верный ответ

Звукоизоляция помещения направлена на:

Варианты ответов:

- а. Создание шума для маскировки речи.
- б. Снижение уровня звукового сигнала, проходящего за пределы помещения, за счет поглощения и отражения звука ограждающими конструкциями.
- в. Поиск скрытых диктофонов.
- г. Улучшение акустики для прослушивания музыки.

6. Прочтите текст задания и выберите один верный ответ

Суть активной акустической маскировки заключается в:

Варианты ответов:

- а. Использовании звукопоглощающих материалов.
- б. Генерации «белого шума» или речеподобных помех в акустическом диапазоне.
- в. Громком разговоре сотрудников.
- г. Включении громкой музыки.

8. Прочтите текст задания и выберите один верный ответ

Какой недостаток имеет метод активного зашумления?

Варианты ответов:

- а. Он слишком дешевый.
- б. Создает электромагнитную несовместимость и может мешать работе легальных радиосредств и здоровью персонала.
- в. Не требует электропитания.
- г. Абсолютно незаметен для окружающих.

A2. Вопросы для обсуждения

- 14. Виды побочных электромагнитных излучений и наводок.
- 15. Чем отличаются активные акустоэлектрические преобразователи от пассивных?
- 16. Какие угрозы создают случайные акустоэлектрические преобразователи?
- 17. Виды паразитных связей. Физические явления, вызывающие емкостные и индуктивные паразитные связи.
- 18. Физический смысл действующей высоты и действующей длины антенны.
- 19. Источники побочных низкочастотных и высокочастотных излучений.
- 20. Причины, вызывающие появление опасных сигналов в цепях электропитания.
- 21. Физические процессы, приводящие к утечке информации по цепям заземления.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тестовые задания

Прочтите текст задания и установите соответствие

Средства контроля/измерений и контролируемый параметр

1. Измеритель напряжённости электромагнитного поля (полемер)	а. Уровень звукового давления (акустический шум)
2. Анализатор спектра	б. Временная форма сигнала

	(осциллограмма) в электрической цепи
3. Шумомер	в. Напряжённость электрической/магнитной составляющих поля в точке измерения
4. Осциллограф	г. Спектральный состав сигнала/излучения по частоте

Прочтите текст задания и установите соответствие

Акустика и виброакустика: тип материала/решения и функция

1. Звукоизоляционные решения	а. Снижение передачи вибрации от источника к конструкции (механическая развязка)
2. Звукопоглощающие материалы	б. Снижение уровня отражённого звука (уменьшение реверберации)
3. Вибродемпфирующие материалы	в. Снижение передачи звука через ограждающие конструкции
4. Виброизолирующие опоры/прокладки	г. Снижение амплитуды колебаний за счёт внутренних потерь (демпфирование)

Прочтите текст задания и установите соответствие

Контроль эффективности мер ТЗИ: объект контроля и что проверяется

1. Контроль целостности экрана	а. Соответствие уровня зашумления требуемому (для снижения разборчивости речи)
2. Контроль уровня маскирующего акустического шума	б. Выявление фактов несанкционированного вскрытия/доступа
3. Контроль сопротивления заземляющего устройства	в. Наличие непрерывности и корректных соединений экранирующих элементов
4. Контроль целостности пломб	г. Соответствие параметров заземления установленным требованиям (электробезопасность/помехозащищённость)

Прочтите текст задания и установите соответствие

Средства поиска закладных устройств и физический признак обнаружения

1. Нелинейный локатор (NLJD)	а. Наличие металлических предметов (по электромагнитной индукции/изменению поля)
2. Селективный радиоприёмник/детектор	б. Наличие полупроводниковых переходов (нелинейные

радиосигналов	отражения/гармоники)
3. Эндоскоп	в. Наличие радиопередачи/радиоизлучения в контролируемом диапазоне
4. Металлодетектор	г. Визуальный осмотр труднодоступных полостей/пространств

В2. Лабораторная работа

Лабораторная работа «Исследование акустического и виброакустического каналов утечки информации»

Цель работы:

- Исследовать эффективность пассивного и активного противодействия утечке речевой информации по акустическому и виброакустическому каналу.
- Изучение способов работы с многофункциональным поисковым прибором ST -031 «Пиранья» в области акустических и виброакустических измерений.
- Знакомство с системой виброакустической защиты (СВАЗ) путем постановки маскирующей помехи «Соната» и пассивным экранированием акустического и виброакустического каналов утечки конфиденциальной информации.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Тестовые задания

Прочтите текст задания и выберите один верный ответ

Описание ситуации: Требуется защитить обсуждаемую речевую информацию от съёма за пределами помещения. Известно, что основной риск — акустический технический канал.

Задание: Что является профильным средством для снижения разборчивости речи за пределами помещения?

Варианты ответов:

- а. Установка системы предотвращения вторжений (IPS)
- б. Акустическое шумление (генераторы шума) и/или повышение звукоизоляции ограждающих конструкций
- в. Настройка прав на файловом сервере
- г. Включение макросов только по подписанным шаблонам

Прочтите текст задания и выберите один верный ответ

Описание ситуации: В комнате конфиденциальные переговоры слышны в соседнем помещении через дверь и вентиляционное отверстие.

Задание: Какой технический канал утечки наиболее явно проявляется по описанию?

Варианты ответов:

- а. Акустический (и частично виброакустический) канал утечки
- б. Сетевой канал утечки через интернет
- в. Криптографический канал (слабые алгоритмы)
- г. Канал утечки через резервные копии

С2. Кейс задача

«В поисках источника утечки информации»

Задача :

1. Составить логическую схему базы знаний по содержанию блока.
2. Составить терминологический словарь.
3. Выполнить все пункты, перечисленные в разделе подготовительного этапа к занятию.

Цели: 1. Закрепить и углубить изучаемый материал студентами.

2. Уметь изложить свою точку зрения по проблемным вопросам инженерно-технической защиты информации.

Участники: Студенты распределены на 3 подгруппы:

1-я подгруппа – сотрудники технической группы службы безопасности;

2-я подгруппа – специалисты по добыванию информации различными способами (в том числе и незаконными);

3-я подгруппа – экспертная группа.

Время: 90 минут.

1. Подготовительный этап (домашняя работа):

1. Подготовить материал по ранее выданной преподавателем проблеме:

- составить план блока;

- составить терминологический словарь: выписать встречаемые в тексте блока термины и дать им расшифровку;

- выбрать одно из предприятий (хранилища и депозитарии банков; предприятия по производству или хранилища химически опасных, наркотических и взрывчатых веществ, боеприпасов ядерных материалов; предприятия оборонного профиля; правительственные учреждения; энергетические комплексы, кассовые залы банков; подъезды инкассаторских машин; помещения для хранения и работы с важной защищаемой информацией; торговые центры по продаже ценных товаров; производственные помещения для изготовления ценной продукции, торговые залы магазинов; служебные помещения учреждений; офисы среднего и малого бизнеса; производственные помещения общего назначения; жилые помещения и т.д.);

2. Исходя из содержания блока, составить применительно к выбранному объекту до десяти вопросов:

- а) сотрудникам технической группы службы безопасности, касающиеся обеспечения безопасности объекта;

б) специалистам по добыванию информации различными способами (в том числе и незаконными), касающиеся способов несанкционированного вторжения на объект, подслушивания, перехвата и т.п.

3. Быть готовыми ответить на любые поставленные вопросы со стороны подгруппы сотрудников технической группы службы безопасности, подгруппы специалистов по добыванию информации различными способами (в том числе и незаконными). Уметь оценить вопросы и ответы участников будучи в подгруппе экспертов.

4. Быть готовыми ответить на вопросы помещенные в конце блока.

5. Оформить работу в виде отчета.

2. Порядок проведения занятия

1. Организация занятия (проверка присутствующих и готовности к занятиям, объявление темы исходя из содержания текущего занятия). (5 минут.)

2. Распределение на подгруппы и доведение порядка проведения занятия. (5 минут.)

3. Присвоение подгруппам первоначальных ролей (сотрудники технической группы службы безопасности, специалисты по добыванию информации различными способами (в том числе и незаконными), экспертная группа). (5 минут.)

4. Обсуждение студентами подгрупп вопросов, вынесенных на практическое занятие с целью выработки общих позиций:

4.1. Вопросы со стороны подгруппы выступающих в роли сотрудников технической группы службы безопасности. (15 минут.)

4.2. Вопросы со стороны подгруппы выступающих в роли специалистов по добыванию информации. (15 минут.)

4.3. Вопросы со стороны подгруппы экспертов. (15 минут.)

4.4. Ответы и дискуссии. (10 минут.)

4.5. Выработка общей позиции и общего подхода к вопросам рассматриваемым на текущем занятии согласно его теме. (5 минут.)

5. Обсуждение преподавателем и старшими групп оценок участников занятия. (5 минут.)

6. Подведение итогов занятия с объявлением окончательных оценок участников занятия. (5 минут.)

7. Объявление проблемы и содержания следующего занятия. (5 минут.)

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Перечень экзаменационных вопросов

22. Структурирование информации.

23. Классификация демаскирующих признаков.

24. Оознавательные признаки и признаки деятельности.

25. Видовые демаскирующие признаки.

26. Демаскирующие признаки сигналов.

27. Демаскирующие признаки веществ. Именные, прямые и косвенные демаскирующие признаки.
28. Виды источников и носителей информации.
29. Прямые и косвенные источники семантической информации.
30. Принципы записи и съема информации с её носителя.
31. Источники функциональных сигналов. Понятие модуляции, манипуляции, демодуляции.
32. Побочные электромагнитные излучения и наводки Угрозы утечки информации. Угрозы преднамеренных воздействий. Угрозы случайных воздействий.
33. Технические каналы утечки информации: наблюдение, подслушивание, перехват.
34. Источники угроз безопасности информации.
35. Опасные сигналы и их источники.

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов, полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции(й) по дисциплине складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции(й) в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции(й) обучающихся на экзамене (максимум – 30 баллов).

Для студентов очно-заочной формы обучения применяются 4-балльная и бинарная шкалы оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

уровни освоения компетенций	продвинутый уровень	базовый уровень	пороговый уровень	допороговый уровень
------------------------------------	----------------------------	------------------------	--------------------------	----------------------------

100 – балльная шкала	85 и $\geq$	70 – 84	51 – 69	0 – 50
4 – балльная шкала	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»

**Шкала оценок при текущем контроле успеваемости
по различным показателям**

<i>Показатели оценивания сформированности компетенций</i>	<i>Баллы</i>	<i>Оценка</i>
Выполнение лабораторных работ	0-15	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение практических заданий	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Решение ситуационных задач (кейсов)	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Ответы на устные вопросы	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

**Соответствие критериев оценивания уровню освоения компетенций
по текущему контролю успеваемости**

<i>Баллы</i>	<i>Оценка</i>	<i>Уровень освоения компетенций</i>	<i>Критерии оценивания</i>
0-50	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины
51-69	«удовлетворительно»	Пороговый уровень	Не менее 50% заданий, подлежащих текущему контролю успеваемости,

			выполнены без существенных ошибок
70-84	«хорошо»	Базовый уровень	Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок
85-100	«отлично»	Продвинутый уровень	100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами

Шкала оценок по промежуточной аттестации

<i>Наименование формы промежуточной аттестации</i>	<i>Баллы</i>	<i>Оценка</i>
Экзамен	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

<i>Баллы</i>	<i>Оценка</i>	<i>Уровень освоения компетенций</i>	<i>Критерии оценивания</i>
0-9	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы

10-16	«удовлетворительно»	Пороговый уровень	Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме.
17-23	«хорошо»	Базовый уровень	Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по дисциплине компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примерами; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала и полностью выполнил практические задания
25-30	«отлично»	Продвинутый уровень	Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал и выполняет практические задания с подробными пояснениями и аргументированными выводами

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий включает 30 вопросов.

Методика оценивания выполнения тестов

Баллы	Оценка	Показатели	Критерии
25-30	«отлично»	1. Полнота выполнения тестовых заданий; 2. Своевременность выполнения; 3. Правильность ответов	Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос
19-24	«хорошо»	на вопросы; 4. Самостоятельность тестирования; 5. и т.д.	Выполнено более 70 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др.
15-18	«удовлетворительно»		Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.
0-14	«неудовлетворительно»		Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Ответы на ситуационные задачи (кейс-задачи) оформляются студентом в письменном виде и сдаются преподавателю в электронной форме с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного

университета народного хозяйства.

На решение каждой кейс-задачи отводится 45 минут. Представленный ответ должен отражать однозначную позицию по поставленной задаче.

Методика оценивания решения ситуационных (кейс) задач

Баллы	Оценка	Показатели	Критерии
9-10	«отлично»	1. Полнота решения кейс-задач; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. и т.д.	Основные требования к решению кейс-задач выполнены. Продемонстрированы умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для уточнения ситуации, навыки четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения;
7-8	«хорошо»		Основные требования к решению кейс-задач выполнены, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений
5-6	«удовлетворительно»		Имеются существенные отступления от решения кейс-задач. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
0-4	«неудовлетворительно»		Задача кейса не раскрыта, обнаруживается существенное непонимание проблемы

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдая очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до отдельного аспекта обсуждаемой темы.

Методика оценивания ответов на устные вопросы

<i>Баллы</i>	<i>Оценка</i>	<i>Показатели</i>	<i>Критерии</i>
5	«отлично»	1. Полнота данных ответов; 2. Аргументированность данных ответов; 3. Правильность ответов на вопросы; 4. и т.д.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные. Изложение материала последовательно и правильно.
3-4	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
1-2	«удовлетворительно»		Студент обнаруживает знание и понимание основных положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.
0	«неудовлетворительно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в

			<i>формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал; отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.</i>
--	--	--	--

Практические задания выполняются непосредственно во время занятий семинарского типа (одно задание на одну пару согласно текущей тематике занятия). Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности представленного решения. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения задания, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения практических заданий

Баллы	Оценка	Показатели	Критерии
9-10	«отлично»	1. Полнота выполнения заданий 2. Выполнение дополнительных заданий 3. Подготовка отчета	- задание выполнено правильно и в полном объеме в соответствии с требованиями; - в логических рассуждениях нет ошибок, задание выполнено рациональным способом. - своевременно предоставлен отчет о выполнении работы.
7-8	«хорошо»		- задание выполнено правильно и в полном объеме в соответствии с требованиями; - в логических рассуждениях, в выборе способов выполнения нет ошибок, но задание решено нерациональным способом или допущено не более двух несущественных ошибок. - своевременно предоставлен отчет о выполнении работы.
5-6	«удовлетворительно»		- Задание выполнено с подсказками преподавателя. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, но

		допущены существенные ошибки при расчетах; - задание выполнено не полностью или в общем виде.; - несвоевременно предоставлен отчет о выполнении работы.
0-4	«неудовлетворительно»	- выполнено менее 50% лабораторной работы; - не выполнены дополнительные задания; - отчет о выполнении работы не предоставлен

Лабораторные работы выполняются в специализированной аудитории во время лабораторных занятий. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения лабораторных работ

Баллы	Оценка	Показатели	Критерии
13-15	«отлично»	1. Полнота выполнения заданий 2. Выполнение дополнительных заданий 3. Подготовка отчета	- правильно выполнены все задания лабораторной работы в соответствии с требованиями; - правильно выполнены дополнительные задания; - своевременно предоставлен отчет о выполнении работы.
10-12	«хорошо»		- правильно выполнены все задания в основной части; - дополнительные задания выполнены не в полном объеме; - предоставлен отчет о выполнении работы, либо в случае несвоевременного предоставления отчета или с наличием несущественных ошибок в выполнении лабораторных заданиях
6-9	«удовлетворительно»		- выполнены не все, но более 50% заданий лабораторной работы; - дополнительные задания не выполнены, - несвоевременно предоставлен

		отчет о выполнении работы.
0-5	«неудовлетворительно»	- выполнено менее 50% лабораторной работы; - не выполнены дополнительные задания; - отчет о выполнении работы не предоставлен

Процедура промежуточной аттестации проходит в соответствии с Положением о промежуточной аттестации знаний студентов и учащихся ДГУНХ.

Аттестационные испытания проводятся преподавателем, ведущим лекционные занятия по данной дисциплине, или преподавателями, ведущими практические и лабораторные занятия (кроме устного экзамена). Присутствие посторонних лиц в ходе проведения аттестационных испытаний без разрешения ректора или проректора по учебной работе не допускается (за исключением работников университета, выполняющих контролирующие функции в соответствии со своими должностными обязанностями). В случае отсутствия ведущего преподавателя аттестационные испытания проводятся преподавателем, назначенным письменным распоряжением по кафедре (структурному подразделению).

Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения опорно-двигательного аппарата, допускаются на аттестационные испытания в сопровождении ассистентов-сопровождающих.

Во время аттестационных испытаний обучающиеся могут пользоваться программой дисциплины, а также с разрешения преподавателя справочной и нормативной литературой, непрограммируемыми калькуляторами.

**Лист актуализации оценочных материалов по дисциплине
«Защита информации от утечки по техническим каналам»**

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____» _____ 20____ г. № _____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____» _____ 20____ г. № _____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____» _____ 20____ г. № _____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____» _____ 20____ г. № _____

Зав. кафедрой _____