МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Защита информации от утечки по техническим каналам

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Защита информации от утечки по техническим каналам", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-15 - Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Осуществляет администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем от утечки по техническим каналам

Результаты обучения по дисциплине:

Знать технические каналы утечки информации; способы и средства зашиты информации от утечек по техническим каналам; возможности технических разведок.

Уметь анализировать и оценивать угрозы информационной безопасности объекта; применять нормативные документы по метрологии, стандартизации и сертификации па практике.

Владеть методами технической защиты информации; навыками обеспечения безопасности информации с помощью типовых программных и технических средств.

2 Место дисциплины "Защита информации от утечки по техническим каналам" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Нормативные требования по защите информации, Основы информатики, организации ЭВМ, вычислительных и информационных систем, Информационные угрозы, Методы и средства защиты информационных систем, Методы обнаружения угроз безопасности информационных систем.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Защита информации от утечки по техническим каналам" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Защита информации от утечки по техническим каналам" составляет 5 зачетных единиц, 180 часов.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 5/Семестр 10			
Всего часов	180		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	16		
Лабораторные занятия			
Практические занятия	32		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Самостоятельная работа под руководством преподавателя	32		
Самостоятельная работа	64		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Защита информации от утечки по техническим каналам", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
1. Современные угрозы и модели каналов утечки информации 1.1. Источники, носители, методы и средства разведки, защищаемой информации: Понятие угрозы безопасности информации. Виды угроз и возможные пути их проявления. Показатели оценивания безопасности информации. Основные признаки обеспечения безопасности информации. Источники, носители и несанкционированные получатели информации. Виды источников и носителей информации. Сигналы как материальные носители информации. Классификация сигналов. Источники опасных сигналов. Параметры модулированных сигналов. Геометрическое, спектральное и временное представление сигналов. Сигналы как случайные процессы. Характеристика и возможные действия технических разведок и служб противодействия техническим разведкам. Характеристика современных средств несанкционированного доступа к информации. 1.2. Физические основы и особенности образования технических каналов утечки информации: Понятие о каналах несанкционированного получения информации, причинах нарушения целостности информации и технических каналах утечки информации (ТКУИ). Классификация ТКУИ. Физические основы электромагнитных каналов утечки информации. Основные свойства электромагнитного поля, элементарные источники побочных электромагнитных излучений (ПЭМИ). Источники возникновения и характер помеховых электромагнитных излучений (ЭМИ). ЭМИ на частотах работы высокочастотных генераторов и на частотах самовозбуждения усилителей низкой чистоты (УНЧ). Наводки информационных сигналов ТСПИ на цепи питания, цепи заземления, абонентские линии связи, а также на посторонние провода и кабели, гальванически не связанные со средствами обработки информации, но проходящие в непосредственной близости от них. Физические основы возникновения технических каналов утечки акустической информации (ТКУАИ). Классификация ТКУАИ. Воздушные и вибрационные ТКУАИ. Оптико-электронные и акустоэлектрические ТКУАИ. Несанкционированный доступ к информации передаваемой по линии связи.	4

2. Методы и средства защиты информации от утечки по техническим каналам. 2.1. Основные положения современной концепции защиты информации техническими средствами: Основные направления инженерно-технической защиты информации. Задачи и принципы инженерно-технической защиты информации. Характеристика зонового принципа защиты информации. 2.2. Методы и средства защиты информации обрабатываемой ТСПИ от утечки по техническим каналам: Пассивные методы защиты информации, обрабатываемой ТСПИ: экранирование технических средств, заземление технических средств, фильтрация информационных сигналов. Экологически чистые технологии пассивной защиты информации. Активные методы и средства защиты информации, обрабатываемой ТСПИ. Методы и средства пространственного и линейного зашумления. 2.3. Методы и средства защиты акустической информации от утечки по техническим каналам: Задачи, решаемые пассивными методами защиты акустической информации. Звукоизоляция помещений. Акустические экраны. Звукопоглощающие материалы. Звукоизолирующая способность различных конструкций. Задачи, решаемые активными методами защиты акустической информации. Виброакустическая маскировка. Современные средства виброакустической защиты. Методы и средства защиты акустической информации, передаваемой по телефонным линиям.	4
3. Контроль эффективности защиты информации от ее утечки по техническим каналам 3.1. Особенности обработки информации при инструментальном контроле эффективности ее защиты: Основные виды погрешностей измерений и погрешностей средств измерений, оказывающих влияние на качество обработки информации при оценивании эффективности ее защиты. Обработка результатов прямых однократных измерений при инструментальном контроле эффективности ее защиты. Обработка результатов прямых многократных измерений параметров, оценивающих эффективность защиты информации. Обработка результатов косвенного инструментального контроля эффективности защиты информации. 3.2. Методы и средства контроля эффективности защиты информации: Методы и средства контроля эффективности защиты информации от ее утечки по электромагнитным каналам. Измерительные антенны. Калибровка измерительных антенн. Методы и средства измерения параметров опасных сигналов в электромагнитном поле. Современные средства автоматизации измерений при специсследованиях технических средств. Методы и средства оценивания эффективности защиты акустической информации от утечки по виброакустическим каналам с использованием инструментальных средств.	4

4. Организация работ по защите информации от утечки по техническим каналам 4.1 Основы проектирования защиты объектов информатизации: Понятие о моделировании объектов защиты информации. Проектирование защиты информации: определение требований к защите информации; анализ условий защиты информации; выявление возможных ТКУИ; оценивание защищенности информации от утечки по возможным ТКУИ; выбор средств защиты информации; документальное оформление проекта защиты информации. Разработка элементов проекта защиты информации на объекте информатизации. 4.2. Методы и средства поиска и нейтрализации несанкционированного съема информации: Методы и средства поиска с использованием индикаторов, радиочастотомеров. Сканирующие приемники и анализаторы спектра для поиска устройств перехвата информации. Программно-аппаратные комплекты радиоконтроля. Методы поиска устройств съема информации с использованием нелинейных локаторов, металлоискателей, рентгеновских аппаратов. Средства и методы контроля проводных линий. Специальные проверки служебных помещений. Программа организации работ.	4
Итого	**16**

4.2. Практические занятия

Наименование работы Вид СРС	**Трудоемкость в часах**
	ОФ
1. Маскировка: Техническая реализация маскировки средств вычислительной техники	2
2. Обнаружение радиозакладок: Статистический анализ загрузки заданного диапазона и обнаружение закладок в помещении	2
3. Сетевые закладки: Обнаружение сигналов линейных и сетевых закладок	2
4. ИК-диапазон: Анализ ИК диапазона	2
5. Анализ поля: Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля	2
6. ПЭМИН по электрической составляющей: Обнаружение ПЭМИН по электрической составляющей электромагнитного поля	2
7. ПЭМИН по магнитной составляющей: Обнаружение ПЭМИН по магнитной составляющей электромагнитного	2
8. Измерение наводок в цепях электропитания: Обнаружение ПЭМИН в электрических цепях	2
9. Акустический канал: Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу	4
10. Виброакустический канал: Оценка защищенности ограждающих конструкций помещения от утечки информации по виброакустическому каналу	2

11. Электроакустический канал: Оценка защищенности ограждающих конструкций помещения от утечки информации по электроакустическому каналу	2
12. Защита виброакустического канала	2
13. Блокирование сотовых телефонов: Блокирование GSM 900/1800, E-GSM, CDMA2000 1X, NMT-450i	2
14. Блокирование Bluetooth и Wifi диапазонов	2
15. Пропускной контроль	2
Итого	**32**

4.3 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Наименование работы Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	34
Оформление отчетов по практическим и(или) лабораторным работам	24
Подготовка к промежуточной аттестации	6
Итого	**64**
Самостоятельная работа под руководством преподавателя	32
Экзамен	36

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Защита информации от утечки по техническим каналам"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**

Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-15 - Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Осуществляет администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем от утечки по техническим каналам.	**Знать** технические каналы утечки информации; способы и средства зашиты информации от утечек по техническим каналам; возможности технических разведок. **Уметь** анализировать и оценивать угрозы информационной безопасности объекта; применять нормативные документы по метрологии, стандартизации и сертификации па практике. **Владеть** методами технической защиты информации; навыками обеспечения безопасности информации с помощью типовых программных и технических средств.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов

- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:
- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

1. Современные угрозы и модели каналов утечки информации

1. В каком ГОСТ описана общая классификация угроз безопасности информации, составляющей коммерческую тайну?
2. Изобразите модель нарушения информационной безопасности, разместив в середине схемы ПК, подключенный к компьютерной сети, а от него стрелки, изображающие каналы утечки информации
3. Перечислите технические каналы утечки информации, классифицировав их по физической природе
4. Классифицируйте оборудование, позволяющее добыть информацию по техническим каналам утечки информации
5. Приведите классификацию угроз безопасности конфиденциальной информации

2. Методы и средства защиты информации от утечки по техническим каналам.

1. Комплекс каких мероприятий представляет собой защита информации от утечки по техническим каналам?
2. Приведите пример активных и пассивных мероприятий, обеспечивающих защиту информации от утечки по техническим каналам
3. Что представляют собой конструкторско-технологические мероприятия по защите информации от утечки по техническим каналам? Какова их цель?
4. Что представляет собой параметр «прочность средства защиты» и как он рассчитывается?
5. Модели многозвенной и многоуровневой защиты. Их принципиальные отличия, преимущества и недостатки

3. Контроль эффективности защиты информации от ее утечки по техническим каналам

1. Перечислите основные виды контроля эффективности защиты информации
2. Виды контроля защищенности объектов от разведки ПЭМИН
3. Что представляет собой средство контроля эффективности защиты информации?
4. Какие технические показатели используются для оценки эффективности принятых мер защиты?
5. В каких случаях используют инструментально-расчетные методы для оценки эффективности принятых мер защиты?

4. Организация работ по защите информации от утечки по техническим каналам

1. Опишите типовой алгоритм использования / внедрения средств защиты информации от утечки по техническим каналам
2. В чем заключается стратегия и тактика защиты от преднамеренного несанкционированного доступа к информации по техническим каналам?
3. На основе чего определяется перечень организационно-административных мер по защите информации?
4. На кого возлагается организация работ по защите информации?
5. Лицензия какой федеральной структуры должна быть у организации, занимающейся разработкой и

внедрением средств технической защиты информации?

Примерный перечень тестовых заданий:

1. Современные угрозы и модели каналов утечки информации

1. По каким техническим каналам возможен перехват речевой информации без проникновения в пределы КЗ объекта: выбрать все верные

А) Прямые акустические технические каналы утечки информации.
Б) Акустовибрационный технический канал утечки информации.
В) Акустооптический технический канал утечки информации.
Г) Акустоэлектрический технический канал утечки информации.
Д) Акустоэлектромагнитный технический канал утечки информации

2. В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?

оптический
радиоэлектронный
акустический
материально-вещественный

3. Каналы, в которых утечка информации носит случайный разовый характер, называются:

постоянные
периодические
эпизодические
неконтролируемые

2. Методы и средства защиты информации от утечки по техническим каналам.

1. Как называются технические средства защиты, которые ослабляют уровень информативного сигнала?

активные
пассивные
динамические
демаскирующие

2. Выделите технические мероприятия с использованием активных средств защиты информации:

звукоизоляция
пространственное зашумление
линейное зашумление
заземление
экранирование

3. Какое зашумление используется для исключения перехвата ПЭМИН по электромагнитному каналу?

пространственное
параллельное
последовательное
линейное

3. Контроль эффективности защиты информации от ее утечки по техническим каналам

1. На какие типы разделяется контроль эффективности защиты информации?

организационный контроль эффективности защиты информации
программный контроль эффективности защиты информации
нормативный контроль эффективности защиты информации
технический контроль эффективности защиты информации

2. При оценке защищенности информации по методике оценки реального затухания в

техническом канале информация считается защищенной, если…

значение максимального пробега наведенного информативного сигнала больше пробега исследуемой линии до границы контура защиты
значение максимального пробега наведенного информативного сигнала меньше пробега исследуемой линии до границы контура защиты
значение минимального пробега наведенного информативного сигнала больше пробега исследуемой линии до границы контура защиты
значение минимального пробега наведенного информативного сигнала меньше пробега исследуемой линии до границы контура защиты

3. Аудит / контроль эффективности защиты информации в организации может осуществляться:

независимой организацией (третьей стороной) по договору с проверяемой организацией,
подразделением или должностным лицом организации
оба варианта верны

4. Организация работ по защите информации от утечки по техническим каналам

1. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
Улучшить контроль за безопасностью этой информации
Снизить уровень классификации этой информации

2. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Поддержка высшего руководства
Эффективные защитные меры и методы их внедрения
Актуальные и адекватные политики и процедуры безопасности
Проведение тренингов по безопасности для всех сотрудников

3. Эффективная программа безопасности требует сбалансированного применения:

Технических и нетехнических методов
Контрмер и защитных механизмов
Физической безопасности и технических средств защиты
Процедур безопасности и шифрования

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации являютя экзамен, в процессе которого определяется

сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:
- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:
- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. Способы и принципы работы средств защиты информации от наблюдения.
2. Способы и средства противодействия наблюдению в оптическом диапазоне волн.
3. Способы информационного скрытия объектов от радиолокационного наблюдения.
4. Классификация объектов информатизации.
5. Экранирование технических средств их соединительных линий.
6. Экранированные помещения.
7. Заземление технических средств.
8. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке).
9. Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке).
10. Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства.
11. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы.
12. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.
13. Способы и принципы работы средств защиты информации от перехвата.
14. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей.
15. Способы и принципы работы средств защиты информации от подслушивания.
16. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов,

глушителей.

17. Способы и средства предотвращения утечки информации с помощью закладных устройств. Показатели эффективности защиты речевой информации.
18. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений;
19. Порядок проведения измерений уровня звуко- и виброизоляции.
20. Методика расчета словесной разборчивости речи.
21. Методика оценки возможностей средств акустической разведки по перехвату речевой информации.
22. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.
23. Организационные и технические меры инженерно-технической защиты информации.
24. Контроль эффективности защиты информации. рекомендации по выбору средств защиты информации
25. Способы перехвата речевой информации из защищаемых помещений по прямому акустическому каналу.
26. Способы перехвата речевой информации из защищаемых помещений по акустовибрационным каналам.
27. Способы перехвата речевой информации из защищаемых помещений по акустооптическому каналу.
28. Способы перехвата речевой информации из защищаемых помещений по акустоэлектрическим каналам.
29. Классификация способов и средств защиты конфиденциальной информации от утечки по техническим каналам
30. 1.Пассивные способы и средства защиты конфиденциальной информации от утечки по техническим каналам.
31. Активные способы и средства защиты конфиденциальной информации от утечки по техническим каналам.
32. Основные характеристики систем линейного электромагнитного зашумления.
33. Способы и средства защиты конфиденциальной информации от утечки по цепям электропитания и заземления.
34. Классификация способов и средств защиты речевой конфиденциальной информации по техническим каналам.
35. Пассивные способы защиты речевой конфиденциальной информации от утечки по техническим каналам.
36. Активные способы защиты речевой конфиденциальной информации от утечки по техническим каналам.
37. Системы и средства виброакустической маскировки
38. Средства защиты речевой конфиденциальной информации от утечки по акустоэлектрическим каналам в ВТСС.
39. Пассивные способы защиты речевой конфиденциальной информации от утечки по акустоэлектрическим каналам в ВТСС.
40. Активные способы защиты речевой конфиденциальной информации от утечки по акустоэлектрическим каналам в ВТСС.
41. Принципы построения средств защиты конфиденциальной информации в ВТСС, основанных на использовании ограничителей малой амплитуды и фильтров нижних частот.
42. Принципы построения средств защиты конфиденциальной информации в ВТСС, основанных на отключении акустоэлектрических преобразователей.

Примерный перечень тестовых заданий на экзамен:

1. По каким техническим каналам возможен перехват речевой информации без проникновения в пределы КЗ объекта: выбрать все верные

А) Прямые акустические технические каналы утечки информации.
Б) Акустовибрационный технический канал утечки информации.
В) Акустооптический технический канал утечки информации.
Г) Акустоэлектрический технический канал утечки информации.
Д) Акустоэлектромагнитный технический канал утечки информации

2. В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?

оптический
радиоэлектронный
акустический
материально-вещественный

3. Каналы, в которых утечка информации носит случайный разовый характер, называются:

постоянные
периодические
эпизодические
неконтролируемые

4. Как называются технические средства защиты, которые ослабляют уровень информативного сигнала?

активные
пассивные
динамические
демаскирующие

5. Выделите технические мероприятия с использованием активных средств защиты информации:

звукоизоляция
пространственное зашумление
линейное зашумление
заземление
экранирование

6. Какое зашумление используется для исключения перехвата ПЭМИН по электромагнитному каналу?

пространственное
параллельное
последовательное
линейное

7. На какие типы разделяется контроль эффективности защиты информации?

организационный контроль эффективности защиты информации
программный контроль эффективности защиты информации
нормативный контроль эффективности защиты информации
технический контроль эффективности защиты информации

8. При оценке защищенности информации по методике оценки реального затухания в техническом канале информация считается защищенной, если…

значение максимального пробега наведенного информативного сигнала больше пробега исследуемой линии до границы контура защиты
значение максимального пробега наведенного информативного сигнала меньше пробега исследуемой линии до границы контура защиты
значение минимального пробега наведенного информативного сигнала больше пробега исследуемой линии до границы контура защиты
значение минимального пробега наведенного информативного сигнала меньше пробега исследуемой линии до границы контура защиты

9. Аудит / контроль эффективности защиты информации в организации может осуществляться:

независимой организацией (третьей стороной) по договору с проверяемой организацией,
подразделением или должностным лицом организации
оба варианта верны

0. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
Улучшить контроль за безопасностью этой информации
Снизить уровень классификации этой информации

11. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Поддержка высшего руководства
Эффективные защитные меры и методы их внедрения
Актуальные и адекватные политики и процедуры безопасности
Проведение тренингов по безопасности для всех сотрудников

12. Эффективная программа безопасности требует сбалансированного применения:

Технических и нетехнических методов
Контрмер и защитных механизмов
Физической безопасности и технических средств защиты
Процедур безопасности и шифрования

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в

семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А. М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636 (дата обращения: 17.04.2026). – Библиогр.: с. 213. – Текст : электронный.

2. Иванов, А. В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок : учебное пособие : [16+] / А. В. Иванов. – Новосибирск : Новосибирский государственный технический университет, 2018. – 64 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575420 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-3713-1. – Текст : электронный.

6.2 Дополнительная литература

1. Иванов, А. В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок : [учебное пособие] / А. В. Иванов ; А. В. Иванов ; Новосибирский государственный технический университет, Факультет автоматики и вычислительной техники. – Новосибирск : Изд-во НГТУ, 2018. – 1 файл (4,7 Мб). – URL: http://library.kuzstu.ru/meto.php?n=239355.pdf&type=nstu:common (дата обращения: 23.03.2026). – Текст : электронный.

2. Иванов, А. В. Оценка защищенности информации от утечки по виброакустическим каналам : учебное пособие : [16+] / А. В. Иванов. – Новосибирск : Новосибирский государственный технический университет, 2018. – 76 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575421 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-3712-4. – Текст : электронный.

3. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Иванов, А. В. Защита речевой информации от утечки по акустоэлектрическим каналам : учебное пособие : [16+] / А. В. Иванов, В. А. Трушин ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2012. – 43 с. : ил.,табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=228846 (дата обращения: 15.04.2026). – ISBN 978-5-7782-1888-8. – Текст : электронный.

6.3 Методическая литература

1. Системы защиты от утечки конфиденциальной информации : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 7 с. – URL: http://library.kuzstu.ru/meto.php?n=9106 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
4. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
5. Образовательная платформа «Юрайт» https://urait.ru/
6. Электронная библиотека "Эксперт" Системы Технорматив https://gost.online/index.htm
7. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
8. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Информационные системы и технологии : научно-технический журнал https://eivis.ru/browse/publication/542286
2. Информационные технологии и вычислительные системы : журнал https://elibrary.ru/contents.asp?titleid=8746
3. Информация и безопасность : научный журнал
4. Программные продукты и системы : международный научно-практический журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Защита информации от утечки по техническим каналам"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой

аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Защита информации от утечки по техническим каналам", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Mozilla Firefox
2. Google Chrome
3. 7-zip
4. Microsoft Windows
5. ESET NOD32 Smart Security Business Edition
6. Kaspersky Endpoint Security
7. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Защита информации от утечки по техническим каналам"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.