МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»
Первый проректор-
проректор по ОД
И.Т. Гайрабеков
_____
«26» 06 2026г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ»

Направление подготовки

10.03.01 *«Информационная безопасность»*

Направленность (профиль)

«*Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*»

Квалификация

бакалавр

Год начала подготовки – 2026

Грозный – 2026

1. Цели и задачи дисциплины

Целью дисциплины «Защита информации от утечки по техническим каналам» является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в защищаемых помещениях, изучение студентами технических средств защиты конфиденциальной информации, методов и технических средств съема информации, методов и средств контроля эффективности принимаемых мер защиты информации.

Задачи дисциплины «Аппаратные средства вычислительной техники»:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- ознакомление с техническими каналами утечки акустической (речевой) информации;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Защита информации от утечки по техническим каналам» входит в обязательную часть Блока 1 подготовки бакалавров по направлению подготовки 10.03.01 Информационная безопасность, изучается в четвертом семестре второго курса, обучение длится один семестр. Форма итогового контроля: экзамен – 4 семестр.

Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):

1. Физика;
2. Информатика.
3. Электротехника;
4. Безопасность жизнедеятельности;

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Таблица 1

Код по ОП	**Индикаторы достижения**	**Планируемые результаты обучения по дисциплине (ЗУВ)**
	Общепрофессиональные	
ОПК-9 способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	**ОПК-9.1.** Знать: принципы работы средств криптографической и технической защиты информации для решения стандартных задач профессиональной деятельности **ОПК-9.2.** Уметь: применять программные программно-аппаратные криптографические и технические средства защиты информации для решения задач профессиональной деятельности **ОПК-9.3**. Владеть: навыками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	**Знать**: принципы работы средств криптографической и технической защиты информации для решения стандартных задач профессиональной деятельности **Уметь**: применять программные программно-аппаратные криптографические и технические средства защиты информации для решения задач профессиональной деятельности **Владеть**: навыками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности,	**ОПК-10.1.** Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности. **ОПК-10.2**. Уметь: в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять	**Знать:** основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности. **Уметь:** в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению

управлять процессом их реализации на объекте защиты	процессом их реализации на объекте защиты. **ОПК-10.3**. Владеть: методами формирования и выполнения комплекса мер по информационной безопасности.	информационной безопасности, управлять процессом их реализации на объекте защиты. **Владеть:** методами формирования и выполнения комплекса мер по информационной безопасности.

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы		**Всего часов/ зач. ед.**		**Семестры**	
				6	**6**
		ОФО	**ОЗФО**	**ОФО**	**ОЗФО**
Контактная работа (всего)		**48/1,3**	**48/1,3**	**48/1,3**	**48/1,3**
В том числе:					
Лекции		16/0,4	16/0,4	16/0,4	16/0,4
Практические занятия		-	-	-	-
Семинары		-	-	-	-
Лабораторные работы		32/0,8	32/0,8	32/0,8	32/0,8
Самостоятельная работа (всего)		**60/1,6**	**60/1,6**	**60/1,6**	**60/1,6**
В том числе:					
Курсовая работа (проект)					
ИТР					
Рефераты		20/0,5	20/0,5	20/0,5	20/0,5
Работа над проектом		20/0,5	20/0,5	20/0,5	20/0,5
И (или) другие виды самостоятельной работы:					
Подготовка к лабораторным работам		10/0,3	10/0,3	10/0,3	10/0,3
Подготовка к практическим работам					
Подготовка к зачету		10/0,3	10/0,3	10/0,3	10/0,3
Подготовка к экзамену					
Контроль		-	-	-	-
Вид отчетности		**зачет**	**зачет**	**зачет**	**зачет**
Общая трудоемкость дисциплины	**ВСЕГО в часах**	**108**	**108**	**108**	**108**
	ВСЕГО в зач. единицах	**3**	**3**	**3**	**3**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	Наименование раздела дисциплины	Лекц. зан. часы		Лаб.зан. часы		Всего часов	
		ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
1	Объекты информационной безопасности	2	2	6	6	8	8
2	Угрозы безопасности информации	3	3	6	6	9	9
3	Методы, способы и средства инженерно-технической защиты информации	3	3	6	6	9	9
4	Организация инженерно-технической защиты информации	3	3	6	6	9	9
5	Основы методического обеспечения инженерно-технической защиты информации	3	3	8	8	9	9

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	ВВЕДЕНИЕ. Основные свойства информации как предмета технической защиты	Информация как объект защиты. Конфиденциальность, целостность и доступность. Ценность информации и последствия ее утечки. Особенности защиты речевой, визуальной и обрабатываемой техническими средствами информации
2.	Демаскирующие признаки объектов защиты	Понятие демаскирующих признаков. Информативные и побочные признаки объектов защиты. Виды сигналов и физических полей, которые могут содержать сведения о защищаемой информации.
3.	Источники и носители конфиденциальной информации	Источники информации на объектах информатизации. Технические средства обработки, хранения и передачи информации. Носители информации и возможные пути ее утечки.
4.	Источники опасных сигналов	Источники опасных информационных сигналов. Основные виды электрических, электромагнитных,

		акустических и виброакустических сигналов. Условия возникновения и распространения опасных сигналов.
5.	Виды угроз безопасности информации	Понятие угрозы безопасности информации. Классификация угроз. Угрозы утечки информации по техническим каналам. Источники угроз и факторы, влияющие на вероятность утечки.
6.	Органы и средства технической разведки	Общие сведения о технической разведке. Возможности технических средств добывания информации. Основные направления противодействия технической разведке.
7.	Технология разведки и способы несанкционированного доступа	Основные этапы добывания информации техническими средствами. Способы несанкционированного доступа к источникам информации. Меры предупреждения и обнаружения попыток съема информации.

5.3. Лабораторный практикум

Таблица 5

№ п/п	Наименование раздела	Наименование лабораторных работ
1.	ВВЕДЕНИЕ. Основные свойства информации как предмета технической защиты	Лабораторная работа №1. Анализ объекта защиты и выявление источников конфиденциальной информации.
2.	Демаскирующие признаки объектов защиты	Лабораторная работа №2. Выявление и классификация технических каналов утечки информации.
3.	Источники и носители конфиденциальной информации	Лабораторная работа №3. Анализ акустического и виброакустического каналов утечки информации.
4.	Источники опасных сигналов	Лабораторная работа №4. Анализ побочных электромагнитных излучений и наводок как канала утечки.
5.	Виды угроз безопасности информации	Лабораторная работа №5 Выбор способов и средств защиты информации от акустической и визуальной утечки.
6.	Методы, способы и редства инженерно-ехнической защиты нформации	Лабораторная работа №6 Разработка комплекса мер защиты объекта от утечки по техническим каналам.

5.4. Практические (семинарские) занятия: нет

Таблица 6

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	**-**	**-**

6. Самостоятельная работа студентов по дисциплине

Способ организации самостоятельной работы: подготовка проекта по заданной тематике, в соответствии таблицы 7

Таблица 7

№№ п/п	Тематика докладов с презентациями
1.	Технические каналы утечки информации: понятие и классификация.
2.	Демаскирующие признаки объектов защиты.
3.	Источники и носители конфиденциальной информации.
4.	Акустический канал утечки речевой информации.
5.	Виброакустический канал утечки информации.
6.	Побочные электромагнитные излучения и наводки.
7.	Электрические каналы утечки информации.
8.	Оптические и оптико-электронные каналы утечки информации.
9.	Материально-вещественный канал утечки информации.
10.	Основные способы и средства добывания информации техническими средствами.
11.	Способы и средства защиты информации от визуального наблюдения.
12.	Способы и средства защиты от подслушивания.
13.	Звукоизоляция и виброизоляция защищаемых помещений.
14.	Экранирование как метод защиты от электромагнитных излучений.
15.	Фильтрация и заземление в системе технической защиты информации.
16.	Инженерные средства защиты и техническая охрана объектов.
17.	Организационные и технические меры инженерно-технической защиты.
18.	Моделирование объекта защиты.
19.	Моделирование угроз утечки информации по техническим каналам.

Преподаватель поясняет требования к оформлению работы, предлагает тематику самостоятельной работы с использованием программного обеспечения, согласованного с преподавателем. При защите самостоятельной работы студенту необходимо представить презентацию на выполненную работу с использованием ПО MS Power Point

Учебно-методическое обеспечение для самостоятельной работы студентов:

1. Газизов А.Р. Техническая защита информации : учебное пособие / А. Р. Газизов, Д. В. Фатхи. — Ростов-на-Дону : Донской государственный технический университет, 2022. — 108 с. — ISBN 978-5-7890-2053-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/130429.html (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

2. Киренберг А.Г. Защита информации от утечки по техническим каналам : учебное пособие / А. Г. Киренберг, В. О. Коротин. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. — 221 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/135100.html (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

3. Скрипник Д.А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) ; Ай Пи Ар Медиа, 2024. — 424 с. — ISBN 978-5-4497-2415-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133955.html (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

7. Оценочные средства

7.1. Вопросы к рубежным аттестациям

***Вопросы к первой рубежной аттестации*:**

1. Основные свойства информации как предмета технической защиты.
2. Понятие объекта защиты и его основные характеристики.
3. Демаскирующие признаки объектов защиты информации.
4. Источники и носители конфиденциальной информации.
5. Источники опасных сигналов и их классификация.
6. Понятие угрозы безопасности информации.
7. Основные виды угроз безопасности информации по техническим каналам.
8. Понятие технического канала утечки информации.
9. Классификация технических каналов утечки информации.
10. Акустический канал утечки информации.
11. Виброакустический канал утечки информации.
12. Электромагнитный канал утечки информации.
13. Электрический канал утечки информации.
14. Оптический канал утечки информации.
15. Радиоканал как возможный канал утечки информации.

***Вопросы ко второй рубежной аттестации*:**

1. Концепция инженерно-технической защиты информации.
2. Основные принципы инженерно-технической защиты информации.
3. Способы и средства инженерной защиты и технической охраны.

4. Задачи технической охраны объектов информатизации.
5. Способы и средства защиты информации от наблюдения.
6. Способы и средства защиты информации от подслушивания.
7. Средства защиты речевой (акустической) информации.
8. Способы предотвращения утечки информации через побочные электромагнитные излучения.
9. Способы предотвращения утечки информации через электромагнитные наводки.
10. Способы предотвращения утечки информации по материально-вещественному каналу.
11. Общие положения по инженерно-технической защите информации в организации.
12. Организационные и технические меры инженерно-технической защиты информации.

Образцы билетов рубежных аттестаций:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информации от утечки по техническим каналам»
1-я рубежная аттестация
Группа: Семестр: 6
Билет №

1. Понятие угрозы безопасности информации
2. Оптический канал утечки информации

Преподаватель_____

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информации от утечки по техническим каналам»
2-я рубежная аттестация
Группа: Семестр: 6
Билет №

1. Способы и средства защиты информации от подслушивания
2. Основные принципы инженерно-технической защиты информации

Преподаватель_____

7.2. Вопросы к зачету

ОФО 6 семестр, ОЗФО 6 семестр

1. Цели и задачи технической защиты информации от утечки по техническим каналам.
2. Основные свойства информации как предмета технической защиты.
3. Объекты защиты информации и их демаскирующие признаки.

4. Источники и носители конфиденциальной информации.
5. Источники опасных сигналов.
6. Понятие угрозы безопасности информации и классификация угроз.
7. Технология технической разведки и ее основные этапы.
8. Способы несанкционированного доступа к источникам информации.
9. Способы и средства добывания информации техническими средствами.
10. Способы и средства наблюдения.
11. Способы и средства перехвата сигналов.
12. Способы и средства подслушивания акустических сигналов.
13. Способы и средства добывания информации о демаскирующих признаках веществ.
14. Понятие технического канала утечки информации и его структура.
15. Основные виды технических каналов утечки информации.
16. Акустический и виброакустический каналы утечки информации.
17. Электромагнитные и электрические каналы утечки информации.
18. Побочные электромагнитные излучения и наводки.
19. Оптические и радиотехнические каналы утечки информации.
20. Концепция инженерно-технической защиты информации.
21. Способы и средства инженерной защиты и технической охраны.
22. Защита информации от наблюдения.
23. Защита информации от подслушивания.
24. Защита от утечки информации через побочные электромагнитные излучения и наводки.
25. Предотвращение утечки информации по материально-вещественному каналу.
26. Организация инженерно-технической защиты информации в организации.
27. Организационные и технические меры инженерно-технической защиты.

Образец билета к зачету:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информации от утечки по техническим каналам»
Группа: Семестр: 6
Билет №

1. Предотвращение утечки информации по материально-вещественному каналу
2. Организационные и технические меры инженерно-технической защиты
3. Способы и средства перехвата сигналов

Подпись преподавателя_____ Подпись заведующего кафедрой _____

7.3. Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа № 2

Оценка уровня побочных электромагнитных излучений технических средств обработки информации

Цель работы:

Получить практические навыки выявления технического канала утечки информации, возникающего за счёт побочных электромагнитных излучений и наводок (ПЭМИН), и освоить методику оценки опасности таких излучений.

Задача:

Выполнить измерение уровня электромагнитного поля от работающего ПК (или его имитационной модели) в заданном частотном диапазоне, сравнить полученные значения с нормативными требованиями и предложить меры по снижению уровня опасных сигналов.

Задание:

1. Ознакомьтесь с теоретическими основами возникновения ПЭМИН и методами их регистрации (по материалам лекций и рекомендованной литературе).
2. Подготовьте к работе измерительное оборудование (анализатор спектра или селективный микровольтметр с измерительной антенной). Если оборудование недоступно, используйте симуляционную среду, предоставленную преподавателем, или расчётную методику с заданными параметрами источника.
3. Проведите измерение уровня сигналов ПЭМИН от исследуемого объекта (ПК или его модель) на расстоянии 1 м в следующих режимах работы:
   - режим ожидания (без активных операций);
   - режим типовой работы (запуск текстового редактора, чтение/запись файлов);
   - режим максимальной загрузки (запуск ресурсоёмкого приложения).
4. Зафиксируйте частоты, на которых наблюдаются наибольшие выбросы уровней сигнала. Заполните таблицу:

Режим работы	Частота, МГц	Уровень сигнала, дБмкВ	Примечание
Ожидание	...	...	
Типовая	...	...	
Загрузка	...	...	

5. Сравните полученные уровни с допустимыми значениями согласно нормативным документам ФСТЭК России (например, по классу защищённости).
6. Предложите меры защиты от утечки по выявленному каналу (экранирование, заземление, применение фильтров, активная маскировка). Оцените их эффективность (при наличии возможности повторного измерения или расчёта).
7. Подготовьте отчёт о проделанной работе, включающий цели, методику, таблицы результатов, графики (построить в Excel или аналогичном ПО) и выводы.

Вопросы для защиты работы:

1. Что такое ПЭМИН и каков механизм их возникновения?

2. Какие технические средства создают наибольший уровень ПЭМИН?
3. Какими приборами измеряют уровень электромагнитных излучений?
4. Какие параметры сигнала являются информативными для восстановления обрабатываемой информации?
5. Какие пассивные методы защиты от утечки по каналу ПЭМИН вы знаете?
6. В чём отличие активной защиты от пассивной?
7. Какие нормативные документы устанавливают допустимые уровни излучений?
8. Как влияет расстояние между источником и приёмником на возможность перехвата информации?
9. Как можно оценить эффективность экрана по ослаблению сигнала?
10. Для каких типов оборудования защита от ПЭМИН является обязательной по классам защищённости?

7.4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания.

Таблица 8

Планируемые результаты освоения компетенции	**Критерии оценивания результатов обучения**				**Наименование оценочного**
	менее 41 баллов (неудовлетворительно)	**41-60 баллов (удовлетворительно)**	**61-80 баллов (хорошо)**	**81-100 баллов (отлично)**	
ОПК-9 способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности					
Знать: принципы работы средств криптографической и технической защиты информации	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельны е пробелы знания	Сформированные систематические знания	Комплект заданий для выполнения лабораторных работ, темы докладов с презентациями, вопросы по темам / разделам дисциплины
Уметь: применять программные, программно-аппаратные криптографические и технические средства защиты информации для решения задач профессиональной деятельности	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками применения средств криптографической и технической защиты информации	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты					

Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельны е пробелы знания	Сформированные систематические знания	Комплект заданий для выполнения лабораторных работ, темы докладов с презентациями, вопросы по темам / разделам дисциплины
Уметь: в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: методами формирования и выполнения комплекса мер по информационной безопасности	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- **для слепых:** задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- **для слабовидящих:** обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих нарушения опорно-двигательного аппарата:**

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

1. Газизов А.Р. Техническая защита информации : учебное пособие / А. Р. Газизов, Д. В. Фатхи. — Ростов-на-Дону : Донской государственный технический университет, 2022. — 108 с. — ISBN 978-5-7890-2053-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/130429.html (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

2. Киренберг А.Г. Защита информации от утечки по техническим каналам : учебное пособие / А. Г. Киренберг, В. О. Коротин. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. — 221 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/135100.html (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей.

3. Скрипник Д.А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) ; Ай Пи Ар Медиа, 2024. — 424 с. — ISBN 978-5-4497-2415-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133955.html (дата обращения: 20.04.2025). — Режим доступа: для авторизир. пользователей

10. Материально-техническое обеспечение дисциплины

10.1. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Перечень материально-технических средств учебной аудитории для проведения занятий по дисциплине:

- учебная аудитория, доска;
- стационарные компьютеры;
- мультимедийный проектор;
- настенный экран.

10.2. Помещения для самостоятельной работы

Учебная аудитория для самостоятельной работы – 3-05.

Аудитория 3-05, интерактивная доска SB 480-H2-062616, проектор Smart v25, аппаратная Nettop.

Методические указания по освоению дисциплины
«Защита информации от утечки по техническим каналам»

1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, её структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Дисциплина «Защита информации от утечки по техническим каналам» состоит из нескольких связанных между собой разделов, обеспечивающих последовательное изучение материала: от классификации технических каналов утечки информации и физических полей-носителей до методов и средств пассивной и активной защиты, а также контроля эффективности защитных мер.

Обучение по дисциплине осуществляется в следующих формах:

1. Аудиторные занятия (лекции, лабораторные занятия).
2. Самостоятельная работа студента (подготовка к лекциям, лабораторным занятиям, работа над проектом, индивидуальная консультация с преподавателем).

Учебный материал структурирован тематически. Каждой лабораторной работе и самостоятельному изучению материала предшествует лекция по соответствующей теме. Обучающиеся самостоятельно проводят предварительную подготовку к занятию, принимают активное и творческое участие в обсуждении теоретических вопросов, разборе практических ситуаций и поиске путей их решения.

Описание последовательности действий обучающегося:

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10–15 минут).
2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10–15 минут).
3. В течение недели выбрать время для работы с литературой в электронной библиотечной системе (по 1 часу).
4. При подготовке к лабораторному занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, – предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1–2 задачи.

2. Методические указания по работе обучающихся во время проведения лекций

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах: физические основы возникновения технических каналов утечки информации (электромагнитные, акустические, виброакустические, оптические, электрические и др.), нормативно-правовая

база защиты информации, методы и средства активной и пассивной защиты, порядок проведения специальных проверок и контроля эффективности.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателем. Следует обращать внимание на акценты, выводы, которые делает преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения (например, виды каналов утечки, нормы ослабления сигналов, названия средств защиты).

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

3. Методические указания обучающимся по подготовке к лабораторным занятиям

На лабораторных занятиях приветствуется активное участие в обсуждении конкретных ситуаций по выявлению технических каналов утечки, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем (например, выбор типа экранирования, расчёт затухания сигнала, подбор средств активной маскировки), уметь находить полезный дополнительный материал по тематике занятий (методики измерений, технические характеристики оборудования).

Студенту рекомендуется следующая схема подготовки к лабораторному занятию:

1. Ознакомиться с планом занятия, который отражает содержание предложенной темы.
2. Проработать конспект лекций.
3. Прочитать основную и дополнительную литературу.

В процессе подготовки к лабораторным занятиям необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы и нормативных документов. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение к конкретной проблеме. Все новые понятия по изучаемой теме (виды каналов утечки, параметры средств защиты, нормативные требования) необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

4. Методические указания обучающимся по организации самостоятельной работы

Цель организации самостоятельной работы по дисциплине «Защита информации от утечки по техническим каналам» – это углубление и расширение знаний в области технической защиты информации, освоение методов выявления и нейтрализации каналов утечки; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к лабораторным занятиям и к контрольной работе. Сюда же относятся и самостоятельное углублённое изучение тем дисциплины (например, изучение современных средств защиты, анализ новых видов каналов утечки, освоение методик проведения специальных проверок). Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и носит исследовательский характер, что послужит в будущем основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учётом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Самостоятельная работа реализуется:

– непосредственно в процессе аудиторных занятий – на лекциях, лабораторных занятиях;

– в контакте с преподавателем вне рамок расписания – на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

– в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок
(по балльно-рейтинговой системе ГГНТУ, СРС оценивается в 15
баллов) 1. Проект с защитой
2. Подготовка к лабораторным занятиям

Темы для самостоятельной работы прописаны в рабочей программе дисциплины

Разработчик:

Старший преподаватель кафедры
«Информатика и вычислительная техника»  / Х.М.Бапаева /

СОГЛАСОВАНО:

Зав.кафедрой «Информатика
и вычислительная техника»  /Э. Д. Алисултанова/

Директор ДУМР  / М.А. Магомаева /