МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора
по учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации от утечки по техническим каналам
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Защита информации от утечки по техническим каналам» предоставить студентам теоретические знания и практические навыки по основам инженерно-технической защиты информации от утечки по техническим каналам.

Задачи изучения дисциплины. Приобретение студентами знаний, умений и практических навыков, необходимых для изучения способов реализации частных политик ИБ с применением ТСЗИ, требования к мониторингу и аудиту безопасности АС в части ТСЗИ; научиться осуществлять мониторинг и аудит безопасности АС в части ТСЗИ.

Дисциплина направлена на формирование общепрофессиональных (ПК-1) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по направлениям подготовки 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Физика», «Математика», «Электротехника», «Информатика», «Основы информационной безопасности».

Является основой для изучения следующих дисциплин: «Организация ЭВМ и вычислительных систем», «Программно-аппаратные средства обеспечения информационной безопасности».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения общепрофессиональных задач деятельности, связанных с применением вычислительных систем в области информационной безопасности.

Курс является фундаментом для ориентации студентов в сфере разработки защищенных информационных систем.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия и самостоятельная работа студента (108 ак.ч.).

Дисциплина изучается на 4 курсе в 7 семестре. Форма промежуточной аттестации – экзамен.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Защита информации от утечки по техническим каналам» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен разрабатывать системы защиты информации автоматизированных систем	ПК-1	ПК-1.1 Осуществляет формирование требований к защите информации автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 5 зачётных единицы, 180 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к лабораторным занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к экзамену.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		7
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	36	36
Лабораторные работы (ЛР)	-	-
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	108	108
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	12	12
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	15	15
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	18	18
Работа в библиотеке	18	18
Подготовка к экзамену	36	36
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	180	180
з.е.	5	5

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 4 темы:

– тема 1 (Основы технической защиты информации);

– тема 2 (Технические средства получения информации);

– тема 3 (Оценка угроз и методы противодействия утечке информации);

- тема 4 (Практические аспекты и современные угрозы).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Основы технической защиты информации	Введение в техническую защиту информации. Концепция технической защиты информации. Организационные основы технической защиты информации. Физические основы утечки информации.	8	–	–	Организация аттестации выделенного помещения по требованиям безопасности информации Моделирование объекта защиты.	4 4
2	Технические средства получения информации	Классификация технических средств получения информации. Акустические и виброакустические каналы утечки информации. Электромагнитные каналы утечки информации. Оптические и визуальные каналы утечки информации. Беспроводные каналы утечки информации.	10	–	–	Моделирование технических каналов утечки информации Исследование звукоизоляционных свойств различных материалов.	4 6

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Оценка угроз и методы противодействия утечке информации	Методы оценки угроз утечки информации. Методы противодействия утечке информации. Технические средства защиты информации. Аттестация объектов защиты.	10	–	–	Экспериментально-расчетная оценка разборчивости речи. Определение класса средств криптографической защиты информации. Разработка модели угроз по документам ФСБ.	4 4
4	Практические аспекты и современные угрозы	Практические аспекты защиты информации. Современные угрозы и вызовы в области защиты информации. Защита информации в критически важных объектах.	8	–	–	Многофункциональный поисковый прибор ST131.S «Пиранья II».	8
Всего аудиторных часов		36		–		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ПК-1	Экзамен	Комплект контролирующих материалов для экзамена

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– рефераты (2 шт.) – всего 20 баллов;

- практические работы – всего 80 баллов.

Оценка по экзамену проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Экзамен по дисциплине «Защита информации от утечки по техническим каналам» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку в форме устного собеседования по приведенным ниже вопросам.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

Тема 1: Основы технической защиты информации

1. Концепция технической защиты информации: основные принципы и задачи.
2. Нормативно-правовая база в области защиты информации.
3. Международные стандарты в области защиты информации (ISO/IEC 27001).
4. Российские стандарты защиты информации (ГОСТ Р 50922-2006).
5. Организационные меры технической защиты информации.
6. Роль человеческого фактора в утечке информации.
7. История развития технической защиты информации.
8. Этические аспекты защиты информации.
9. Баланс между безопасностью и приватностью в технической защите.
10. Основные угрозы информационной безопасности в современном мире.

Тема 2: Технические каналы утечки информации

11. Классификация технических каналов утечки информации.
12. Акустические каналы утечки информации: методы перехвата и защиты.
13. Виброакустические каналы утечки информации.
14. Электромагнитные каналы утечки информации (ПЭМИН).
15. Оптические каналы утечки информации.
16. Беспроводные каналы утечки информации: Wi-Fi, Bluetooth, GSM.
17. Утечка информации через кабельные линии связи.
18. Технические средства перехвата информации: классификация и принципы работы.

19. Современные методы перехвата информации через IoT-устройства.
20. Утечка информации через облачные технологии.

Тема 3: Методы и средства защиты информации

21. Методы подавления акустических сигналов.
22. Методы защиты от утечки информации через ПЭМИН.
23. Экранирование как метод защиты информации.
24. Технические средства защиты информации: обзор и применение.
25. Программные средства защиты информации.
26. Методы защиты информации в беспроводных сетях.
27. Защита информации в облачных средах.
28. Криптографические методы защиты информации.
29. Физические методы защиты информации.
30. Комплексный подход к защите информации.

Тема 4: Оценка угроз и рисков

31. Методы оценки угроз утечки информации.
32. Анализ рисков в технической защите информации.
33. Методики оценки уязвимостей информационных систем.
34. Оценка эффективности защитных мер.
35. Методы моделирования угроз утечки информации.
36. Анализ инцидентов утечки информации.
37. Оценка угроз в IoT-устройствах.
38. Оценка угроз в облачных технологиях.
39. Оценка угроз в беспроводных сетях.
40. Оценка угроз в критически важных объектах.

Тема 5: Аттестация объектов защиты

41. Процедура аттестации объектов защиты.
42. Требования к аттестации объектов в соответствии с ГОСТ Р 50922-2006.
43. Методики проведения аттестации объектов.
44. Аттестация объектов информатизации.
45. Аттестация объектов в облачных средах.
46. Аттестация объектов в IoT-системах.
47. Аттестация объектов в беспроводных сетях.
48. Аттестация объектов в промышленных системах.
49. Аттестация объектов в государственных учреждениях.
50. Аттестация объектов в финансовой сфере.

Тема 6: Современные угрозы и вызовы

51. Современные угрозы утечки информации через IoT.

52. Угрозы утечки информации в облачных технологиях.
53. Угрозы утечки информации в Big Data.
54. Угрозы утечки информации в блокчейн-технологиях.
55. Угрозы утечки информации в квантовых технологиях.
56. Угрозы утечки информации через социальную инженерию.
57. Угрозы утечки информации через мобильные устройства.
58. Угрозы утечки информации в умных домах.
59. Угрозы утечки информации в промышленных IoT-системах.
60. Угрозы утечки информации в автономных транспортных средствах.

Тема 7: Практические аспекты защиты информации

61. Разбор реальных кейсов утечки информации.
62. Практические методы защиты информации в офисах.
63. Практические методы защиты информации на промышленных объектах.
64. Практические методы защиты информации в государственных учреждениях.
65. Практические методы защиты информации в финансовой сфере.
66. Практические методы защиты информации в медицинских учреждениях.
67. Практические методы защиты информации в образовательных учреждениях.
68. Практические методы защиты информации в транспортной сфере.
69. Практические методы защиты информации в энергетической сфере.
70. Практические методы защиты информации в телекоммуникациях.

Тема 8: Международный опыт и стандарты

71. Международный опыт защиты информации от утечек.
72. Сравнение российских и международных стандартов защиты информации.
73. Опыт защиты информации в США.
74. Опыт защиты информации в Европе.
75. Опыт защиты информации в Китае.
76. Опыт защиты информации в Японии.
77. Опыт защиты информации в странах СНГ.
78. Международные организации в области защиты информации.
79. Международные конференции по защите информации.
80. Международные исследования в области защиты информации.

Тема 9: Инновационные технологии защиты информации

81. Использование искусственного интеллекта для защиты информации.
82. Использование блокчейна для защиты информации.
83. Использование квантовых технологий для защиты информации.
84. Использование Big Data для защиты информации.
85. Использование IoT для защиты информации.
86. Использование облачных технологий для защиты информации.
87. Использование биометрических данных для защиты информации.
88. Использование нейронных сетей для защиты информации.
89. Использование машинного обучения для защиты информации.
90. Использование виртуальной реальности для защиты информации.

Тема 10: Будущее технической защиты информации

91. Будущее технической защиты информации: тренды и прогнозы.
92. Будущее защиты информации в IoT.
93. Будущее защиты информации в облачных технологиях.
94. Будущее защиты информации в Big Data.
95. Будущее защиты информации в блокчейн-технологиях.
96. Будущее защиты информации в квантовых технологиях.
97. Будущее защиты информации в искусственном интеллекте.
98. Будущее защиты информации в умных городах.
99. Будущее защиты информации в автономных системах.
100. Будущее защиты информации в глобальных сетях.

Дополнительные темы рефератов

1. Утечки информации
2. Случаи утечки информации
3. Технические каналы утечки информации
4. Технические каналы утечки информации ГОСТ
5. Выявление каналов утечки информации
6. Утечка информации по каналам ПЭМИН
7. Классификация каналов утечки информации
8. Последствия утечки информации
9. Случаи утечки информации в медицине
10. Ущерб от утечки информации
11. Виброакустический канал утечки информации
12. Каналы утечки информации на предприятии
13. Каналы утечки информации в компьютерных системах
14. Каналы утечки информации за счет паразитных связей
15. Каналы утечки персональных данных

16. Радиоканалы утечки информации
17. Способы блокирования каналов утечки информации
18. Акустический канал утечки информации
19. Материально-вещественные каналы утечки информации
20. Оптические каналы утечки информации
21. Параметрические каналы утечки информации
22. Скрытые логические каналы утечки информации
23. Электромагнитные каналы утечки информации
24. Анализ технических каналов утечки информации
25. Виды технических каналов утечки информации
26. Мероприятия по выявлению технических каналов утечки информации
27. Предотвращение утечки информации по техническим каналам
28. Способы и средства защиты информации от утечки по техническим каналам
29. Угрозы реализации технических каналов утечки информации
30. Аналитическая работа по выявлению каналов утечки информации фирмы
31. Средства выявления каналов утечки информации
32. Разработка мероприятий по защите информации от утечки по каналам ПЭМИН
33. Угрозы утечки информации по каналам ПЭМИН
34. Причины утечки информации
35. Источники утечки информации
36. Утечка данных
37. Утечка данных кредитных карт
38. Утечка информации в облачные хранилища
39. Утечка информации через мобильные телефоны
40. Утечка конфиденциальной информации
41. Печать и утечка информации
42. Современные технологии защиты от утечки конфиденциальной информации
43. Утечка банковской информации
44. Утечка информации из компании
45. Утечка информации конкуренту
46. Утечка личной информации в сеть Интернет
47. Утечки персональных данных
48. Как защитить персональные данные от утечки
49. Как узнать, кто в компании сливает информацию конкурентам

50. Утечка коммерческой информации
51. Причины утечки информации на предприятии
52. Основные каналы утечки информации
53. Причины и условия утечки защищаемой информации
54. Способы предотвращения утечки информации
55. Расследование утечки информации
56. Как избежать утечки информации
57. Противодействие утечкам информации
58. Виды угроз утечки информации
59. Разработка системы защиты от электромагнитных каналов утечки информации.
60. Разработка системы защиты акустических каналов утечки информации.
61. Сравнительный анализ характеристик средств обнаружения радиозакладок.
62. Оптические каналы утечки информации и их локализация.
63. Реализация защиты информации от утечки через ПЭМИН.
64. Сравнительный анализ моделей безопасности компьютерных систем.
65. Сравнительный анализ методов защиты персональных данных.
66. Сравнительный анализ уязвимостей сайтов от возможных атак.
67. Сравнительный анализ методов аутентификации пользователей информационных систем.
68. Сравнительный анализ методов, используемых в типовых системах контроля и управления доступом (СКУД) предприятий.
69. Сравнительный анализ методов доступа в информационных системах.
70. Сравнительный анализ возможностей программно-аппаратных комплексов защиты информации от НСД.
71. Сравнительный анализ методов стеганографии для скрытия информации.
72. Сравнительный анализ методов защиты информации в базах данных.
73. Сравнительный анализ методов физической защиты объектов информатизации.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

*Тема 1 (*Основы технической защиты информации*)*

Базовые тесты (выбор одного правильного ответа)

1. Что понимается под техническим каналом утечки информации в соответствии с ГОСТ Р 50922-2006?

a) Способ передачи данных через интернет

b) Физический или технический способ несанкционированного получения информации.

c) Метод шифрования данных.

d) Программное обеспечение для защиты информации.

Ответ: b)

2. Какой из перечисленных принципов технической защиты информации соответствует требованиям ФСТЭК России?

a) Принцип открытости.

b) Принцип комплексности.

c) Принцип минимальной защиты.

d) Принцип случайности.

Ответ: b)

3. Что относится к организационным мерам защиты информации в соответствии с ГОСТ Р 57580-2017?

a) Установка антивируса.

b) Разработка политики безопасности.

c) Использование генератора шума.

d) Экранирование помещений.

Ответ: b)

4. Какой документ регулирует защиту персональных данных в РФ?

a) Уголовный кодекс РФ.

b) Федеральный закон № 152-ФЗ "О персональных данных".

c) Конституция РФ.

d) Гражданский кодекс РФ.

Ответ: b)

5. Что является целью аттестации объекта защиты в соответствии с требованиями ФСТЭК России?

a) Проверка соответствия объекта требованиям по защите информации.

b) Установка антивирусного программного обеспечения.

c) Проведение аудита финансовой отчетности.

d) Оценка производительности оборудования.

Ответ: а)

Тесты повышенного уровня (вставьте пропущенный термин)

6. Основной целью технической защиты информации является предотвращение _____ информации в соответствии с ГОСТ Р 50922-2006.

Ответ: утечки

7. Принцип _____ предполагает использование всех доступных методов и средств защиты в соответствии с требованиями ФСТЭК России.

Ответ: комплексности

8. Организационные меры защиты информации включают разработку _____ безопасности в соответствии с ГОСТ Р 57580-2017.

Ответ: политики

9. Федеральный закон № 152-ФЗ регулирует _____ персональных данных.

Ответ: защиту

10. Аттестация объекта защиты включает проверку соответствия _____ требованиям по защите информации.

Ответ: объекта

Тесты высокого уровня (напишите формулу или определение)

11. Дайте определение понятию "технический канал утечки информации" в соответствии с ГОСТ Р 50922-2006.

Ответ: Технический канал утечки информации — это физический или технический способ несанкционированного получения информации, связанный с использованием технических средств.

12. Напишите формулу для расчета уровня защищенности информации в соответствии с методиками ФСТЭК России.

Ответ: Уровень защищенности (УЗ) = (Количество выявленных угроз) / (Общее количество угроз) * 100%.

13. Дайте определение понятию "аттестация объекта защиты" в соответствии с требованиями ФСТЭК России.

Ответ: Аттестация объекта защиты — это процесс проверки соответствия объекта требованиям по защите информации, установленным нормативными документами.

*Тема 2 (*Технические средства получения информации*)*

Базовые тесты

1. Какое устройство используется для съема акустической информации в соответствии с ГОСТ Р 50922-2006?

a) Лазерный микрофон.

b) Генератор шума.

c) Экранирующая сетка.

d) Антивирус.

Ответ: a)

2. Что такое ПЭМИН в соответствии с ГОСТ Р 50922-2006?

a) Программное обеспечение для защиты информации.

b) Побочные электромагнитные излучения и наводки.

c) Метод шифрования данных.

d) Устройство для подавления сигналов.

Ответ: b)

3. Какой канал утечки информации связан с вибрациями в соответствии с ГОСТ Р 50922-2006?

a) Акустический.

b) Виброакустический.

c) Электромагнитный.

d) Оптический.

Ответ: b)

4. Какое устройство используется для подавления акустических сигналов в соответствии с требованиями ФСТЭК России?

a) Лазерный микрофон.

b) Генератор шума.

c) Экранирующая сетка.

d) Антивирус.

Ответ: b)

5. Какие из перечисленных параметров проверяются при аттестации объекта защиты?

a) Уровень защищенности от ПЭМИН.

b) Наличие антивирусного программного обеспечения.

c) Производительность серверного оборудования.

d) Качество интернет-соединения.

Ответ: a)

Тесты повышенного уровня

6. Лазерный микрофон используется для съема _____ информации в соответствии с ГОСТ Р 50922-2006.

Ответ: акустической

7. ПЭМИН расшифровывается как _____ в соответствии с ГОСТ Р 50922-2006.

Ответ: побочные электромагнитные излучения и наводки

8. Виброакустические каналы утечки связаны с _____ в соответствии с ГОСТ Р 50922-2006.

Ответ: вибрациями

9. Генератор шума используется для _____ акустических сигналов в соответствии с требованиями ФСТЭК России.

Ответ: подавления

10. При аттестации объекта защиты проверяется уровень защищенности от _____.

Ответ: ПЭМИН

Тесты высокого уровня

11. Дайте определение понятию "ПЭМИН" в соответствии с ГОСТ Р 50922-2006.

Ответ: ПЭМИН — это побочные электромагнитные излучения и наводки, возникающие при работе технических средств и используемые для несанкционированного получения информации.

12. Напишите формулу для расчета уровня сигнала при подавлении в соответствии с методиками ФСТЭК России.

Ответ: Уровень сигнала (УС) = Исходный уровень сигнала (ИУС) - Уровень подавления (УП).

13. Напишите формулу для расчета уровня защищенности объекта от ПЭМИН в соответствии с методиками ФСТЭК России.

Ответ: Уровень защищенности (УЗ) = (Количество выявленных угроз ПЭМИН) / (Общее количество угроз ПЭМИН) * 100%.

*Тема 3 (*Оценка угроз и методы противодействия утечке информации*)*

Базовые тесты

1. Что является основным методом подавления опасных сигналов в соответствии с требованиями ФСТЭК России?

a) Шифрование данных.

b) Использование генератора шума.

c) Установка антивируса.

d) Экранирование помещений.

Ответ: b)

2. Какой метод защиты используется для предотвращения утечек через сети электропитания в соответствии с ГОСТ Р 50922-2006?

a) Экранирование.

b) Шифрование.

c) Использование фильтров.

d) Установка антивируса.

Ответ: c)

3. Что такое экранирование в соответствии с ГОСТ Р 50922-2006?

a) Метод подавления сигналов.

b) Метод защиты информации путем создания барьера для электромагнитных излучений.

c) Метод шифрования данных.

d) Метод анализа угроз.

Ответ: b)

4. Какой метод используется для оценки угроз утечки информации в соответствии с ГОСТ Р 57580-2017?

a) Анализ рисков.

b) Шифрование данных.

c) Использование генератора шума.

d) Экранирование помещений.

Ответ: a)

5. Какой документ оформляется по результатам аттестации объекта защиты?

a) Акт проверки.

b) Заключение о соответствии.

c) Финансовый отчет.

d) Техническое задание.

Ответ: b)

Тесты повышенного уровня

6. Генератор шума используется для _____ опасных сигналов в соответствии с требованиями ФСТЭК России.

Ответ: подавления

7. Фильтры используются для защиты от утечек через _____ в

соответствии с ГОСТ Р 50922-2006.

Ответ: сети электропитания

8. Экранирование создает барьер для _____ излучений в соответствии с ГОСТ Р 50922-2006.

Ответ: электромагнитных

9. Анализ _____ используется для оценки угроз утечки информации в соответствии с ГОСТ Р 57580-2017.

Ответ: рисков

10. По результатам аттестации объекта защиты оформляется _____ о соответствии.

Ответ: заключение

Тесты высокого уровня

11. Дайте определение понятию "экранирование" в соответствии с ГОСТ Р 50922-2006.

Ответ: Экранирование — это метод защиты информации путем создания физического барьера, препятствующего распространению электромагнитных излучений.

12. Напишите формулу для расчета эффективности экранирования в соответствии с методиками ФСТЭК России.

Ответ: Эффективность экранирования (ЭЭ) = Уровень сигнала до экранирования (УС1) - Уровень сигнала после экранирования (УС2).

13. Дайте определение понятию "заключение о соответствии" в соответствии с требованиями ФСТЭК России.

Ответ: Заключение о соответствии — это документ, подтверждающий, что объект защиты соответствует установленным требованиям по защите информации.

*Тема 4 (*Практические аспекты и современные угрозы*)*

Базовые тесты

1. Что относится к современным угрозам утечки информации в соответствии с требованиями ФСТЭК России?

a) Атаки с использованием искусственного интеллекта.

b) Утечки через IoT-устройства.

c) Оба варианта верны.

d) Ни один из вариантов не верен.

Ответ: c)

2. Какой метод защиты используется для предотвращения утечек

через IoT-устройства в соответствии с ГОСТ Р 57580-2017?

a) Шифрование данных.

b) Использование генератора шума.

c) Экранирование помещений.

d) Установка антивируса.

Ответ: a)

3. Что такое квантовые вычисления в соответствии с современными стандартами?

a) Метод шифрования данных.

b) Технология, использующая квантовые биты для обработки информации.

c) Метод подавления сигналов.

d) Метод анализа угроз.

Ответ: b)

4. Какой метод используется для защиты от атак с использованием искусственного интеллекта в соответствии с требованиями ФСТЭК России?

a) Использование антивируса.

b) Применение алгоритмов машинного обучения для обнаружения аномалий.

c) Экранирование помещений.

d) Использование генератора шума.

Ответ: b)

5. Какие современные угрозы учитываются при аттестации объектов защиты?

a) Утечки через IoT-устройства.

b) Атаки с использованием искусственного интеллекта.

c) Оба варианта верны.

d) Ни один из вариантов не верен.

Ответ: c)

Тесты повышенного уровня

6. Современные угрозы включают атаки с использованием _____ в соответствии с требованиями ФСТЭК России.

Ответ: искусственного интеллекта

7. Защита от утечек через IoT-устройства включает _____ данных в соответствии с ГОСТ Р 57580-2017.

Ответ: шифрование

8. Квантовые вычисления используют _____ для обработки информации в соответствии с современными стандартами.
Ответ: квантовые биты

9. Для защиты от атак с использованием искусственного интеллекта применяются алгоритмы _____ в соответствии с требованиями ФСТЭК России.
Ответ: машинного обучения

10. При аттестации объектов защиты учитываются современные угрозы, такие как утечки через _____.
Ответ: IoT-устройства

Тесты высокого уровня

11. Дайте определение понятию "квантовые вычисления" в соответствии с современными стандартами.
Ответ: Квантовые вычисления — это технология, использующая квантовые биты (кубиты) для обработки информации, что позволяет решать задачи, недоступные для классических компьютеров.

12. Напишите формулу для расчета эффективности алгоритма машинного обучения в соответствии с методиками ФСТЭК России.
Ответ: Эффективность (Э) = (Количество правильно классифицированных данных) / (Общее количество данных) * 100%.

13. Напишите формулу для расчета уровня защищенности объекта от современных угроз в соответствии с методиками ФСТЭК России.

Ответ: Уровень защищенности (УЗ) = (Количество выявленных современных угроз) / (Общее количество современных угроз) * 100%.

6.5 Вопросы для подготовки к экзамену

1) Опишите объекты защиты информации?
2) Что такое случайные антенны?
3) Технические каналы утечки информации. Дайте общую характеристику?
4) Что такое каналы утечки речевой информации?
5) Что такое каналы утечки видовой информации?
6) Что такое каналы утечки информации при передаче ее по каналам связи?
7) Что такое электромагнитное поле побочных электромагнитных излучений?
8) Что такое электромагнитные волны и их свойства?

9) Что такое ближняя зона излучения электромагнитного поля? Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля в ближней зоне?

10) Что такое элементарные дипольные излучатели?

11) В каких границах располагается дальняя зона электромагнитного поля?

12) Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля в дальней зоне?

13) Что такое электромагнитные каналы утечки информации ТСПИ?

14) Что такое звуковое поле? Приведите характеристики.

15) Что такое звуковое давление и звуковая мощность. Сила звука?

16) Что такое демаскирующие признаки объекта?

17) Какие демаскирующие признаки характеризуют радиоэлектронные средства?

18) Что такое пространственно-энергетические характеристики радиоэлектронных средств?

19) Что такое спектральные характеристики радиоизлучений?

20) Что такое спектральные характеристики акустических сигналов?

21) Какие Вы знаете основные задачи, решаемые пассивными средствами защиты?

22) Какие Вы знаете основные задачи, решаемые активными средствами защиты?

23) Каков состав системы обеспечения безопасности объектов?

24) В чем заключается сущность электромагнитного экранирования? Как оценивается эффективность экранирования?

25) Что представляют собой экранированные камеры? Их назначение.

26) С какой целью применяется фильтрация сигналов?

27) Что такое методы пассивной и активной маскировки объектов?

28) Что понимают под аттестационной проверкой?

29) В чем цель и сущность технического контроля эффективности защиты информации?

30) Что такое методы контроля эффективности защиты информации?

31) Каков состав нормативной и методической документации на методы испытаний?

32) Какие Вы знаете задачи эксплуатационного контроля защищенности от утечки по ПЭМИН?

33) Каковы причины и последствия модуляции информационным речевым сигналом высокочастотных колебаний у генераторов технических

средств?

34) Какие документы являются нормативно-техническими при проведении аттестации объектов?

35) Какие объекты подлежат обязательной аттестации?

36) Что представляют собой специальные проверки объекта защиты?

37) Какие узлы и устройства ПЭВМ представляют наибольшую опасность утечки информации через ПЭМИН?

38) Что такое утечка информации по оптоволоконным каналам связи?

39) Какие Вы знаете криптографические и случайные методы защиты информации?

40) Что такое квантовая криптография?

41) Каковы состав и назначение прибора «СИГУРД»?

42) Каковы состав и назначение прибора «ПИРАНЬЯ»?

43) Каковы состав и назначение комплекса «КАССАНДРА»?

44) Каковы состав и назначение комплекса «СМАРТ»?

45) Какие Вы знаете случайные электромагнитные антенны, обнаруженные при проведении лабораторных измерений в помещении?

46) Как практически обеспечить экранирование мобильного устройства связи по электромагнитному каналу?

47) Как практически обеспечить экранирование мобильного устройства связи по акустическому каналу?

48) Какие Вы знаете каналы утечки по электромагнитному каналу, обнаруженные при проведении лабораторных измерений в помещении?

49) Какие Вы знаете каналы утечки по акустическому каналу, обнаруженные при проведении лабораторных измерений в помещении?

50) Как обнаружить появление нового электромагнитного сигнала с помощью комплекса «КАССАНДРА»?

51) Как обнаружить наличие источников электромагнитного излучения и их тип с помощью прибора «ПИРАНЬЯ»?

52) Как осуществить и проверить защиту от утечки информации по акустическому каналу помощью прибора ГШ-1?

53) Для чего и как используется виброакустический датчик в приборе «ПИРАНЬЯ»?

54) В какой зоне излучения (ближней, дальней) легче обнаружить источник и почему?

55) Почему при измерениях прибором «ПИРАНЬЯ» электромагнитного излучения интенсивность сигнала зависит от ориентации антенны? Как это влияет на процедуру измерений?

56) Что такое техническая защита информации?

57) Какие Вы знаете основные принципы технической защиты информации?

58) Какие Вы знаете основные нормативно-правовые документы в области защиты информации?

59) Что такое виброакустические каналы утечки информации?

60) Опишите электромагнитные каналы утечки информации.

61) Что такое экранирование и как оно применяется для защиты информации?

62) Опишите основные методы подавления электромагнитных излучений.

63) Какие технические средства используются для перехвата информации?

64) Что такое аттестация объектов защиты? Опишите ее основные этапы.

65) Какие стандарты регулируют защиту информации в России и за рубежом?

66) Опишите основные угрозы утечки информации через беспроводные сети.

67) Что такое социальная инженерия и как она связана с утечкой информации?

68) Опишите основные методы защиты информации в облачных технологиях.

69) Какие угрозы связаны с IoT-устройствами?

70) Что такое Big Data и какие угрозы утечки информации с ним связаны?

71) Опишите основные методы защиты информации в блокчейн-технологиях.

72) Какие методы используются для оценки угроз утечки информации?

73) Что такое анализ рисков и как он применяется в защите информации?

74) Опишите основные этапы проведения аттестации объектов защиты.

75) Какие методы используются для защиты информации в промышленных системах?

76) Объясните, почему акустические каналы утечки информации считаются одними из самых опасных.

77) Почему электромагнитные каналы утечки информации трудно обнаружить?

78) Как виброакустические каналы утечки информации могут быть использованы для перехвата данных?

79) Почему беспроводные сети (Wi-Fi, Bluetooth) уязвимы для утечки информации?

80) Почему облачные технологии считаются уязвимыми для утечки информации?

81) Объясните, как методы подавления сигналов помогают защитить информацию.

82) Объясните, почему защита информации в медицинских учреждениях требует особого внимания.

83) Почему защита информации в финансовой сфере считается критически важной?

84) Как методы машинного обучения могут быть использованы для защиты информации?

85) Как методы виртуальной реальности могут быть использованы для защиты информации?

6.6 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Бузов Г. А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2024. – 586 с., ил. – Режим доступа: https://z-library.sk/book/5559015/0ec70d/Защита-информации-ограниченного-доступа-от-утечки-по-техническим-каналам.html. (Дата обращения 26.08.2023).

2. Бурлаков, Михаил Евгеньевич Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум: учебное пособие / М.Е. Бурлаков, М.Н. Осипов. – Самара: Издательство Самарского университета, 2021. – 96 с.: ил. - Режим доступа: https://repo.ssau.ru/bitstream/Uchebnye-izdaniya/Akusticheskie-i-vibroakustic heskie-kanaly-utechki-informacii-Teoreticheskie-osnovy-i-bazovyi-praktikum-92539/1/Бурлаков%20М.Е.%20Акустические%20и%20виброакустические%20каналы%202021.pdf. (Дата обращения 26.08.2023).

3. Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с. – Режим доступа: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf. (дата обращения: 26.08.2023).

4. Тельный, А. В. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ : Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и характеристики : учеб. пособие / А. В. Тельный, Ю. М. Монахов ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2018. – 161 с. – Режим доступа: https://dspace.www1.vlsu.ru/bitstream/123456789/7165/1/00792.pdf. (Дата обращения 26.08.2023).

Дополнительная литература

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с. // Режим доступа: https://books.ifmo.ru/file/pdf/975.pdf. (Дата обращения: 26.08.2023).

2. Голиков А.М. Защита информации от утечки по техническим каналам: учебное пособие. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники,, 2015. – 256 с. - Режим доступа: https://edu.study.tusur.ru/publications/5263/download. (Дата обращения 26.08.2023).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education. — Текст : электронный.

2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/. — Текст : электронный.

3. Консультант студента : электронно-библиотечная система.— Москва. — URL: http://www.studentlibrary.ru/cgi-bin/mb4x. — Текст : электронный.

4. Университетская библиотека онлайн: электронно-библиотечная система. – URL: http://biblioclub.ru/index.php?page=main_ub_red. – Текст : электронный.

5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: http://www.iprbookshop.ru/. — Текст : электронный.

6. Сайт кафедры ИСИБ http://scs.dstu.education.

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 6.

Таблица 6 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: Аудитории для проведения лекции: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (парта трехместная – 18 шт., парта двухместная – 6 шт, стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран.	ауд. *207* корп. *4*
Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:	ауд. *217* корп. *3* ауд. *211* корп. *4*

Лист согласования РПД

Разработал:
ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)

(подпись) А.С. Закутный
(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Протокол №__1__ заседания кафедры от __27.08. 2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)

(подпись) В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03
Информационная безопасность
автоматизированных систем

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Начальник учебно-методического центра

(подпись) О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

<table>
<tr><td colspan="2">Номер изменения, дата внесения изменения, номер страницы для внесения изменений</td></tr>
<tr><td>ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td><td>ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>