

Документ подписан простой электронной подписью
Информация о подписи:
ФИО: Вишневский Дмитрий Александрович
Должность: Ректор
Дата подписания: 30.04.2025 11:55:50
Уникальный программный ключ:
03474917c4d012283e5ad996a48a5e70bf6da057

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

Физические основы построения технических средств защиты информации
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование направления)

Безопасность открытых информационных систем
(специализация)

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

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

1 Цель и задачи учебной дисциплины

Цели дисциплины. Целью изучения дисциплины «Физические основы построения технических средств защиты информации» является формирование у будущего специалиста профессиональных навыков для разработки и эксплуатации технических средств защиты информации.

Задачи изучения дисциплины:

- приобретение студентами знаний, умений и навыков в области разработки и эксплуатации технических средств защиты информации;
- выбор рациональных архитектурных решений при синтезе систем и их подсистем;
- применение программно-аппаратных средств для разработки и эксплуатации технических средств защиты информации.

Дисциплина направлена на формирование:

- профессиональных компетенций (ОПК-4);

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в формируемую участниками образовательных отношений часть блока 1 подготовки обучающихся по направлению 10.05.03 Информационная безопасность автоматизированных систем.

Дисциплина реализуется кафедрой специализированных компьютерных систем. Основывается на базе дисциплин «Высшая математика», «Методы математической физики», «Оптика», «Математическое моделирование», «Информатика», «Алгоритмы и методы вычислений», «Микропроцессорные системы».

Является основой для изучения следующих дисциплин: «Физические основы защиты информации», «Безопасность систем баз данных», «Безопасность операционных систем», «Безопасность сетей ЭВМ», а также, приобретенные знания, могут быть использованы при подготовке и защите выпускной квалификационной работы, при прохождении преддипломной практики, а также в профессиональной деятельности. Дисциплина способствует углубленной подготовке к решению специальных практических профессиональных задач и формированию необходимых компетенций.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 ак. ч. Программой дисциплины предусмотрены лекционные (18 ак. ч.) лабораторные (36 ч.) занятия и самостоятельная работа студента (54 ч.). Дисциплина изучается на 2 курсе в 4 семестре.

Форма промежуточной аттестации – экзамен.

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

Процесс изучения дисциплины «Физические основы построения технических средств защиты информации» 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 анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4	ОПК-4.2. Применяет основные физические законы и модели для решения задач профессиональной деятельности

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144ак. ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим 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
		4
Аудиторная работа, в том числе:	54	54
Лекции (Л)	18	18
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	54	54
Подготовка к лекциям	4	4
Подготовка к лабораторным работам	18	18
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	12	12
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	-	-
Работа в библиотеке	4	4
Подготовка к экзамену	16	16
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоёмкость дисциплины		
	ак. ч.	108
	з.е.	3

5 Содержание дисциплины

С целью освоения компетенции, приведенной в п.3 дисциплина разбита на 9 тем:

- тема 1 (Цели, задачи и организация разведки техническими средствами. Концепция инженерно-технической защиты информации);
- тема 2 (Физические основы технической защиты информации. Физические поля как носители информации);
- тема 3 (Основные принципы технической защиты информации. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов);
- тема 4 (Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок. Системы защиты от утечки информации по акустическому каналу);
- тема 5 (Системы защиты от утечки информации по вибрационному каналу. Системы защиты от утечки информации по электромагнитному каналу);
- тема 6 (Системы защиты от утечки информации по оптическому каналу. Физические принципы формирования каналов утечки информации в волоконно-оптических линиях связи);
- тема 7 (Получение информации в компьютерных сетях. Методы и средства инженерной защиты и технической охраны объектов);
- тема 8 (Технический контроль эффективности мер защиты информации);
- тема 9 (Криптографические методы и средства защиты информации).

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

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудо-емкость в ак. ч.	Темы практических занятий	Трудо-емкость в ак. ч.	Тема лабораторных занятий	Трудо-емкость в ак. ч.
1	2	3	4	5	6	7	8
1	Цели, задачи и организация разведки техническими средствами. Концепция инженерно-технической защиты информации.	<ul style="list-style-type: none"> – Происхождение разведки техническими средствами (РТС). Понятие разведки техническими средствами. Организация технической разведки. Классификация разведки техническими средствами. Физические основы получения разведывательной информации с помощью РТС. – Предмет и задачи технической защиты информации. – Общие положения защиты информации техническими средствами. 	2	-	-	Физические основы получения разведывательной информации с помощью РТС.	4

Продолжение таблицы3

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудо-емкость в ак. ч.	Темы практических занятий	Трудо-емкость в ак. ч.	Тема лабораторных занятий	Трудо-емкость в ак. ч.
1	2	3	4	5	6	7	8
2	Физические основы технической защиты информации. Физические поля как носители информации.	<p>–Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.</p> <p>– Физические процессы при подавлении опасных сигналов.</p> <p>– Многообразие физических полей. Электромагнитные поля. Акустические поля. Звуковые поля. Сейсмические поля. Электромагнитные волны и их характеристики. Свойства электромагнитных волн.</p> <p>– Электрические сигналы и их модуляция. Антенны и их технические характеристики. Неравномерность АЧХ антенн. Диаграмма направленности (ДН) антенн. Классификация антенн и назначение различных типов антенн.</p>	2	-	-	Регистрация электромагнитных сигналов различных частот в атмосфере.	4

Продолжение таблицы 3

№ 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
3	<p>Основные принципы технической защиты информации.</p> <p>Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов.</p>	<p>– Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Методы инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей.</p> <p>– Распространение сигналов в технических каналах утечки информации. Распространение радиосигналов различных диапазонов в пространстве и направляющим линиям связи. Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.</p>	2	-	-	Регистрация электромагнитных сигналов в различных средах.	4

Продолжение таблицы 3

№ 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
4	Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок. Системы защиты от утечки информации по акустическому каналу.	<p>– Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.</p> <p>– Звуковые волны. Плоская волна. Характеристики звуковых волн. Связь между звуковым давлением и колебательной скоростью. Удельное акустическое сопротивление среды. Энергетические характеристики звукового поля. Плотность звуковой энергии. Особенности распространения звуковых волн. Технические средства акустической разведки.</p>	2	-	-	Регистрация речевой информации средства акустической разведки.	4

Продолжение таблицы3

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудо-емкость в ак. ч.	Темы практических занятий	Трудо-емкость в ак. ч.	Тема лабораторных занятий	Трудо-емкость в ак. ч.
1	2	3	4	5	6	7	8
5	Системы защиты от утечки информации по вибрационному каналу. Системы защиты от утечки информации по электромагнитному каналу.	<p>– Звукопоглощающие материалы и конструкции. Акустоэлектрические преобразователи информации. Электронные стетоскопы. Гидроакустические преобразователи.</p> <p>– Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.</p> <p>– Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Перехват сообщений в каналах сотовой связи. Архитектура GSM сети.</p>	2	-	-	Перехват сообщений в каналах сотовой связи.	4

Продолжение таблицы 3

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудо-емкость в ак. ч.	Темы практических занятий	Трудо-емкость в ак. ч.	Тема лабораторных занятий	Трудо-емкость в ак. ч.
1	2	3	4	5	6	7	8
6	Системы защиты от утечки информации по оптическому каналу. Физические принципы формирования каналов утечки информации в волоконно-оптических линиях связи.	<p>– Волновые и квантовые свойства света. Волновая оптика. Интерференция. Оптико-механические приборы. Приборы ночного видения.</p> <p>– Средства для проведения скрытой фотосъемки Оптические квантовые генераторы — лазеры. Типы и принципы работы лазеров. Лазерные системы подслушивания.</p> <p>– Оптоэлектроника. Оптическая связь. Волоконная оптика. Физические основы утечки информации ВОЛС. Нарушение полного внутреннего отражения. Регистрация рассеянного излучения. Параметрические методы регистрации проходящего излучения.</p>	2	-	-	Передача информации лазерными системами	4

Продолжение таблицы3

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудо-емкость в ак. ч.	Темы практических занятий	Трудо-емкость в ак. ч.	Тема лабораторных занятий	Трудо-емкость в ак. ч.
1	2	3	4	5	6	7	8
7	Получение информации в компьютерных сетях. Методы и средства инженерной защиты и технической охраны объектов.	<ul style="list-style-type: none"> – Основные способы несанкционированного доступа. Несанкционированный доступ к информации на физическом носителе. Перехват информации в каналах связи. – Категории объектов защиты. Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов. – Система охранно-тревожной сигнализации. Система контроля и управления доступом. Телевизионные системы. Система пожарной сигнализации. Периметровая охрана. 	2	-	-	Исследование методов защиты от несанкционированного доступ к информации на физическом носителе.	4

Завершение таблицы3

№ 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
8	Технический контроль эффективности мер защиты информации.	–Цели и задачи технического контроля эффективности мер защиты информации. – Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ.	2	-	-	Проведение контроля защищенности выделенных помещений от утечки акустической речевой информации.	4
9	Тема 9. Криптографические методы и средства защиты информации.	– Аналоговое преобразование. Цифровое шифрование. Технические средства.	2	-	-	Проведение контроля защищенности выделенных помещений от утечки акустической речевой информации.	4
Всего аудиторных часов за 5-й семестр			18	-		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 работ по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4– Перечень работ по дисциплине и способы оценивания знаний

Вид учебной работы	Способ оценивания	Количество баллов
Выполнение лабораторных работ	Предоставление отчетов	50 - 80
Выполнение реферата	Предоставление реферата	10-20
Итого	-	60-100

Всего по текущей работе в семестре студент может набрать 100 баллов.

Экзамен 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 «Физические основы построения технических средств защиты информации» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время зачетной сессии студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п. п. б.4), либо в результате тестирования.

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 Темы для рефератов.

- 1) Методы инженерно-технической защиты информации.
- 2) Классификация методов инженерно-технической защиты информации.
- 3) Методы инженерной защиты и технической охраны объектов.
- 4) Методы скрытия информации и ее носителей.
- 5) Распространение сигналов в технических каналах утечки информации.
- 6) Распространение радиосигналов различных диапазонов в пространстве и направляющим линиям связи.
- 7) Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.
- 8) Искусственные нейронные сети.
- 9) Многообразие физических полей. Электромагнитные поля. Акустические поля. Звуковые поля. Сейсмические поля. Электромагнитные волны и их характеристики. Свойства электромагнитных волн.
- 10) Электрические сигналы и их модуляция.
- 11) Антенны и их технические характеристики. Неравномерность АЧХ антенн. Диаграмма направленности (ДН) антенн. Классификация антенн и назначение различных типов антенн.
- 12) Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Методы инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей.
- 13) Распространение сигналов в технических каналах утечки информации. Распространение радиосигналов различных диапазонов в пространстве и направляющим линиям связи. Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.

14) Звуковые волны. Плоская волна. Характеристики звуковых волн. Связь между звуковым давлением и колебательной скоростью. Удельное акустическое сопротивление среды. Энергетические характеристики звукового поля. Плотность звуковой энергии. Особенности распространения звуковых волн. Технические средства акустической разведки.

15) Звукопоглощающие материалы и конструкции. Акустоэлектрические преобразователи информации. Электронные стетоскопы. Гидроакустические преобразователи.

16) Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.

17) Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Перехват сообщений в каналах сотовой связи. Архитектура GSM сети.

18) Волновые и квантовые свойства света. Волновая оптика. Интерференция. Оптико-механические приборы. Приборы ночного видения.

19) Средства для проведения скрытой фотосъемки. Оптические квантовые генераторы — лазеры. Типы и принципы работы лазеров. Лазерные системы подслушивания.

20) Оптоэлектроника. Оптическая связь. Волоконная оптика. Физические основы утечки информации ВОЛС. Нарушение полного внутреннего отражения. Регистрация рассеянного излучения. Параметрические методы регистрации проходящего излучения.

21) Основные способы несанкционированного доступа. Несанкционированный доступ к информации на физическом носителе. Перехват информации в каналах связи.

22) Категории объектов защиты. Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов.

23) Система охранно-тревожной сигнализации. Система контроля и управления доступом. Телевизионные системы. Система пожарной сигнализации. Периметровая охрана.

24) Цели и задачи технического контроля эффективности мер защиты информации.

25) Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ.

26) Аналоговое преобразование. Цифровое шифрование. Технические средства.

6.3 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 Цели, задачи и организация разведки техническими средствами. Концепция инженерно-технической защиты информации

- 1) Что такое непосредственные и косвенные каналы утечки информации?
- 2) Что такое искусственные и естественные угрозы информационной безопасности?
- 3) Какие существуют виды воздействий на защищаемую информацию, цели защиты и основные характеристики защищаемой информации.
- 4) Какие существуют основные способы защиты от несанкционированного доступа и возможной утечки информации?
- 5) Что такое естественный канал утечки информации?

Тема 2 Физические основы технической защиты информации. Физические поля как носители информации

- 1) Какие существуют задачи инженерно-технических методов и средств защиты информации?
- 2) Что такое упругие волны?
- 3) Что такое звуковые волны?
- 4) Что такое речевой сигнал, его физические и информационные характеристики и параметры?
- 5) Что такое радиоволны?

Тема 3 Основные принципы технической защиты информации. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов

- 1) Какие существуют принципы экранирования статических и динамических полей?
- 2) Какие существуют принципы и реализация электромагнитного экранирования приборов и помещений, его эффективность?
- 3) Какие существуют требования к экранам и их характеристики?
- 4) Какие существуют методы и средства защиты от утечки информации по каналам ПЭМИН?
- 5) Какие существуют основные и вспомогательные аппаратные средства защиты информации?

Тема 4 Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок. Системы защиты от утечки информации по акустическому каналу

- 1) В чем заключается физическая сущность возникновения побочных электромагнитных излучений и наводок?

2) Какие потенциально возможные технические каналы утечки информации по каналам побочных электромагнитных излучений и наводок?

3) Какие технические каналы утечки речевой информации.

4) В чем заключается система защиты от утечки информации по акустическому каналу?

5) В чем заключается специфика акустики помещений?

Тема 5 Системы защиты от утечки информации по вибрационному каналу. Системы защиты от утечки информации по электромагнитному каналу

1) Что такое шумомер?

2) Какие меры принимают организации для защиты от утечки информации по вибрационному каналу.

3) Какие существуют электромагнитные каналы утечки информации.

4) Какие меры принимают организации для защиты от утечки информации по вибрационному каналу.

5) В чем заключаются конструкторско-технологические мероприятия по локализации возможности образования условий возникновения каналов утечки информации

Тема 6 Системы защиты от утечки информации по оптическому каналу. Физические принципы формирования каналов утечки информации в волоконно-оптических линиях связи

1) Как работает оптическая линия связи?

2) Как работают спектральные анализаторы?

3) Что такое пропускная способность канала связи?

4) Какие физические процессы используются для передачи информации на расстояние?

5) Какие существуют задачи инженерно-технических методов и средств защиты информации?

Тема 7 Получение информации в компьютерных сетях. Методы и средства инженерной защиты и технической охраны объектов

1) Что такое искусственные и естественные угрозы информационной безопасности?

2) Что такое непосредственные и косвенные каналы утечки информации?

3) Какие существуют задачи инженерно-технических методов и средств защиты информации?

4) Какие существуют методы и средства защиты от утечки информации по каналам ПЭМИН?

5) Какие существуют основные и вспомогательные способы несанкционированного доступа к информации, модель и уровни?

Тема 8 Технический контроль эффективности мер защиты информации

- 1) Как работает двухпроводная линия связи?
- 2) Как работает оптическая линия связи?
- 3) Что такое отношение сигнал/шум?
- 4) Какие виды шумов вам известны?
- 5) Что такое технический канал утечки информации?

Тема 9 Криптографические методы и средства защиты информации

- 1) Каковы основные характеристики дискретных каналов связи?
- 2) Что такое звук?
- 3) Что такое видимый свет?
- 4) Что такое радиоволны?
- 5) Каким образом информация может быть представлена на бумажном носителе?

6.4 Вопросы для подготовки к экзамену

- 1) Какие существуют принципы экранирования статических и динамических полей?
- 2) Какие существуют принципы и реализация электромагнитного экранирования приборов и помещений, его эффективность?
- 4) Какие существуют требования к экранам и их характеристики?
- 4) Какие существуют понятие об электромагнитной совместимости радиоэлектронных устройств?
- 5) Что такое упругие волны?
- 6) Что такое звуковые волны?
- 7) Как распространяется звук в различных средах?
- 8) Какие основы акустики речи и слуха?
- 9) Что такое речевой сигнал, его физические и информационные характеристики и параметры?
- 10) Какие существуют характеристики восприятия речевого сигнала?
- 11) В чем заключается различие искажений речевого сигнала и их влияние на восприятие?
- 12) Что такое параметризация речевых сигналов и акустических шумов применительно к задачам оценки качества связи, комфортности и защиты информации?
- 13) В чем заключается специфика акустики помещений?
- 14) Звуковое поле в помещениях, Акустические характеристики и параметры помещений.
- 15) Какие существуют звукоотражающие и звукопоглощающие материалы и конструкции?
- 16) В чем заключается звукоизоляция помещений, характеристики звукоизоляции?
- 17) Что такое информация?

- 18) Какие физические процессы используются для хранения информации?
- 19) Какие физические процессы используются для передачи информации на расстояние?
- 20) Что такое пропускная способность канала связи?
- 21) Каким образом та или иная информация представляется в цифровом виде?
- 22) Какие сведения может содержать цифровой носитель информации?
- 23) Каковы основные характеристики цифровых носителей информации?
- 24) Каковы основные характеристики дискретных каналов связи?
- 25) Что такое звук?
- 26) Что такое видимый свет?
- 27) Что такое радиоволны?
- 28) Каким образом информация может быть представлена на бумажном носителе?
- 29) Инфразвук. Ультразвук. Особенности распространения инфразвука и ультразвука.
- 30) Области применения инфразвуковых и ультразвуковых волн.
- 31) Виды воздействий на защищаемую информацию, цели защиты и основные характеристики защищаемой информации.
- 32) Что такое искусственные и естественные угрозы информационной безопасности?
- 33) Что такое непосредственные и косвенные каналы утечки информации?
- 34) Какие существуют задачи инженерно-технических методов и средств защиты информации?
- 35) Какие существуют методы и средства защиты от утечки информации по каналам ПЭМИН?
- 36) Какие существуют основные и вспомогательные аппаратные средства защиты информации?
- 37) Какие существуют основные и вспомогательные способы несанкционированного доступа к информации, модель и уровни?
- 38) Какие существуют основные способы защиты от несанкционированного доступа и возможной утечки информации?
- 39) Что такое база данных по физическим эффектам?
- 40) Что такое стеганография?
- 41) Что такое модуляция радиосигнала? Какие виды модуляции Вам известны?
- 42) Как работает двухпроводная линия связи?
- 43) Как работает оптическая линия связи?
- 44) Что такое отношение сигнал/шум?
- 45) Какие виды шумов вам известны?
- 46) Что такое технический канал утечки информации?
- 47) Что такое естественный канал утечки информации?

- 48) Что такое амплитуда и частота гармонического колебания?
- 49) Что такое разность фаз гармонических колебаний?
- 50) Как связаны амплитуда и действующее (среднеквадратическое) значение гармонического сигнала?
- 51) Что такое мнимая единица, что такое комплексное число?
- 52) Какие существуют формы записи комплексных чисел?
- 53) Как производятся арифметические операции с комплексными числами?
- 54) Запишите формулу Эйлера.
- 55) Что такое комплексная амплитуда гармонического колебания?
- 56) В каких случаях удобно использовать метод комплексных амплитуд?
- 57) Что происходит при сложении двух гармонических колебаний с близкими амплитудами и небольшой разницей по частоте? Что такое «биения»?
- 58) Опишите основные свойства показательной и логарифмической функций.
- 59) Как осуществить перевод в децибелы отношения энергетических величин?
- 60) Как выполнить обратный переход от децибел к отношению энергетических величин?
- 61) Что такое динамический диапазон шумового сигнала?
- 62) Как перевести отношение напряжений или токов в децибелы?
- 63) Почему децибелы широко применяются в инженерной практике?
- 64) Что такое ряд Фурье?
- 65) Как периодические колебания раскладываются в ряд Фурье?
- 66) Что такое преобразования Фурье?
- 67) Что такое спектр фаз и спектр амплитуд?
- 68) Что такое спектральная плотность энергии?
- 69) Как в частотной области представляются случайные сигналы? Что такое спектральная плотность мощности?
- 70) Каков теоретический спектр идеального гармонического колебания?
- 71) Как работают спектральные анализаторы?
- 72) Что такое разрешение спектрального анализа? Сформулируйте критерий Релея.
- 73) Как выбирается длительность и форма временного окна для спектрального оценивания?
- 74) Чем отличается спектр модулированного радиосигнала от спектра гармонического колебания?
- 75) Расскажите, как связан уровень звукового давления и воспринимаемая громкость звука. Что такое кривые равной громкости?
- 76) Опишите качественно шкалу звуковых давлений, воспринимаемых человеком.
- 77) От чего зависит разборчивость речи?

- 78) Укажите частотные диапазоны слышимости для людей и животных.
- 79) Что такое белый шум, что такое розовый шум?
- 80) Как скорость распространения звука в воздухе зависит от температуры воздуха?
- 81) Как проявляется эффект Доплера в акустике?
- 82) Как акустические волны распространяются в твёрдых телах?
- 83) Что такое акустический волновод?
- 84) Что такое интерференция?
- 85) В чём заключается явление реверберации?
- 86) Что такое электрический фильтр?
- 87) Что такое амплитудно-частотная характеристика фильтра?
- 88) Что такое полоса пропускания фильтра? Что такое полоса задерживания фильтра?
- 89) Какие паразитные эффекты ограничивают задерживание фильтрами определённых диапазонов частот?
- 90) Что такое пассивные и активные фильтры?
- 91) Какие достоинства и недостатки имеют пассивные фильтры?
- 92) Какие достоинства и недостатки имеют активные фильтры?
- 93) Изобразите АЧХ фильтра нижних частот.
- 94) Изобразите АЧХ полосового фильтра.
- 95) Изобразите АЧХ фильтра верхних частот.
- 96) Изобразите АЧХ режекторного фильтра.
- 97) Где могут использоваться режекторные фильтры с частотами подавления 50 Гц, 100 Гц, 150 Гц, 200 Гц, 250 Гц, 300 Гц?
- 98) Как строятся цифровые фильтры?
- 99) Какие преимущества и недостатки имеют цифровые фильтры?
- 100) Приведите несколько принципиальных схем пассивных фильтров нижних частот.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации: учеб. пособие по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Документ read. - Москва : РИОР [и др.], 2022. - 336 с. - (Высшее образование). - Прил. - URL: <https://znanium.com/read?id=393765> (дата обращения: 25.08.2024).

2. Сухостат В.В. Основы информационной безопасности: учебное пособие / В.В. Сухостат, И.Н. Васильева. – СПб.: Изд-во СПбГЭТУ, 2019. – 103 с. Режим доступа: <https://infosec.spb.ru/wp-content/uploads/2020/06/osnovy-informacionnoj-bezopasnosti.pdf> (дата обращения: 25.08.2024).

3. Родичев Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации: учебное пособие для студентов, обучающихся по программам высшего образования / Ю. А. Родичев. – Москва [и др.]: Питер, 2019. – 304 с. Режим доступа: <https://chitat-online.org/str/informacionnaya-bezopasnost-nacionalnye-standarty-rossiyskoy> (дата обращения: 25.08.2024).

4. Гродзенский Я.С. Информационная безопасность: учебное пособие / Я. С. Гродзенский. - Москва: Проспект, 2021. - 142 с. Режим доступа: <https://knigogid.ru/books/1582163-informacionnaya-bezopasnost-nacionalnye-standarty-rossiyskoy-federacii/toread/fragment> (дата обращения: 25.08.2024).

Дополнительная литература

1. Акустика: Справочник. / Ефимов А.П., Никонов А.В., Сапожников М.А., Шоров В.Й. / Под ред. М.А. Сапожков. 2-е изд., перераб. и доп.— М.: Радио и связь, 1989. —336 с. <https://djvu.online/file/M8iaRxreMsaei?ysclid=m3bz5q0ibj191987760> (дата обращения: 25.08.2024).

2. Варганесян В.А. Радиоэлектронная разведка - М.: Воениздат, 1991–254 с. <https://djvu.online/file/RyB48NEvCQnPy?ysclid=m3bz8tgvjw728877862> (дата обращения: 25.08.2024).

3. Верещагин И.К., Косяченко Л.А., Кокин СМ. Введение в оптоэлектронику: Учебное пособие для вузов — М.: Высшая школа, 1991. —191 с. <https://m.eruditor.one/file/1709471/?ysclid=m3bzbw9cvh807003090> (дата обращения: 25.08.2024).

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

1. Научная библиотека ФГБОУ ВО «ДонГТУ»
<http://library.dstu.education>
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. Федеральная служба по экологическому, технологическому и атомному надзору (Ростехнадзор): официальный сайт. — Москва. — <https://www.gosnadzor.ru/>. — Текст: электронный.
7. Сайт кафедры СКС <http://scs.dstu.education/>
8. Сайт дистанционного обучения ДонГТУ <http://do.dstu.education>

8 Условия реализации дисциплины

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

Материально-техническое обеспечение представлено в таблице 7.

Таблица 7 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
<p>Специальные помещения: <i>Мультимедийная аудитория. (60 посадочных мест)</i>, оборудованная специализированной (учебной) мебелью (скамья учебная – 20 шт., стол – 1 шт., доска аудиторная – 1 шт.), учебный ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций:</p> <p><i>Компьютерные классы (22 посадочных места)</i>, оборудованные учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: -ПК Intel Core 2 DUO 2.5 Ghz, 1024,160 – 1 шт.; - ПК Intel Celeron 2.0, 256, 40- 1 шт. Доска – 1 шт.</p> <p>- ПК Intel Celeron 2.0, 256, 40-1 шт - ПК Intel Pentium IV 2.4, 2X256, 2x 80 - 1 шт - ПК AMD Athlon 1.6, 4096, 500 -10 шт.</p>	<p>ауд. <u>207</u> корп. <u>4</u></p> <p>ауд. <u>208</u> корп. <u>4</u> ауд. <u>211</u> корп. <u>4</u></p> <p>ауд. <u>217</u> корп. <u>3</u></p>

Студенты имеют доступ в компьютерные классы с 8 до 16 часов, в том числе для выполнения индивидуальных заданий и самостоятельной работы.

Лист согласования РПД

Разработал
И.о.заведующего кафедрой
интеллектуальных систем и
информационной безопасности
 (должность)


 (подпись)

Е.Е.Бизянов
 (Ф.И.О.)

 (должность)

 (подпись)

 (Ф.И.О.)

 (должность)

 (подпись)

 (Ф.И.О.)

И.о. заведующего кафедрой
 интеллектуальных систем и
 информационной безопасности


 (подпись)

Е.Е. Бизянов
 (Ф.И.О.)

Протокол № 1 заседания кафедры
 интеллектуальных систем и
 информационной безопасности

от 27.08.2024 г.

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


 (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

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	