

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

РЕКОМЕНДОВАНО К

УТВЕРЖДЕНИЮ:

Декан, председатель совета

факультета КТ, ВТиЭ

 Ш.А. Юсуфов

18 10 2018 г.

УТВЕРЖДАЮ:

Проректор по учебной работе,

председатель методического

совета ДГТУ

 Н.С. Суракатов

21 10 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.Б.12 Теория информации
для специальности 10.05.03 – Информационная безопасность автоматизированных систем

специализация Безопасность открытых информационных систем

факультет Компьютерных технологий, вычислительной техники и энергетики

наименование факультета, где ведется дисциплина

кафедра Программного обеспечения вычислительной техники и автоматизированных систем

наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) специалист по защите информации

Форма обучения очная; курс 3; семестр(ы) 5;

Всего трудоемкость в зачетных единицах (часах) 2 ЗЕТ(72);

Лекции 34 (час); Экзамен -

Практические (семинарские) занятия -; Зачет 5 семестры 2 ЗЕТ (72ч.)

Лабораторные занятия 17 (час); Курсовая работа - (семестр);

Самостоятельная работа 21 (час).

Зав. кафедрой  В.Б. Мелехин

Начальник УО  Э.В. Магомаева



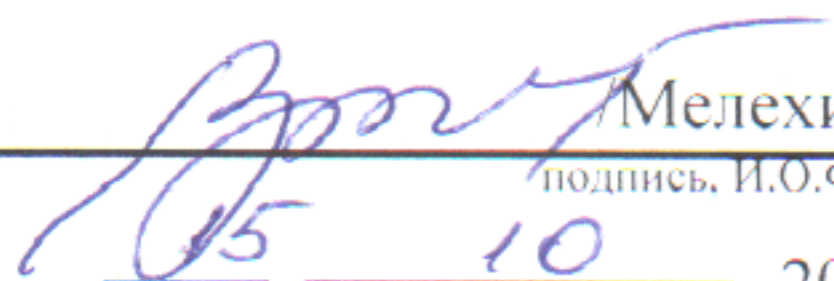
Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению 10.05.03 «Информационная безопасность», профилю подготовки «Безопасность автоматизированных систем».

Программа одобрена на заседании выпускающей кафедры ИБ от 15. 10 2018 г., протокол № 2

Зав. кафедрой  Качаева Г.И.

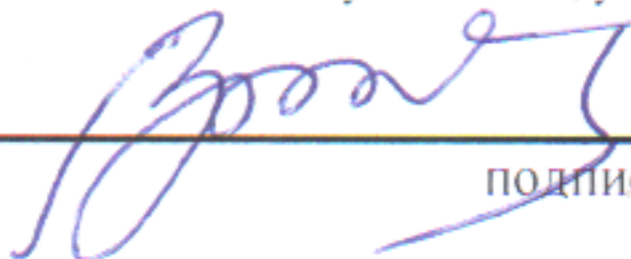
**ОДОБРЕНО:
МЕТОДИЧЕСКОЙ КОМИССИЕЙ ПО
УКРУПНЕННЫМ ГРУППАМ
СПЕЦИАЛЬНОСТЕЙ И НАПРАВЛЕНИЙ
ПОДГОТОВКИ
10.00.00 – Информационная безопасность**

**ПРЕДСЕДАТЕЛЬ МЕТОДИЧЕСКОЙ
КОМИССИИ**

 Мелехин В.Б./
подпись, И.О.Ф.
15 10 2018г.

АВТОР(Ы) ПРОГРАММЫ:

Мелехин В.Б. д.т.н., профессор
И.О.Ф., уч. степень, ученое звание


подпись

1. Цели освоения дисциплины

Учебная дисциплина «Теория информации» является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Она призвана обеспечить знакомство слушателей с основными понятиями и методами теории информации и ее приложениями в современных информационных технологиях, ознакомление с методами количественной оценки информации, тем самым создавая у обучающихся представление о структуре профессиональных навыков получаемой специальности.

Дисциплина «Теория информации» относится к числу прикладных математических дисциплин в силу отбора изучаемого материала и его важности для подготовки специалиста. Во всех разделах дисциплины большое внимание уделяется построению алгоритмов для решения практических задач.

Задачи дисциплины:

- раскрыть содержание базовых понятий теории информации;
- изучить математические модели источников информации и каналов связи;
- дать представление о предельно допустимых значениях теоретико-информационных характеристик систем передачи информации.

Таким образом, дисциплина «Теория информации» является неотъемлемой составной частью профессиональной подготовки по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных». Вместе с другими дисциплинами математического и естественнонаучного цикла изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

- строгость в суждениях,
- творческое мышление,
- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

2. Место дисциплины в структуре ООП

Дисциплина принадлежит математическому и естественнонаучному циклу дисциплин.

Дисциплина «Теория информации» основывается на знаниях, полученных при изучении дисциплин

- «Математический анализ»,
- «Алгебра»,
- «Теория вероятностей и математическая статистика»,
- «Дискретная математика»,
- «Математическая логика и теория алгоритмов».

Знания, полученные при изучении дисциплины «Теория информации», используются при изучении дисциплин

- «Криптографические методы защиты информации»,
- «Криптографические протоколы».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Теория информации»

В результате освоения дисциплины у обучающихся должна быть сформирована следующая общекультурная компетенция:

- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);
- способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);
- способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);
- способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);
- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6).

В результате освоения дисциплины студент должен:

Знать:

- как измеряется информация, законы изменения количества информации при ее преобразовании, какие средства существуют для борьбы с помехами, как устроены алгоритмы сжатия информации;
- современные информационные технологии.

Уметь:

- применять на практике знания, полученные по курсу "Теория информации",
- применять вероятностный и информационный подход к смежным дисциплинам,
- самостоятельно приобретать новые знания в области кодирования и передачи сигналов.

Владеть навыками:

- теоретическими знаниями о свойствах энтропии, знать определения эргодического источника, канала, уметь доказывать основные теоремы кодирования для дискретных источников и каналов, знать строение основных помехоустойчивых кодов, знать оценки предельного сжатия информации

Демонстрировать способность и готовность:

- решать задачи, связанные с анализом систем, подверженных влиянию шумов,
- составлять математические модели анализируемых систем,
- применять современные информационные технологии.

4. Структура и содержание дисциплины (модуля) «Теория информации»

4.1. Содержание дисциплины

№ п/ п	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля (по срокам текущей аттестации)
				ЛК	ПЗ	ЛР	СРС	
1	2	3	4	5	6	7	8	9
3 семестр								
1.	<p>Лекция 1. Тема: Модели детерминированных сигналов. Понятие модели сигнала. Обобщенное спектральное представление детерминированных сигналов. Временная форма представления сигналов. Частотное представление периодических сигналов. Распределение энергии в спектре периодического сигнала. Частотное представление непериодических сигналов. Распределение энергии в спектре непериодического сигнала.</p>	5	1	2	-	-	1	<i>Входная контрольная работа</i>
2.	<p>Лекция 2. Тема: Модели случайных сигналов. Случайный процесс как модель сигнала. Спектральное представление случайных сигналов. Частотное представление стационарных случайных сигналов, дискретные спектры. Частотное представление стационарных случайных сигналов, непрерывные спектры. Спектральная плотность мощности</p>	5	2	2	-	2	2	
3.	<p>Лекция 3. Тема: Преобразование непрерывных сигналов в дискретные. Формулировка задачи дискретизации. Критерии качества восстановления непрерывного сигнала. Теорема Котельникова. Квантование сигналов</p>	5	3	2	-	-	1	
4.	<p>Лекция 4. Тема: Меры неопределенности дискретных множеств Вероятностное описание дискретных ансамблей и источников. Энтропия, как мера неопределенности выбора. Свойства энтропии. Условная энтропия и её свойства</p>	5	4	2	-	2	1	

5	<p>Лекция 5. Тема: Меры неопределенности непрерывных случайных величин. Понятие дифференциальной энтропии. Понятие дифференциальной условной энтропии. Свойства дифференциальной энтропии. Распределения, обладающие максимальной дифференциальной энтропией</p>	5	5	2	-	-	1	Атт-я КР№1
6.	<p>Лекция 6 Тема: Количество информации как мера снятой неопределенности. Количество информации при передаче отдельного элемента дискретного сообщения. Свойства частного количества информации. Среднее количество информации в любом элементе дискретного сообщения. Свойства среднего количества информации в элементе сообщения. Количество информации при передаче сообщений от непрерывного источника. Эпсилон-энтропия случайной величины. Избыточность сообщений.</p>	5	6	2	-	2	1	
7.	<p>Лекция 7. Тема: Оценка информационных характеристик источников сообщений. Понятие эргодического источника сообщений. Теорема о свойствах эргодических последовательностей знаков. Производительность источника дискретных сообщений. Эпсилон-производительность источника непрерывных сообщений</p>	5	7	2	-	-	1	
8.	<p>Лекция 8. Тема: Информационные характеристики каналов связи. Модели дискретных каналов. Скорость передачи информации по дискретному каналу. Пропускная способность дискретного канала без помех. Пропускная способность дискретного канала с помехами. Скорость передачи по непрерывному гауссову каналу связи. Пропускная способность непрерывного гауссова канала связи. Согласование физических характеристик сигнала и канала</p>	5	8	2	-	2	1	
9.	<p>Лекция 9. Тема: Эффективное кодирование. Цель кодирования. Основные понятия и определения. Основная теорема Шеннона о кодировании для канала без помех. Методы эффективного кодирования некоррелированной последовательности знаков, код Шеннона-Фано. Методика кодирования Хаффмана. Методы эффективного кодирования коррелированной последовательности знаков. Недостатки системы эффективного кодирования</p>	5	9	2	-	-	1	

10.	<p>Лекция 10. Тема Введение в теорию помехоустойчивого кодирования. Теорема Шеннона о кодировании для канала с помехами. Общие принципы построения помехоустойчивых кодов. Математическое введение к линейным кодам</p>	5	10	2	-	2	2	АТТ-я КР№2
11.	<p>Лекция 11. Тема: Построение групповых кодов. Понятие корректирующей способности кода. Общая схема построения группового кода. Связь корректирующей способности с кодовым расстоянием. Построение опознавателей ошибок. Определение проверочных равенств и уравнений кодирования.</p>	5	11	2	-	-	1	
12.	<p>Лекция 12. Тема: Циклические коды. Математическое введение к циклическим кодам. Понятие и общая схема построения циклического кода. Построение циклического кода на кольце многочленов. Выбор образующих многочленов для обнаружения и исправления одиночных ошибок. Методы формирования комбинаций и декодирования циклического кода</p>	5	12	2	-	2	2	
13.	<p>Лекция 13. Тема: Матричные представления в теории кодирования. Групповой код как подпространство линейного пространства. Понятие образующей матрицы. Построение разрешенных кодовых комбинаций с использованием образующей матрицы. Построение матрицы-дополнения. Понятие и построение проверочной (контрольной) матрицы. Границы для числа разрешенных комбинаций. Матричное представление циклических кодов. Построение проверочной матрицы циклического кода</p>	5	13	2	-	-	1	
14.	<p>Лекция 14. Тема: Кодирование линейными последовательными машинами. Понятие линейной последовательной машины (ЛПМ) Матричное описание ЛПМ. Каноническая и естественная нормальная форма ЛПМ. Подобные и минимальные ЛПМ. Понятие простой автономной ЛПМ (АЛПМ). Формирование разрешенных комбинаций циклического кода с помощью АЛПМ. Образующая матрица АЛПМ</p>	5	14	2	-	2	1	

15.	Лекция 15. Тема: Обнаружение и различение сигналов. Постановка задачи обнаружения сигналов при наличии помех. Обнаружение по критерию максимального правдоподобия. Обнаружение сигналов по критерию максимума апостериорной вероятности. Информационный критерий обнаружения. Обнаружение по критерию Неймана-Пирсона. Обнаружение сигналов по критерию минимального риска. Различение сигналов.	5	15	2	-	2	2	Атт-я КР№3
16.	Лекция 16 Тема: Оценка параметров сигналов. Общая формулировка задачи восстановления сигналов. Задача оценки параметров линейных моделей. Достижимая точность, неравенство Крамера-Рао.	5	16	2	-	1	1	
17	Лекция 17 Тема: Оценка параметров сигналов. Оценки, минимизирующие среднеквадратическую ошибку. Оценки максимального правдоподобия. Оптимальность оценок МНК и максимального правдоподобия. Байесовские оценки	5	17				1	
Итого за 5 семестр				34		17	21	Зачет
Итого 72 часа								

4.2. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	Количество часов	Рекомендуемая литература и методические разработки(№источника из списка литературы)
5 семестр				
1	№1	Спектральная плотность мощности	2	№1 - №5
2	№2	Энтропия	2	№1 - №4
3	№3	Количество информации	2	№1 - №5
4	№4	Эффективное кодирование.	4	№1-№5
5	№5	Циклические коды	2	№1-№5
6	№6	Кодирование линейными последовательными машинами.	2	№1, №2, №5
7	№7	Задача оценки параметров линейных моделей.	3	№1-№5
Итого за 5 семестр			17	

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Форма контроля СРС
3 семестр				
1	Распределение энергии в спектре периодического сигнала.	1	№1-№5	Кр№1
2	Модели случайных сигналов.	2	№1, №2, №5	КР№1
3	Преобразование непрерывных сигналов в дискретные.	1	№1-№4	КР№1
4	Энтропия, как мера неопределенности выбора. Свойства энтропии.	1	№1-№5	Кр№1
5	Дифференциальная энтропия.	1	№1-№4	КР№1
6	Количество информации как мера снятой неопределенности.	1	№2	КР№1
7	Понятие эргодического источника сообщений.	1	№1.№2,№5	КР№1
8	Модели дискретных каналов.	1	№2	КР№2
9	Методика кодирования Хаффмана	1	№1, №2, №5	КР№2
10	Теорема Шеннона о кодировании для канала с помехами.	2	№4, №4	КР№2
11	Общая схема построения группового кода.	1	№3, №4	КР№2
12	Понятие и общая схема построения циклического кода.	2	№3, №4, №5	КР№2
13	Построение разрешенных кодовых комбинаций с использованием образующей матрицы.	1	№1, №3, №5	КР№2
14	Понятие линейной последовательной машины (ЛПМ) Матричное описание ЛПМ.	1	№1, №5	КР№3
15	Обнаружение и различение сигналов.	2	№2, №5	КР№3
16	Задача оценки параметров линейных моделей.	1	№1, №2, №4	КР№3
17	Оптимальность оценок МНК и максимального правдоподобия.	1	№1- №5	КР№3
Итого за 5 семестр		21		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

При проведении занятий по учебной дисциплине рекомендуется следовать и традиционным технологиям, в частности, в каждом разделе курса выделять наиболее важные моменты, акцентировать на них внимание обучаемых.

При чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволит сделать изложение наглядным и продемонстрировать обучаемым приемы программирования.

При изучении всех разделов программы добиться точного знания обучаемыми основных исходных понятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно– методическое обеспечение самостоятельной работы студентов

5 СЕМЕСТР

Аттестационная контрольная работа №1

1. Введение в теорию информации и информационных систем.
2. Понятие информации и количественные меры информации.
3. Источники информации.
4. Информационные характеристики источников сообщений и каналов передачи информации.
5. Скорость передачи информации и пропускная способность каналов.
6. Теоремы Шеннона для идеального и реального каналов, согласование источников с каналами.
7. Основные понятия теории кодирования информации.
8. Моделирование и генерация кода.

Аттестационная контрольная работа №2

1. Эффективные и криптографические коды. Эффективность кода.
2. Вычислительная сложность алгоритма кодирования.
3. Принципы эффективного кодирования.
4. Неравенство Крафта и теорема Макмиллана.
5. Теорема кодирования Шеннона. Коды Коломба и Райса.
6. Коды Шеннона-Фано и Хаффмена.
7. Методы генерации блочных кодов.
8. Арифметическое кодирование.
9. Методы эффективного кодирования на основе вероятностных и комбинаторных моделей.
10. Корректирующие коды.
11. Избыточность сообщений.
12. Расстояния Хемминга.
13. Линейные коды.
14. Понятие циклической перестановки и циклические коды.
15. Эффективность корректирующего кодирования.

Аттестационная контрольная работа №3

1. Информационные системы и сигналы.
2. Линейные и нелинейные системы.
3. Модели детерминированных и стохастических систем и сигналов.
4. Дискретизация и квантование сигналов.
5. Модуляция и управление информационными параметрами сигналов.
6. Критерии верности и потенциальная помехоустойчивость передачи сообщений.
7. Принципы обнаружения, оценивания параметров и фильтрации сигналов.
8. Методы оптимального приема сообщений.

Вопросы для зачетной работы

1. Избыточность естественного языка. Задачи теории информации.
2. Энтропия и сжатие информации.
3. Теорема Шеннона. Измерение информации. Примеры.
4. Метод Хаффмана сжатия информации.
5. Арифметическое кодирование.
6. Взаимная энтропия и взаимная информация.
7. Емкость зашумленного канала.
8. Теорема кодирования для канала с шумом.
9. Основные результаты для канала с шумом и байесовский вывод.
10. Вывод параметром и моделей.
11. Аппроксимация распределений вероятностей: кластеризация.
12. Метод Монте-Карло.
13. Вариационный метод.
14. Емкость нейрона.
15. Ассоциативная память.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Рекомендуемая литература и источники информации

(основная и дополнительная)

№	Виды занятий (лк, пр, лб, срс)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литер-ры	
					в библи	на каф
О С Н О В Н А Я						
1.	Лк, лб, срс	Введение в дискретную теорию информации и кодирования	Чечёта С. И.	– М.: МЦНМО, 2011.		
2.	Лк, лб, срс	Сапоженко А.А. Задачи и упражнения по дискретной математике.	Гаврилов Г.П.	– М.: ФИЗМАТ ЛИТ, 2004.		
3.	Лк, лб, срс	. Теория информации и кодирования (vimvd.ru/institute/structure/chairs/vm/methodical/inf.pdf)	Думачев В.Н	–Воронеж: В-кий институт МВД России, 2012. -200 с.		
4.	Лк, лб, срс	Теория информации и кодирования (Часть 1 – Теория потенциальной помехоустойчивости) http://api.rucont.ru/api/efd/reader?file=641654	О.В. Горячкин	.— Самара : Изд-во ПГУТИ, 2017.— 94 с		
5.	Лк, лб, срс	Теоретические основы информатики : учебное пособие [для студентов очной формы обучения] https://esstu.bibliotech.ru/Reader/Book/2015100805052646400000447909	Л. Д. Жимбуева, Т. Ц. Дамдинова, Б. Б. Будажапова ;	. - Улан-Удэ : Издательство ВСГУТУ, 2015. - 105 с.		
Д О П О Л Н И Т Е Л Ь Н А Я						
6.	Лк, лб, срс	Основы теории передачи информации : учебное пособие	Литвинская О. С.	— М. : КНОРУС, 2010. — 168 с		
7.	Лк, лб, срс	Компьютерные сети. Принципы, технологии, протоколы :	В. Г. Олифер, Н. А. Олифер	Нижний Новгород : ПИТЕР, 2015. - 943 с.		

8. Материально-техническое обеспечение дисциплины


Для проведения лекционных занятий и лабораторного практикума на основе интерактивных методов обучения необходим доступ в Интернет из компьютерного зала, наличие цифрового проектора для применения современных обучающих мультимедиа – технологий. Для проведения лабораторных занятий необходимы аудитории оснащенные современными персональными компьютерами, объединенными в локальную вычислительную сеть и укомплектованным необходимым системным и прикладным программным обеспечением.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», профилю подготовки «Безопасность открытых информационных систем».

Рецензент рабочей программы от выпускающей кафедры по направлению 10.05.03 – Информационная безопасность автоматизированных систем


подпись


должность


ФИО