

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)



«УТВЕРЖДАЮ»
Проректор по ОД
А.А.Панфилов
« 09 » 2016г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
"Методы защиты информации"

Направление подготовки: 11.04.01 «Радиотехника»

Профили / программа подготовки:

Уровень высшего образования: магистратура

Форма обучения: очная

Семестр	Трудоемкость (зач. ед, /час.)	Лекций, (час.)	Практ. занятий, (час.)	Лаборат. работ, (час.)	СРС, (час.)	Форма контроля (экз./зачет)
2	3/108	-	18	36	54	Зачет
Итого	3/108	-	18	36	54	Зачет

Владимир, 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Методы защиты информации» являются:

1. Подготовка в области знания основных средств повышения помехоустойчивости современных радиотехнических систем при создании радиоэлектронной аппаратуры.
2. Формирование практических навыков работы с научными методами расчета и проектирования.
3. Основная подготовка магистров в области радиотехники производится для научно-исследовательской сферы профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина "Методы защиты информации" относится к вариативной части дисциплин по выбору (Б1.В.ДВ.2)

Взаимосвязь с другими дисциплинами

Курс "Методы защиты информации" основывается на знании предметов бакалаврского образования, таких, как «Математика», «Физика», «Основы теории связи» и магистерского образования, такого, как «История и методология науки и техники (применительно к радиотехнике)», и др., логически и содержательно-методически связан с ними.

Полученные знания могут быть использованы при подготовке магистерской диссертации, а также в процессе разработки и проектирования радиоаппаратуры.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Способность самостоятельно приобретать и использовать в практической деятельности новые знания и умения в своей предметной области. (ОПК-4);

Способность самостоятельно осуществлять постановку задачи исследования, формирование плана его реализации, выбор методов исследования и обработку результатов (ПК-1);

Способность выполнять анализа и оптимизации их параметров с использованием имеющихся средств исследований, включая стандартные пакеты прикладных программ (ПК-2);

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

Знать: методики разработки рабочих планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей; пути сбора, обработки и систематизации научно-технической информации по теме планируемых исследований, выбор методик и средств решения сформулированных задач;

Уметь: проводить моделирование объектов и процессов в радиотехнических устройствах с целью анализа и оптимизации их параметров с использованием имеющихся средств исследований, включая стандартные пакеты прикладных программ; осуществлять разработку программ экспериментальных исследований, ее реализация, включая выбор технических средств и обработку результатов;

Владеть: навыками подготовки научно-технических отчетов в соответствии с требованиями нормативных документов, составления обзоров и подготовки публикаций; разработки патентных документов на образцы новой техники.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ: "Методы защиты информации"
Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)								Объем учебно й работы с приме ние м интер актив ных методо в	Формы текуще го контро ля успева емости, форма промеж уточной аттестаци и
				Лекции	Консультации	Семинары	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП/КР		
1.	Постановка задачи защиты информации. Обзор основных методов кодирования	2	1				1			2			
2.	Сверточные коды	2	2,3				2	4		6		2/33	
3.	Блочные коды	2	4,5				2	4		6		2/33	Рейтин г- контр оль 1
4.	Недвоичные и нелинейные коды	2	6				1			2			
5.	Виды сложных кодов. Модифицированные, укороченные и расширенные коды	2	7				1	4		2		1/20	
6.	Перфорированные коды	2	8				1	4		6			
7.	Комбинированные и каскадные коды	2	9				2	4		6		2/33	Рейти нг- контр оль 2
8.	Турбокоды	2	10				2			4		1/50	

9.	Итеративно декодируемые коды и многопороговое декодирование	2	11, 12				2		+	4		1/50	
10	Сигнально-кодовые конструкции. Перспективы развития методов защиты информации	2	13				1			4		1/100	
11	Декодирование сверточных кодов	2	14, 15				2	8		6		4/33	
12	Декодирование блочных кодов	2	16-18				2	8		6		4/33	Рейтинг-контроль 3
Всего							18	36		54		18/33	зачет

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

5.1. Активные и интерактивные формы обучения

С целью формирования и развития профессиональных навыков студентов в учебном процессе используются активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой: (практические работы, контрольные аудиторские работы, индивидуальные домашние работы). Объем занятий, проводимых в интерактивных формах, составляет 18 часов, 12 часов консультационных занятий (вне расписания), контрольные работы 4 часа (на практических занятиях).

5.2. Самостоятельная работа студентов

Самостоятельная (внеаудиторная) работа студентов включает закрепление теоретического материала при подготовке к выполнению практических заданий, а также при выполнении индивидуальной домашней работы. Основа самостоятельной работы - изучение литературы по рекомендованным источникам и конспекту лекций.

5.3. Мультимедийные технологии обучения

Практические занятия могут дополняться презентациями в мультимедийной аудитории с использованием компьютерного проектора и представлением от 10 до 20 слайдов по каждой теме.

Студентам предоставляется компьютерный курс теоретических сведений.

5.4. Рейтинговая система обучения

Рейтинг-контроль проводится три раза за семестр. Он предполагает оценку суммарных баллов по следующим составляющим: активность на контрольных занятиях; качество выполнения домашних рейтинговых заданий и лабораторных работ

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6.1. Вопросы к зачету

1. Использование кодирования сигналов для защиты информации
2. Классификация основных видов кодов.
3. Основные принципы сверточного кодирования.
4. Связь параметров сверточного кода со структурами для его получения.
5. Систематические и несистематические сверточные коды.
6. Двоичные блочные коды.
7. Построение блочного кода с помощью таблицы соответствия.
8. Построение блочного кода с помощью порождающей матрицы.
9. Алгоритм построения циклических кодов.
10. Коды Хэмминга и Голея.
11. Коды Рида-Малера и БЧХ.
12. Недвоичные и нелинейные коды.
13. Методы построения модифицированных кодов.
14. Перфорированные коды.
15. Каскадные коды.
16. Турбокоды.
17. Итеративно декодируемые коды.
18. Сигнально-кодовые конструкции.
19. Методы декодирования сверточных кодов.
20. Методы декодирования блочных кодов.

6.2. Тесты для рейтинг-контроля

Рейтинг-контроль 1

1. За счет каких факторов при кодировании различными методами возникает выигрыш в помехоустойчивости передачи сигналов.
 - за счет введения различных видов модуляции;
 - за счет введения избыточности символов;
 - за счет сужения занимаемой полосы частот.
2. Основные отличия сверточных кодов от кодов прочих видов заключаются:
 - в том, что каждый кодовый символ получается на основе нескольких предыдущих информационных символов;
 - в том, что каждый кодовый символ получается на основе одного специально выбранного предыдущего информационного символа;
 - в том, что каждый кодовый символ получается умножением очередного информационного символа на предыдущий кодовый символ.
3. Основные отличия блочных кодов от кодов прочих видов заключаются:
 - в поочередной группировке информационных и кодовых символов;
 - в формировании на приемной стороне блоков из принятых символов;
 - в вычислении кодовых символов на основе блоков информационных символов.
4. Основные отличия систематических и несистематических кодов в сверточных и блочных алгоритмах кодирования заключаются в:
 - кодовые символы формируются систематически или бессистемно;
 - в формируемой кодовой последовательности можно или нельзя выделить информационные символы;
 - виды кодов образуют или не образуют строгую систему для их классификации;

5. Основные отличия двоичных и недвоичных блоковых кодов.

- каждый символ принимает значения из двоичной (троичной, четвертичной и т.д.) систем исчисления;
- для недвоичных кодов необходимо использовать специальные виды модуляции;
- для формирования кодов требуется использовать алгебру Буля или алгебру Галуа.

Рейтинг-контроль 2

1. Сравнить сложность построения блоковых кодов с помощью таблиц соответствия, с помощью порождающих матриц и с помощью порождающих полиномов.

- самый простой путь дают таблицы соответствия;
- самый простой путь заключается в использовании порождающих полиномов;
- самый простой путь заключается в использовании порождающих матриц.

2. В чем отличия кода Хемминга и кодов БЧХ.

- в принципах формирования
- в сложности получения;
- в использовании различной элементной базы.

3. Назначение модификации кодов и выигрыш от их применения.

- удешевление применяемой элементной базы;
- увеличение помехоустойчивости;
- изменение кодовой скорости.

4. Особенности алгоритма перфорации кодов.

- удаление части кодовых символов после кодирования
- удаление части информационных символов до кодирования;
- удаление части принятых символов на приемной стороне;
- передача различных кодовых символов с разной мощностью.

5. Структура каскадных кодов.

- результирующий код состоит в последовательном кодировании двумя кодами;
- результирующий код состоит в параллельном кодировании несколькими кодами;
- на различных интервалах радиолинии применяются различные виды кодирования.

Рейтинг-контроль 3

1. Достоинства итеративно декодируемых кодов:

- повышение помехоустойчивости;
- реализация «мягкого» декодирования;
- применение однотипной элементной базы.

2. Недостатки итеративно декодируемых кодов:

- замедление операции декодирования;
- возможные срывы алгоритмов декодирования;
- увеличение объема и массы декодеров.

3. Особенности сигнально-кодовых конструкций.

- упрощение операции кодирования;
- комплексное осуществление операций кодирования и модуляции;
- упрощение передачи кодированных сигналов;
- упрощение приема кодированных сигналов.

4. Основные принципы декодирования сверточных кодов.
 - вычисление и сравнение метрик различных путей по кодовой решетке;
 - обратное развертывание кодов;
 - отбрасывание ненужных проверочных символов.
5. Основные принципы декодирования блочных кодов.
 - разбиение принятых блоков в одномерную последовательность;
 - вычисление синдромов;
 - преобразование блочного кода в сверточный код;
 - запрос на повторную передачу поврежденных символов.

6.3. Задания к СРС

В рамках выполнения задания к СРС магистрант подготавливает и защищает реферат по вопросам следующей тематики:

1. Место кодирования сигналов в методах защиты информации.
2. Виды параметрической избыточности и связанные с ними особенности различных методов кодирования.
3. Реализация сверточной обработки информационных последовательностей как принцип построения сверточных кодов.
4. Особенности применения порождающих полиномов и порождающих матриц при формировании блочных кодов.
5. Взаимные преимущества систематических и несистематических кодов.
6. Использование методов конечной алгебры при формировании недвоичных блочных кодов.
7. Обзор видов циклических кодов и анализ их возможностей при повышении помехоустойчивости передачи информации.
8. цели использования модифицированных и перфорированных кодов и алгоритмы их формирования.
9. Переход к каскадным кодам и турбокодам, как метод повышения эффективности кодирования сигналов.
10. «Мягкое» и «жесткое» декодирование и коды с низкой плотностью проверки на четность.
11. Особенности реализации «мягкого» декодирования сверточных кодов.
12. Методика использования алгоритма Витерби при декодировании сверточных кодов.
13. Использование синдромов при поиске и устранении ошибок при декодировании сигналов.
14. Применение сигнально-кодовых конструкций.
15. Решетчатое кодирование и алгоритм TSM.

7.УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература (Библиотека ВлГУ):

1. Цифровые видеоинформационные системы (теория и практика) [Электронный ресурс] / Дворкович В.П., Дворкович А.В. - М. : Техносфера, 2012. - <http://www.studentlibrary.ru/book/ISBN9785948363363.html>

2. Основы формирования, передачи и приема цифровой информации [Электронный ресурс] : учебное пособие / В.И. Лузин, Н.П. Никитин, В.И. Гадзиковский. – М. : СОЛОН-ПРЕСС, 2014. – <http://www.studentlibrary.ru/book/ISBN9785321019610.html>
3. Конечные поля в телекоммуникационных приложениях. Теория и применение FEC, CRC, M-последовательностей/Власов Е.Г. - М.: НИЦ ИНФРА-М, 2016. - 280 с.: ISBN 978-5-16-009437-3 <http://znanium.com>

Дополнительная литература:

1. Введение в дискретную теорию информации и кодирования [Электронный ресурс]: учебное издание / Чечёта С.И. – М.: МЦНМО, 2011. – <http://www.studentlibrary.ru/book/ISBN9785940577010.html>
2. Сидельников В.М. Теория кодирования. – Физматлит, 2008. – 324с.– ISBN 978-5-9221-0943-7 – www.e.lanbook.com
3. Аверченков, В. И. Системы защиты информации в ведущих зарубежных странах [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – 3-е изд., стереотип. – М. : ФЛИНТА, 2011. – 224 с. – ISBN 978-5-9765-1274-0 <http://znanium.com/>

Отечественные журналы:

- Радиотехника;
- Радиотехника и электроника;
- Приборы и техника эксперимента;
- Цифровая обработка сигналов.

Реферативные журналы:

- Радиотехника;
- Электроника.

Зарубежные журналы:

- IEEE Transactions on Communications;
- IEEE Transactions on Signal Processing;
- IEEE Transactions on Instrumentation and Measurement.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Материально-техническое обеспечение дисциплины включает:

- кафедральные мультимедийные средства (ауд. 301-3 и 335-3);
- наборы слайдов (от 10 до 20 слайдов по каждому занятию);

Примечания:

1. Общее число подготовленных слайдов более 100, они ежегодно редактируются и модернизируются в соответствии с развитием технической и методической базы.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению «Радиотехника» и профилям подготовки «Радиотехника» и «Радиофизика».

Рабочую программу составил профессор каф. РТ и РС Полушин П.А.

Рецензент,

Генеральный директор ОАО

«Владимирское КБ радиосвязи», к.т.н. А.Е.Богданов

Программа одобрена на заседании каф. РТ и РС

Протокол № 1 от 1.09.2016

Заведующий кафедрой РТ и РС Никитин О.Р.

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления

Протокол № 1 от 2.09.2016 года

Председатель комиссии Никитин О.Р.

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 16/17 учебный год

Протокол заседания кафедры № 1 от 1.09.16 года

Заведующий кафедрой О.Р.Никитин

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий

кафедрой _____