МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Теория информации и кодирования

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Теория информации и кодирования» являются изучение студентами основных принципов построения и анализа математических моделей процессов создания, обработки и передачи информации.

Дисциплина обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, является одной из базовых дисциплин для изучения методов защиты компьютерной информации.

Задачами дисциплины является:

изучение принципов построения кодов;

освоение способов синтеза кода по требуемым показателям достоверности; научиться разрабатывать программы экспериментального исследования каналов связи с целью разработки математической модели источника ошибок в канале связи, выбор аппаратуры для проведения эксперимента, распределение обязанностей между участниками эксперимента;

доказательство по средствам использования аналитических и имитационных моделей соответствие выбранных кодов требуемым показателям достоверности приема информации;

разработка математической модели источника ошибок в канале связи;

доказательство работоспособности кодеров и декодеров помехоустойчивых кодов.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач защиты информации

- нормативно-правовые документы в области защиты информации

- информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

Уметь:

- Применять систему фундаментальных знаниий (математических, естественнонаучных и инженерных) для формулирования и решения проблем задач защиты информации.

- Применять методы математического моделирования для формализации содержательно отчетливо сформулированных проблем.

Владеть:

- навыками анализа информации и информационной безопасности в развитии современного общества, значимость своей будущей профессии.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Сем. №4
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	48	48
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации

образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 64 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Общие вопросы передачи информации Рассматриваемые вопросы: - Общие вопросы передачи информации
2	Общая структурная схема передачи информации. Рассматриваемые вопросы: - Общая структурная схема передачи информации. - Линия связи. - Канал связи. - Сообщение. - Сигнал. - Помеха. - Классификация помех. - Модели помех. - Способы приема.
3	Расчет вероятности ошибки на символ Рассматриваемые вопросы: - Расчет вероятности ошибки на символ
4	Введение в теорию кодирования Рассматриваемые вопросы: - Введение в теорию кодирования
5	Классификация кодов. Рассматриваемые вопросы: - Классификация кодов. - Одноимпульсные и многоимпульсные коды. - Равномерные и неравномерные коды. - Кодовое дерево. - Единичный унитарный код. - Сменно-качественные коды. - Корреляционный код.
6	Минимальное кодовое расстояние, полное и неполное декодирование. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Минимальное кодовое расстояние, полное и неполное декодирование. - Примеры линейных кодов. - Код с проверкой на четность. - Код с повторением. - Код с повторением и инверсией (код Бауэра). - Итеративный код. - Геометрическая модель кода. - Связь dmin со способностью кода обнаруживать и исправлять ошибки.
7	Коды Хэмминга с dmin=3, dmin=4. Рассматриваемые вопросы: - Коды Хэмминга с dmin=3. - Коды Хэмминга с dmin=4.
8	Математическое введение в теорию кодирования Рассматриваемые вопросы: - Математическое введение в теорию кодирования
9	Группы. Рассматриваемые вопросы: - Группы. - Примеры конечных и бесконечных групп. - Циклическая группа. - Разложение групп по подгруппе на смежные классы. - Группа смежных классов. - Кольцо и его аксиоматика.
10	Примеры конечных и бесконечных колец Рассматриваемые вопросы: - Примеры конечных и бесконечных колец. - Идеал. - Разложение кольца по идеалу на классы вычетов. - Кольца классов вычетов. - Поле, его аксиоматика. - Примеры бесконечных и конечных полей. - Поле Галуа (GF(p)).
11	Векторное пространство, его аксиоматика. Рассматриваемые вопросы: - Векторное пространство, его аксиоматика. - Базис векторного пространства. - Нулевое пространство, его базис. - Линейная ассоциативная алгебра, ее аксиоматика. - Алгебра последовательностей длины n.
12	Линейные коды Рассматриваемые вопросы: - Линейные коды. - Способы задания линейных кодов. - Стандартная расстановка. - Укороченные линейные коды. - Декодирование по синдрому.
13	Мажоритарное декодирование Рассматриваемые вопросы: - Мажоритарное декодирование. - Нумераторы весов.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Расчет показателей достоверности (вероятности трансформации, вероятности подавления, вероятности правильного приема).
14	Математическое введение к циклическим кодам Рассматриваемые вопросы: - Математическое введение к циклическим кодам
15	Группа многочленов. Рассматриваемые вопросы: - Группа многочленов. - Кольцо многочленов. - Разложение кольца многочленов по идеалу на классы вычетов. - Кольцо классов вычетов. - Векторное пространство и алгебра классов вычетов. - Идеал в алгебре классов вычетов.
16	Базис векторного пространства классов вычетов. Рассматриваемые вопросы: - Базис векторного пространства классов вычетов. - Базис нулевого пространства. - Расширение поля GF(pm). - Корни многочленов из расширения поля. - Минимальная функция.
17	Циклические коды Рассматриваемые вопросы: - Циклические коды, их определение. - Несистематические и систематические циклические коды. - Способ задания. - Способы декодирования. - Линейные переключательные схемы. - Кодеры и декодеры. - БЧХ-коды. - Коды Файера.
18	Непрерывные коды Рассматриваемые вопросы: - Определение, характеристики непрерывных кодов. - Сверточные коды.
19	Статистическая теория связи Рассматриваемые вопросы: - Роль информации в современных системах управления. - Семантический и статистический подходы в описании информационных процессов. - Теория информации краткий исторический очерк развития. - Алфавит источника сообщения.
20	Ансамбль источника сообщения. Рассматриваемые вопросы: - Ансамбль источника сообщения. - Собственная информация, ее свойства, единицы измерения. - Энтропия источника дискретных сообщений, ее свойства. - Максимум энтропии. - Количество информации по Хартли.
21	Энтропия двух источников сообщений. Рассматриваемые вопросы: - Энтропия двух источников сообщений.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Формула определения энтропии двух источников сообщений. - Условная энтропия, ее свойства. - Взаимная информация, ее свойства. - Средняя взаимная информация, ее свойства.
22	Источники дискретных сообщений. Рассматриваемые вопросы: - Производительность источников дискретных сообщений. - Избыточность источников дискретных сообщений. - Производительность марковского источника сообщений. - Избыточность линейных кодов. - Код Фано-Шеннона. - Метод Хаффмена. - Понятие блочного статистического кодирования. - Основная теорема кодирования.
23	Каналы связи. Рассматриваемые вопросы: - Каналы связи. - Скорость передачи. - Пропускная способность каналов связи. - Скорость передачи и пропускная способность каналов без помех, симметричного бинарного канала без стирания, симметричного бинарного канала связи со стиранием.
24	Понятия энтропии на источники непрерывных сообщений. Рассматриваемые вопросы: - Распространение понятия энтропии на источники непрерывных сообщений. - Дифференциальная энтропия, ее свойства. - Решение вариационной задачи для определения максимума дифференциальной энтропии в двух случаях: при заданном диапазоне изменения передаваемой случайной величины, при заданной мощности источника сообщений. - Пропускная способность Гауссовского канала. - 1-я и 2-я теоремы Шеннона.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ №1 В результате выполнения практического задания студент рассматривает расчет вероятности ошибки на символ при гауссовской помехе и методе приема с однократным отчетом, с интегрированием, расчет оценок вероятности правильного приема, трансформации и отказа от декодирования для симметричного бинарного канала
2	ПЗ №2 В результате работы на практическом занятии, студент получает навык анализа помехоустойчивости кодов по законам перестановок, сменно-качественных кодов, корреляционного кода
3	ПЗ №3 В результате работы на практическом занятии студент отрабатывает умения по построению порождающих и проверочных матриц для кода с проверкой на четкость кодов Бауэра, кода с n-кратным повторением получает навык анализа связи минимального кодового расстояния с корректирующей способностью кодов.

№ п/п	Тематика практических занятий/краткое содержание
4	ПЗ №4 В результате работы на практическом занятии студент отрабатывает умения по построению порождающих и проверочных матриц кодов Хэмминга.
5	ПЗ №5 В результате выполнения практического задания студент рассматривает примеры бесконечных колец, примеры главных идеалов, разложение кольца по идеалу на классы вычетов, операции над классами вычетов, кольцо классов вычетов.
6	ПЗ №6 В результате выполнения практического задания студент рассматривает базис векторного пространства над полем GF(2) всех последовательностей длины n, примеры базиса векторного подпространства векторного пространства всех последовательностей длины n, ортогональность векторов, примеры нулевых пространств.
7	ПЗ №7 В результате работы на практическом занятии студент отрабатывает умения по построению стандартной расстановки для линейных кодов, примеры укорочения линейных кодов.
8	ПЗ №8 В результате работы на практическом занятии студент получает навык по расчету показателей достоверности приема линейных поездов.
9	ПЗ №9 В результате выполнения практического задания студент рассматривают примеры сложения и умножения многочленов с коэффициентами из поля GF(2), определение образующего класса вычетов заданного многочлена при разложении кольца многочленов по идеалу, все элементы которого кратны f(x) = xn+1, решение задач для определения неприводимости многочлена, проверка ортогональности многочленов в кольце классов вычетов.
10	ПЗ №10 В результате выполнения практического задания студент рассматривает базис векторного пространства классов вычетов, расширение поля GF (pm), корни многочлена из расширения поля, решение задач для определения неприводимости многочлена, проверка ортогональности многочленов в кольце классов вычетов.
11	ПЗ №11 В результате выполнения практического задания студент учится построению порождающих матриц несистематических и систематических цикличных кодов, алгоритм задания систематического циклического кода, примеры линейных переключательных схем: умножение, деление, одновременного умножения и деления.
12	ПЗ № 12 В результате выполнения практического задания студент учится построению кодеров и декодеров цикличных кодов, рассматривает примеры построения БЧХ кодов, рассматривает примеры построения кода Файера.
13	ПЗ №13 В результате выполнения практического задания студент учится построению кодов Хакельбергера.
14	ПЗ № 14 В результате выполнения практического задания студент учится построению сверточных кодов.
15	ПЗ №15 В результате выполнения практического задания студент учится примеры определения собственной информации, примеры расчета энтропии.
16	ПЗ № 16 В результате выполнения практического задания студент учится примеры определения взаимной информации, примеры определения средней взаимной информации, примеры расчета условной энтропии, анализ энтропии двух ансамблей.

№ п/п	Тематика практических занятий/краткое содержание
17	ПЗ № 17 В результате работы на практическом занятии студент отрабатывает умения по построению кодов Фано-Шеннона, использованию метода Хаффмена.
18	ПЗ №18 В результате работы на практическом занятии студент отрабатывает умения по расчету дифференциальной энтропии, расчету пропускной способности гауссовского канала.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.
6	Выполнение курсовой работы.
7	Подготовка к промежуточной аттестации.
8	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Курсовая работа имеет целью развитие у обучающихся навыков самостоятельной творческой работы, овладение методами современных научных исследований, углублённое изучение какого-либо вопроса, темы, раздела учебной дисциплины (включая изучение литературы и источников) и носит исследовательский характер. Целью курсовой работы является расчет оценок показателей достоверности приема дискретной информации. Проектирование кодера и декодера БЧХ-кода. Задание на курсовую работу и варианты исходных данных (56 вариант).

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Статистическая теория радиотехнических систем Г.И. Худяков М.: «Академия» , 2009	
2	Кодирование при передаче и хранении информации (Алгебраическая теория блоковых кодов) В. Д. Колесник М: Высшая школа , 2009	
3	Введение в дискретную теорию информации и	

	кодирования С. И. Чечета М.: МЦНМО , 2011	
1	Передача информации. Статистическая теория связи Р. Фано; Пер.: И.А. Овсеевич, М.С. Пинскер; Под ред. Р.Л. Добрушина Однотомное издание Мир , 1965	НТБ (фб.)
2	Коды, исправляющие ошибки У. Питерсон Однотомное издание Мир , 1964	НТБ (фб.)
3	Коды, исправляющие ошибки У. Питерсон, Э. Уэлдон; Под ред. Р.Л. Добрушина, С.И. Самойленко Однотомное издание Мир , 1976	НТБ (фб.)
4	Расчет оценок показателей достоверности приема дискретной информации при заданной модели помехи в канале связи. Проектирование кодера и декодера БЧХ-кода Л.А. Баранов; МИИТ. Каф. "Управление и информатика в технических системах" Однотомное издание МИИТ , 2008	НТБ (фб.); НТБ (чз.2)

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Пакет прикладных программ не ниже MathCad 14

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Курсовая работа в 4 семестре.
Экзамен в 4 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

заведующий кафедрой, профессор,
д.н. кафедры «Управление и защита
информации» Л.А. Баранов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин