

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

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2025

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:

- Правовые и этические нормы, регулирующие отношения в информационной сфере (основы законодательства РФ в области информации, ИТ и защиты данных).

- Фундаментальные разделы математики (математический анализ, линейная алгебра, теория вероятностей, математическая статистика, дискретная математика), необходимые для формализации профессиональных задач.

Уметь:

- Ориентироваться в современном информационном пространстве, критически оценивать достоверность и полноту информации.

- Анализировать полученные результаты, оценивать их достоверность и практическую значимость, корректировать математическую модель при необходимости.

Владеть:

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

- Навыками математического моделирования процессов и явлений в профессиональной сфере.

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	Семестр №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.

№ п/п	Тематика лекционных занятий / краткое содержание
6	<p>Минимальное кодовое расстояние, полное и неполное декодирование.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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 d_{\min} со способностью кода обнаруживать и исправлять ошибки.
7	<p>Коды Хэмминга с $d_{\min}=3$, $d_{\min}=4$.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Коды Хэмминга с $d_{\min}=3$. - Коды Хэмминга с $d_{\min}=4$.
8	<p>Математическое введение в теорию кодирования</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Математическое введение в теорию кодирования
9	<p>Группы.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Группы. - Примеры конечных и бесконечных групп. - Циклическая группа. - Разложение групп по подгруппе на смежные классы. - Группа смежных классов. - Кольцо и его аксиоматика.
10	<p>Примеры конечных и бесконечных колец</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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	<p>Векторное пространство, его аксиоматика.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Векторное пространство, его аксиоматика. - Базис векторного пространства. - Нулевое пространство, его базис. - Линейная ассоциативная алгебра, ее аксиоматика. - Алгебра последовательностей длины n.
12	<p>Линейные коды</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Линейные коды. - Способы задания линейных кодов. - Стандартная расстановка. - Укороченные линейные коды. - Декодирование по синдрому.
13	<p>Мажоритарное декодирование</p> <p>Рассматриваемые вопросы:</p>

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> - Мажоритарное декодирование. - Нумераторы весов. - Расчет показателей достоверности (вероятности трансформации, вероятности подавления, вероятности правильного приема).
14	<p>Математическое введение к циклическим кодам</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Математическое введение к циклическим кодам
15	<p>Группа многочленов.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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	<p>Базис векторного пространства классов вычетов.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Базис векторного пространства классов вычетов. - Базис нулевого пространства. - Расширение поля $GF(pm)$. - Корни многочленов из расширения поля. - Минимальная функция.
17	<p>Циклические коды</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Циклические коды, их определение. - Несистематические и систематические циклические коды. - Способ задания. - Способы декодирования. - Линейные переключательные схемы. - Кодеры и декодеры. - БЧХ-коды. - Коды Файера.
18	<p>Непрерывные коды</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Определение, характеристики непрерывных кодов. - Сверточные коды.
19	<p>Статистическая теория связи</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Роль информации в современных системах управления. - Семантический и статистический подходы в описании информационных процессов. - Теория информации краткий исторический очерк развития. - Алфавит источника сообщения.
20	<p>Ансамбль источника сообщения.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Ансамбль источника сообщения. - Собственная информация, ее свойства, единицы измерения. - Энтропия источника дискретных сообщений, ее свойства. - Максимум энтропии. - Количество информации по Хартли.

№ п/п	Тематика лекционных занятий / краткое содержание
21	<p>Энтропия двух источников сообщений.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Энтропия двух источников сообщений. - Формула определения энтропии двух источников сообщений. - Условная энтропия, ее свойства. - Взаимная информация, ее свойства. - Средняя взаимная информация, ее свойства.
22	<p>Источники дискретных сообщений.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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	<p>Каналы связи.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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	<p>Понятия энтропии на источники непрерывных сообщений.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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	<p>Расчет помехоустойчивости при гауссовском канале и анализ бинарного симметричного канала.</p> <p>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</p>
2	<p>Анализ помехоустойчивости кодов (перестановочные, сменно-качественные, корреляционные).</p> <p>В результате работы на практическом занятии, студент получает навык анализа</p>

№ п/п	Тематика практических занятий/краткое содержание
	помехоустойчивости кодов по законам перестановок, сменно-качественных кодов, корреляционного кода
3	<p>Построение матриц и анализ корректирующей способности кодов с проверкой на четность, кодов Бауэра и кодов с повторением.</p> <p>В результате работы на практическом занятии студент отрабатывает умения по построению порождающих и проверочных матриц для кода с проверкой на четность кодов Бауэра, кода с n-кратным повторением получает навык анализа связи минимального кодового расстояния с корректирующей способностью кодов.</p>
4	<p>Построение порождающих и проверочных матриц кодов Хэмминга.</p> <p>В результате работы на практическом занятии студент отрабатывает умения по построению порождающих и проверочных матриц кодов Хэмминга.</p>
5	<p>Исследование алгебраических структур: кольца, идеалы и классы вычетов.</p> <p>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.</p>
6	<p>Векторные пространства над полем $GF(2)$: базис, подпространства и ортогональность.</p> <p>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.</p>
7	<p>Методы стандартной расстановки и укорочения линейных кодов.</p> <p>В результате работы на практическом занятии студент отрабатывает умения по построению стандартной расстановки для линейных кодов, примеры укорочения линейных кодов.</p>
8	<p>Расчет показателей достоверности приема в линейных трактах (кодах).</p> <p>В результате работы на практическом занятии студент получает навык по расчету показателей достоверности приема линейных поездов.</p>
9	<p>Арифметика многочленов над полем $GF(2)$ и факторкольца.</p> <p>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 $f(x) = x^n + 1$, решение задач для определения неприводимости многочлена, проверка ортогональности многочленов в кольце классов вычетов.</p>
10	<p>Расширение полей Галуа и свойства многочленов (неприводимость, ортогональность).</p> <p>В результате выполнения практического задания студент рассматривает базис векторного пространства классов вычетов, расширение поля $GF(p^m)$, корни многочлена из расширения поля, решение задач для определения неприводимости многочлена, проверка ортогональности многочленов в кольце классов вычетов.</p>
11	<p>Построение циклических кодов: матрицы и реализация на переключаемых схемах.</p> <p>В результате выполнения практического задания студент учится построению порождающих матриц несистематических и систематических циклических кодов, алгоритм задания систематического циклического кода, примеры линейных переключаемых схем: умножение, деление, одновременного умножения и деления.</p>
12	<p>Проектирование кодеров и декодеров циклических кодов (БЧХ, коды Файера).</p> <p>В результате выполнения практического задания студент учится построению кодеров и декодеров циклических кодов, рассматривает примеры построения БЧХ кодов, рассматривает примеры построения кода Файера.</p>

№ п/п	Тематика практических занятий/краткое содержание
13	Построение и анализ кодов Хакельбергера. В результате выполнения практического задания студент учится построению кодов Хакельбергера.
14	Принципы построения сверточных кодов. В результате выполнения практического задания студент учится построению сверточных кодов.
15	Расчет энтропии и собственной информации дискретных источников. В результате выполнения практического задания студент учится примеры определения собственной информации, примеры расчета энтропии; примеры определения взаимной информации, примеры определения средней взаимной информации, примеры расчета условной энтропии, анализ энтропии двух ансамблей.
16	Исследование информационных характеристик: взаимная информация, условная энтропия, дифференциальная энтропия, пропускная способность канала, эффективное кодирование (Фано, Хаффмен). В результате работы на практическом занятии студент отрабатывает умения по построению кодов Фано-Шеннона, использованию метода Хаффмена; 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.

4.4. Примерный перечень тем курсовых работ

Задание на курсовую работу и варианты исходных данных:

Варианта № ? $P_{тр}^3$ n Способ передачи Способ приёма

1 5 $10^{(-11)}$ 511 СП2 Пр2

2 8 $10^{(-12)}$ 511 СП2 Пр2

3 10 $10^{(-8)}$ 3,1 СП2 Пр1

4 15 $10^{(-9)}$ 31 СП2 Пр1

5 20 $10^{(-10)}$ 31 СП2 Пр1

6 25 $10^{(-11)}$ 31 СП1 Пр1

7 30 $10^{(-12)}$ 31 СП1 Пр1

8 15 $10^{(-8)}$ 63 СП2 Пр1

9 20 $10^{(-9)}$ 63 СП2 Пр1

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

№ п/п	Библиографическое описание	Место доступа
1	Основы теории информации и кодирования Березкин Е.Ф. Учебное пособие 5-е изд., стер. - Санкт-Петербург: Лань. - 320 с. - ISBN 978-5--507-50792-4 , 2025	https://reader.lanbook.com/book/465089#2
2	Основы теории информации Бубнов С.А., Овечкин Г.В., Филатов И.Ю. Учебное пособие Изд. Рязань. - 208 с. - ISBN 978-5-7722-0393-4 , 2023	https://reader.lanbook.com/book/439679#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