МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Баранов Леонид Аврамович, д.т.н., профессор

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Теория информации и кодирования»

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой  Л.А. Баранов

Москва 2020 г.

1. Цели освоения учебной дисциплины

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. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Теория информации и кодирования" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-1	Способен представлять 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 существующих математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач защиты информации

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Теория информации и кодирования» осуществляется в форме лекций и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративные).Практические занятия организованы с использованием технологий развивающего обучения. Весь практический курс выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач), а также с использованием современной вычислительной техники, в объёме 36 часов на

практические занятия. Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. Самостоятельное решение задач в виде 3х индивидуальных заданий, охватывающих 2-5 и 8 разделы курса. Выполнение курсовой работы, охватывающей 1, 2, 4-6 разделы курса. К интерактивным (диалоговым) технологиям относиться отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 8 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях..

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
Общие вопросы передачи информации

Тема: 1.1.
Общая структурная схема передачи информации. Линия связи. Канал связи. Сообщение. Сигнал. Помеха. Классификация помех. Модели помех. Способы приема.

Тема: 1.2.
Расчет вероятности ошибки на символ

РАЗДЕЛ 2
Введение в теорию кодирования

Тема: 2.1.
Классификация кодов. Одноимпульсные и многоимпульсные коды. Равномерные и неравномерные коды. Кодовое дерево. Единичный унитарный код. Сменно-качественные коды. Корреляционный код.

Тема: 2.2.
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.

Тема: 2.3.
Коды Хэмминга с dmin=3. Коды Хэмминга с dmin=4.

РАЗДЕЛ 3
Математическое введение в теорию кодирования

Тема: 3.1.
Группы. Примеры конечных и бесконечных групп. Циклическая группа. Разложение групп по подгруппе на смежные классы. Группа смежных классов. Кольцо и его аксиоматика.

Тема: 3.2.
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)).

Тема: 3.3.
Векторное пространство, его аксиоматика. Базис векторного пространства. Нулевое пространство, его базис. Линейная ассоциативная алгебра, ее аксиоматика. Алгебра последовательностей длины n.

Тема: 3.3.
Опросы, индивидуальные задания, тестирование

РАЗДЕЛ 4
Линейные коды

Тема: 4.1.
Линейные коды. Способы задания линейных кодов. Стандартная расстановка. Укороченные линейные коды. Декодирование по синдрому.

Тема: 4.2
Мажоритарное декодирование. Нумераторы весов. Расчет показателей достоверности (вероятности трансформации, вероятности подавления, вероятности правильного приема).

РАЗДЕЛ 5
Математическое введение к циклическим кодам

Тема: 5.1.
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.

Тема: 5.2.
Базис векторного пространства классов вычетов. Базис нулевого пространства. Расширение поля GF(pm). Корни многочленов из расширения поля. Минимальная функция.

РАЗДЕЛ 6
Циклические коды

Тема: 6.1.
Циклические коды, их определение. Несистематические и систематические циклические коды. Способ задания. Способы декодирования. Линейные переключательные схемы. Кодеры и декодеры. БЧХ-коды. Коды Файера.

Тема: 6.1.
Опросы, индивидуальные задания, тестирование, % выполнения курсовой работы

РАЗДЕЛ 7
Непрерывные коды

Тема: 7.1.
Определение, характеристики непрерывных кодов. Сверточные коды.

РАЗДЕЛ 8
Статистическая теория связи

Тема: 8.1.
Роль информации в современных системах управления. Семантический и статистический подходы в описании информационных процессов. Теория информации краткий исторический очерк развития. Алфавит источника сообщения. Ансамбль источника сообщения. Собственная информация, ее свойства, единицы измерения. Энтропия источника дискретных сообщений, ее свойства. Максимум энтропии. Количество информации по Хартли.

Тема: 8.2.
Энтропия двух источников сообщений. Формула определения энтропии двух источников сообщений. Условная энтропия, ее свойства. Взаимная информация, ее свойства. Средняя взаимная информация, ее свойства.

Тема: 8.3.
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.

Тема: 8.4.
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.

Тема: 8.5.
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.

РАЗДЕЛ 9
Курсовая работа
Используются разделы: 1, 4, 6.

РАЗДЕЛ 9
Курсовая работа
Проверка и защита курсовой работы.

Экзамен