МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Вычислительные системы, сети и информационная безопасность»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Теория информации»

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2017

1. Цели освоения учебной дисциплины

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности).
Эксплуатационная:
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;
Проектно-технологическая:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов
Экспериментально-исследовательская деятельность:
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств
Организационно-управленческая деятельность:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.
Организационно-управленческая деятельность

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Теория информации" 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-2	способностью применять соответствующий математический аппарат для решения профессиональных задач

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Теория информации» осуществляется в форме лекций и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 14 часов, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).Практические занятия проводятся на основе выполнения примеров по темам лекционного материала Самостоятельная работа студента организована с использованием традиционных видов работы,т,е. отработка лекционного материала и отработка отдельных тем по предложенной литературе.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на разделы, представляющие собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы. Проведении занятий по дисциплине (модулю) возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости):- использование современных средств коммуникации;- электронная форма обмена материалами;- дистанционная форма групповых и индивидуальных консультаций;- использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д..

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

РАЗДЕЛ 1
Введение в теорию информации
Основные понятия теории информации. Понятие информации и информационных технологий. Измерение информации и этапы обращения информации.

РАЗДЕЛ 2
Системы передачи информации
Структура системы передачи информации.Источник и приемник сообщения. Кодер и декодер ,согласованный со свойствами источника сообщений. Модели канала связи. Основные модели канала связи. Декодирование по принципу максимального правдоподобия.

РАЗДЕЛ 3
Мера количества информации
Выбор меры количества информации. Количество информации и энтропия ансамбля случайных сообщений. Свойства меры количества информации. Связь числа сообщений с количеством информации. Количество информации в равновероятных сообщениях. Логарифмическая мера количества информации. Мера количества информации по Хартли. Связь количества информации с вероятностью сообщений. Единицы измерения количества информации.Количество информации и энтропия ансамбля случайных

сообщений.Алфавит источника сообщений. Полная группа сообщений. Частная собственная информация одного сообщения. Количество информации – случайная величина. Законы распределения количества информации. Числовые характеристики количества информации.Свойства энтропии дискретного ансамбля. Энтропия обединенного ансамбля. Теорема сложения энтропий. Условная энтропия. Свойства условной энтропии.

РАЗДЕЛ 3
Мера количества информации
Выполнение 20% лаб.работ

РАЗДЕЛ 4
Кодирование дискретных сообщений
Эффективное кодирование. Примеры оптимального кодирования сообщений. Теоремы кодирования. Понятие кодирования сообщений. Код, кодовые комбинации, алфавит кода. Эффективность кода. Нижняя граница средней длины кодовых комбинаций. Однозначность декодирования. Максимальное количество информации, содержащееся в среднем в символах кода в каждой кодовой комбинации. Правило эффективного конструирования кодовых слов.
Примеры оптимального кодирования сообщений. Теоремы кодирования. Код Фано-Шеннона. Алгоритм кодирования. Примеры построения кодов для ансамблей с равновероятными сообщениями и сообщениями с вероятностями равными целым степеням двойки. Кодовое дерево. Код Хаффмана. Алгоритм кодирования двоичного кода Хаффмана и примеры кодирования. Основная теорема кодирования. Нижняя и верхняя границы энтропии эффективного кода. Кодирование последовательности статистически независимых сообщений. Блочное кодирование.

РАЗДЕЛ 5
Источники дискретных сообщений. Энтропия источников дискретных сообщений. Дискретные и непрерывные источники сообщений. Ансамбль символов сообщений источника. Последовательность сообщений источника. Условная вероятность появления символа в последовательности сообщений.Классификация источников сообщений.Энтропия источников дискретных сообщений. Классификация источников сообщений. Источник без памяти. Источник с памятью. Стационарный источник. Эргодический источник. Марковский источник. Способы определения энтропия стационарного дискретного источника, приходящаяся на одно сообщение. Теорема о средней энтропии стационарного источника.

РАЗДЕЛ 6
Взаимная информация
Определение и свойства взаимной информации. Свойства взаимной информации. Частная информация об ансамбле и о сообщении, содержащаяся в сообщении другого ансамбля. Примеры расчета энтропии и взаимной информации.

РАЗДЕЛ 7
Кодирование и декодирование в канале

Тема: Характеристики дискретных каналов. Помехоустойчивое кодирование.
Скорость передачи и пропускная способность дискретного канала. Симметричный бинарный канал без памяти и со стиранием. Дискретный канал без памяти и помех. Симметричный бинарный канал с помехами и без памяти. Симметричный бинарный канал без памяти и со стиранием. Дискретные каналы с памятью.Понятие о помехоустойчивом кодировании. Блочные коды. Непрерывные коды. Безызбыточные и избыточные коды. Коды с обнаружением ошибок. Коды с исправлением ошибок. Коды с обнаружением и

исправлением ошибок. Теорема Шеннона о помехоустойчивы кодировании. Код с проверкой на четность.Характеристики избыточных кодов и их декодирование. Равномерные коды. Вес кодовой комбинации. Кодовое расстояние. Минимальное кодовое расстояние. Геометрическая интерпретация равномерного двоичного кода. Кодовый вектор. Вектор ошибки. Декодирование по принципу максимального правдоподобия. Связь корректирующей способности кода с минимальным кодовым расстоянием при обнаружении и исправлении ошибок.

Тема: Характеристики дискретных каналов. Помехоустойчивое кодирование.
выполнение 80% лаб.работ

Тема: Алгебраическое введение в теорию линейных кодов. Линейные блоковые коды. Методы декодирования линейных кодов.
Векторное пространство последовательностей элементов поля GF(2). Алгебраические системы последовательностей элементов поля и их свойства.Операция сложения последовательностей, умножения последователь-ности на скаляр. Базис векторного пространства. Размерность векторного пространства. Порождающая матрица векторного подпространства. Ортогональность векторов. Линейные блоковые коды. Порождающая матрица и проверочная матрицы. Синдром ошибки. Линейный -код. Минимальное кодовое расстояние линейного -кода. Систематический и несистематический линейные коды, получение их порождающих и проверочных матриц.Методы декодирования линейных кодов. Обнаружение ошибок по синдрому. Исправление одиночной ошибки. Коды с повторением. Число разрядов избыточного кода, необходимых для исправления одиночной ошибки. Мажоритарное декодирование. Код Хэмминга. Получение порождающей и проверочной матриц систематического и несистематического кодов Хэмминга. Обнаружение и исправление ошибок.

Тема: Циклический код
Понятие об алгебре многочленов. Операции над многочленами с элементами из поля GF(2). Линейная ассоциативная алгебра многочленов. Систематический и несистематический циклические коды. Применение циклического кода в информационных сетях.

Дифференцированный зачет