

## Аннотация дисциплины С.1.1.35 Дисциплина. Теория информации

Дисциплина "Теория информации" изучается обучающимися по основной профессиональной образовательной программе "Безопасность автоматизированных систем критически важных объектов" направления подготовки "10.05.03 Информационная безопасность автоматизированных систем".

Дисциплина изучается в 7 семестре. Общая трудоемкость дисциплины составляет 180/5 часов/з.ед. Самостоятельная работа заключается в выполнении работ, указанных в разделе 4.

В ходе изучения дисциплины осуществляется текущий контроль в форме технологии рейтингового контроля в соответствии с технологической карты дисциплины, размещенной на электронном курсе, а также промежуточный контроль в форме экзамен.

Целью изучения дисциплины является формирование следующих компетенций:

1. ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
2. ОПК-8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах

В ходе изучения дисциплины последовательно рассматриваются темы:

1. Введение. Основные понятия. Системы связи и теория информации. Обобщенные модели систем передачи и хранения информации. Идея определения количества информации.
2. Математическая модель источника информации.  
Дискретные и непрерывные источники. Количество информации в сообщении. Энтропия дискретного источника. Кодирование источника. Префиксные коды. Неравенство Крафта. Средняя длина кодового слова.
3. Код Шеннона-Фано. Код Хаффмана.  
Теорема кодирования источника (неравномерные коды).  
Равномерное кодирование источника. Словарные коды.  
Алгоритм Лемпеля-Зива.
4. Математическое описание канала связи. Дискретный канал без памяти. Взаимная информация, остаточная энтропия, пропускная способность канала.
5. Ошибка декодирования. Неравенство Фано. Теоремы кодирования для канала.  
Расчет пропускной способности некоторых каналов: дискретный канал без памяти; двоичный симметричный канал (ДСК).
6. Непрерывные источники. Взаимная информация и относительная (дифференциальная) энтропия.  
Пропускная способность непрерывного гауссовского канала.
7. Общая идея канального кодирования. Классификация кодов. Евклидово и хэммингово расстояние.  
Декодирование по максимуму правдоподобия и минимуму расстояния.  
Исправляющая способность кода.
8. Ключевые параметры блочных кодов. Важнейшие границы теории кодирования. Энергетический выигрыш от кодирования. Мягкое и жесткое декодирование.
9. Введение в конечные поля. Векторные пространства над конечными полями.
10. Линейные коды и их порождающие матрицы.  
Проверочная матрица и ее связь с кодовым расстоянием.  
Коды Хэмминга. Расширенные и укороченные коды.
11. Коды симплексные, ортогональные и Рида-Маллера.

- Синдромное декодирование линейных кодов.
12. Циклические коды.  
Кодовые полиномы.  
Полиномиальная арифметика.
  13. Порождающий и проверочный полиномы циклического кода. Систематический циклический код. Порождающая и проверочная матрица циклического кода. Синдромное декодирование циклических кодов.
  14. Коды БЧХ и Рида-Соломона.
  15. Расширенные конечные поля. Мультипликативный порядок элементов поля. Примитивные элементы.  
Построение полиномов с заданными корнями.
  16. Введение в сверточные коды. Диаграмма состояний и решетчатая диаграмма сверточного кода.
  17. Свободное расстояние.  
Передающая функция сверточного кода. Алгоритм декодирования Витерби.
  18. Мягкое декодирование сверточных кодов. Выколотые (перфорированные) сверточные коды. Турбо коды.

Основными стратегическими образовательными технологиями являются: лекционные занятия, практические и лабораторные занятия.

В рамках указанных технологий применяются тактические образовательные технологии: задания, классическая лекция.