БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Председатель Учебно-методического
объединения вузов Республики Беларусь
по естественнонаучному образованию
_____ В.В. Самохвал

«____»_____ 2006 г.

Регистрационный № ТД -_____/тип.

ТЕОРИЯ ИНФОРМАЦИИ

Учебная программа
для Белорусского государственного университета по специальности

1- 98 01 01- 01 Компьютерная безопасность

Минск
2006

Составители:
Е.Е. Жук – профессор кафедры математического моделирования и анализа данных, доктор физ.-мат. наук

Рецензенты:

Кафедра информационных технологий автоматизированных систем Белорусского государственного университета информатики и радиоэлектроники;
А.Д. Егоров – главный научный сотрудник отдела нелинейного и стохастического анализа Института Математики НАН Беларуси, доктор физ.-мат. наук, профессор

Рекомендована к утверждению в качестве базовой для БГУ:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета
(протокол №15 от «04» апреля 2006 г.).

Научно-методической комиссией факультета прикладной математики и информатики Белорусского государственного университета
(протокол №___ от «____»_____2006г.).

Ученым Советом факультета прикладной математики и информатики
(протокол №5 от «25» апреля 2006 г.).

Научно-методическим Советом Белорусского государственного университета
(протокол №___ от «____»_____2006г.).

Согласована
Научно-методическим Советом по компьютерной безопасности УМО вузов Республики Беларусь по естественнонаучному образованию
(протокол №___ от «____»_____2006г.).

Ответственный за редакцию: Е.Е. Жук

Ответственный за выпуск: О.А. Кастрица

Пояснительная записка

Целью данного курса является изучение основ теории информации и ее применение в криптологии. Этот курс предлагается как общий курс для студентов специальности «Компьютерная безопасность» и других родственных специальностей.

В соответствии со стандартом специальности учебная программа предусматривает для изучения дисциплины 68 аудиторных часов, в том числе лекционных – 34 ч., практических – 14 ч., лабораторных – 16 ч. и 4 ч. контролируемой самостоятельной работы.

Содержание

Введение

Предмет курса. Прикладные задачи.

Энтропия и ее свойства

Источники дискретных сообщений и их вероятностные модели. Функционал энтропии. Свойства энтропии. Условная энтропия и ее свойства. Теорема о поведении функционала энтропии при дискретных функциональных преобразованиях. Примеры.

Асимптотические свойства стационарного источника дискретных сообщений без памяти

Теоремы о высоковероятном подмножестве реализаций бернуллиевской случайной последовательности. Теорема Стратоновича. Достаточные условия энтропийной устойчивости.

Обобщение понятия энтропии

Источники непрерывных сообщений. Свойства дифференциальной энтропии. Максимизация энтропии на различных классах вероятностных распределений.

Энтропия случайных процессов

Энтропия марковской цепи. Энтропия стационарного временного ряда: гауссовский случай. Энтропия гауссовского процесса с непрерывным временем; энтропийная мощность.

Функционал количества информации и его свойства

Различные определения количества информации. Свойства функционала Шэнновской информации. Примеры.

Литература

Основная

1. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. – Мн.: БГУ, 1999.
2. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. . – М.: Наука, 1982.
3. Стратонович Р.Л. Теория информации. – М.: Наука, 1975.
4. Кульбак С. Теория информации и статистика. – М.: Наука, 1963.

Дополнительная

5. Шэннон К. Работы по теории информации. – М.: ИЛ, 1963.
6. Орлов В.А., Филлипов Л.И. Теория информации в упражнениях и задачах. – М.: ВШ, 1976.