

Министерство образования Республики Беларусь

Учебно-методическое объединение высших учебных заведений
Республики Беларусь по естественнонаучному образованию

УТВЕРЖДАЮ

Первый заместитель
Министра образования
Республики Беларусь


А.И. Жук

16.06.2010

(дата утверждения)

Регистрационный №ТД- Р. 216/тип.

ТЕОРИЯ ИНФОРМАЦИИ

Типовая учебная программа

для высших учебных заведений по специальности

**1-98 01 01-01 Компьютерная безопасность (математические
методы и программные системы)**

СОГЛАСОВАНО

Председатель Учебно-
методического объединения вузов
Республики Беларусь по естест-
веннонаучному образованию


В.В. Самохвал



СОГЛАСОВАНО

Начальник Управления высшего и
среднего специального образования


Ю.И. Миксюк

16.06.2010

(дата)

Проректор по учебной и
воспитательной работе
Государственного учреждения
образования «Республиканский
институт высшей школы»


В.И. Шупляк

16.06.2010

(дата)

Эксперт-нормоконтролер


Ф.М. Кувшинов

18.05.2010

(дата)

Минск 2009

СОСТАВИТЕЛИ:

А.С. Гурин, доцент кафедры математического моделирования и анализа данных Белорусского государственного университета, кандидат физико-математических наук
Ю.С. Харин, заведующий кафедрой математического моделирования и анализа данных, член-корреспондент Национальной академии наук Беларуси, доктор физико-математических наук, профессор

РЕЦЕНЗЕНТЫ:

Кафедра информационных технологий автоматизированных систем Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

В.И. Берник, заведующий отделом теории чисел Института математики Национальной академии наук Беларуси, доктор физико-математических наук, профессор

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета
(протокол № 02 от 02.09.2008 г.)

Научно-методическим советом Белорусского государственного университета
(протокол № 01 от 01.12.2008 г.)

Научно-методическим советом по специальности 1-98 01 01 Компьютерная безопасность Учебно-методического объединения вузов Республики Беларусь по естественнонаучному образованию
(протокол № 01 от 11.03.2009 г.)

Ответственный за выпуск: Гурин А.С.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дисциплина «Теория информации» является общим курсом, читаемым студентам специальности «Компьютерная безопасность». Он основывается на знаниях, полученных при изучении общих курсов «Теория вероятностей и математическая статистика», «Математический анализ».

Целью курса является изучение математических моделей, методов, алгоритмов и программного обеспечения теории информации.

Задачами дисциплины являются:

1. Определение и установление свойств энтропии источника дискретных сообщений.
2. Определение удельной энтропии символьной последовательности и установление свойств удельной энтропии стационарной символьной последовательности, порождаемой источником дискретных сообщений.
3. Определение и установление свойств энтропии источника непрерывных сообщений.
4. Установление свойств удельной энтропии стационарной гауссовской символьной последовательности.
5. Оптимизация энтропии на классе вероятностных распределений.
6. Установление свойства энтропийной устойчивости символьных последовательностей.
7. Определение и установление свойств количества информации по Шеннону.
8. Изучение Шенноновских моделей криптосистем.
9. Получение теоретико-информационных оценок стойкости симметричных криптосистем.

В результате изучения дисциплины студент должен знать:

- определение и свойства энтропии;
 - определение и свойства удельной энтропии стационарной символьной последовательности;
 - определение и свойства количества информации по Шеннону;
 - теоретико-информационные оценки стойкости симметричных криптосистем;
- должен уметь:
- вычислять энтропию;
 - вычислять удельную энтропию стационарной символьной последовательности;
 - вычислять количество информации по Шеннону;
 - получать теоретико-информационные оценки стойкости симметричных криптосистем.

В соответствии с типовым учебным планом направления специальности 1-98 01 01-01 «Компьютерная безопасность» (математические методы и программные системы) учебная программа предусматривает для изучения всего 145 часов, в том числе 68 аудиторных часов: лекции — 34 часа, лабораторные занятия — 16 часов, практические занятия — 18 часов.

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

№	Название раздела, темы	Количество аудиторных часов			
		Всего	В том числе		
			Лекции	Лабораторные занятия	Практические занятия
	Раздел I. Вероятностно-статистические модели сообщений и их энтропийные свойства				
1	Источники дискретных сообщений и их вероятностные модели	4	2	2	
2	Функционал энтропии и его свойства	4	2		2
3	Условная энтропия и ее свойства	4	2	2	
4	Удельная энтропия стационарной символьной последовательности	4	2		2
5	Энтропийные характеристики марковских символьных последовательностей	4	2	2	
6	Источники непрерывных сообщений и их энтропийные свойства	4	2		2
7	Оптимизация функционала энтропии на классе вероятностных распределений	4	2	2	
	Раздел II. Методы теории информации в криптологии				
8	Асимптотические свойства стационарного источника дискретных сообщений	8	4		4
9	Энтропийная устойчивость случайных символьных последовательностей	8	4	4	
10	Количество информации по Шеннону и его свойства	8	4		4
11	Шенноновские модели криптосистем	8	4	4	
12	Теоретико-информационные оценки стойкости симметричных криптосистем	8	4		4
	Итого	68	34	16	18

Раздел I. Вероятностно-статистические модели сообщений и их энтропийные свойства

1. Источники дискретных сообщений и их вероятностные модели

Источник дискретных сообщений. Дискретная вероятностная модель.

2. Функционал энтропии и его свойства

Энтропия источника дискретных сообщений. Свойства ограниченности энтропии.

3. Условная энтропия и ее свойства

Условная энтропия источника дискретных сообщений. Свойства иерархической аддитивности, невозрастания при добавлении условий, невозрастания при дискретных функциональных преобразованиях.

4. Удельная энтропия стационарной символьной последовательности

Удельная энтропия. Свойство существования удельной энтропии стационарной символьной последовательности.

5. Энтропийные характеристики марковских символьных последовательностей

Удельная энтропия стационарной марковской символьной последовательности.

6. Источники непрерывных сообщений и их энтропийные свойства

Источник непрерывных сообщений. Абсолютно непрерывная вероятностная модель. Энтропия источника непрерывных сообщений. Свойства неизменности при сдвиге распределения вероятностей, «зеркальных отражениях» и «перестановках фрагментов». Условная энтропия. Свойства иерархической аддитивности, неубывания при линейном сглаживании плотности распределения вероятностей. Формула для энтропии при функциональных преобразованиях. Удельная энтропия стационарной гауссовской символьной последовательности.

7. Оптимизация функционала энтропии на классе вероятностных распределений

Класс одномерных плотностей распределения с конечным носителем. Класс одномерных плотностей с конечными моментами первого и второго порядков. Класс n -мерных плотностей распределения с фиксированным вектором математического ожидания и невырожденной ковариационной матрицей. Оптимизация функционала энтропии на классе вероятностных распределений.

Раздел II. Методы теории информации в криптологии

8. Асимптотические свойства стационарного источника дискретных сообщений

Асимптотические свойства стационарного источника дискретных сообщений. Теорема о высоковероятном подмножестве.

9. Энтропийная устойчивость случайных символьных последовательностей

Энтропийная устойчивость случайных символьных последовательностей. Обобщенная теорема Стратоновича.

10. Количество информации по Шеннону и его свойства

Количество информации по Шеннону. Свойства ограниченности количества информации.

11. Шенноновские модели криптосистем

Шенноновские модели криптосистем. Элементарные криптосистемы: подстановка, перестановка, шифр Виженера, шифр Цезаря, шифр Бопора, криптопреобразование Вернама, биграммная подстановка.

12. Теоретико-информационные оценки стойкости симметричных криптосистем

Теоретико-информационные оценки стойкости симметричных криптосистем. Совершенная криптостойкость.

ЛИТЕРАТУРА

Основная

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

Дополнительная

5. Шеннон К. Работы по теории информации / Москва: ИЛ, 1963.
6. Орлов В.А., Филлипов Л.И. Теория информации в упражнениях и задачах / Москва: Высшая школа, 1976.
7. Тарасенко Ф.П. Введение в курс теории информации / Томск: ТГУ, 1973.
8. Брассар Ж. Современная криптология / Москва: Полимед, 1999.
9. Мельников В.В. Защита информации в компьютерных системах / Москва: Финансы и статистика, 1997.