Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе

_____ А.Л. Толстик

06.07.2016

Регистрационный № УД- 1858/ уч.

ТЕОРИЯ ИНФОРМАЦИИ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-98 01 01 Компьютерная безопасность (по направлениям)

2016 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-98 01 01-2013 и учебного плана Р 98-138/уч., 30.05.2013.

Составители:

Е. В. Вечерко, ассистент кафедры математического моделирования и анализа данных Белорусского государственного университета.

Рекомендована к утверждению:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета (протокол № 8 от 01 декабря 2015 г.);

Научно-методическим советом Белорусского государственного университета (протокол № 3 от 25 января 2016 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Предметом изучения учебной дисциплины «Теория информации» являются математически модели, методы и алгоритмы хранения, преобразования, передачи и защиты информации. Основы теории информации были заложены в 1949 г. американским математиком Клодом Шенноном. Значительный клад в развитие теории информации внесли известные ученые: В.А. Котельников, А.Н. Колмогоров, А.Я. Хинчин, Р.Л. Стратанович, А. Файнстейн, Р. Фано. Возникновение теории информации стало возможным после того, как было осознано, что количество информации (несмотря на ее смысловую разнородность) можно задать числом так же, как можно выразить числом расстояние, время, массу, энергию и другие физические величины.

Учебная дисциплина «Теория информации» относится к циклу дисциплин вузовского компонента и взаимосвязана с учебными дисциплинами «Математический анализ», «Дискретные функции», «Теория вероятностей и математическая статистика». Главная задача дисциплины – ознакомление студентов с методами решения комбинаторных задач. Методы, излагаемые в дисциплине «Теория информации», могут быть использованы при изучении ряда других дисциплин по специальности «Компьютерная безопасность».

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

Задачами курса являются:

1. Определение и установление свойств энтропии источника дискретных и непрерывных сообщений.
2. Оптимизация энтропии на классе вероятностных распределений.
3. Определение и установление свойств функционала количества информации по Шеннону.
4. Установление свойства энтропийной устойчивости символьных последовательностей.
5. Установление свойств энтропии для марсковских источников.
6. Изучение Шенноновских моделей криптосистем.

В результате изучения курса 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;

уметь:

— вычислять энтропию;

— вычислять удельную энтропию стационарной символьной последовательности;

— вычислять количество информации по Шеннону;

В соответствии с образовательным стандартом специальности 1-98 01 01 «Компьютерная безопасность» учебная программа предусматривает для изучения дисциплины всего 148 часов, из них 68 аудиторных часов, в том числе лекций – 34 часов, практических занятий – 14 часов, лабораторных занятий – 12 часов, УСР – 8 часов (3 курс, 6 семестр).

Формы текущей аттестации по учебной дисциплине – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

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

Тема 1.1. Введение. Источники дискретных сообщений и их вероятностные модели. Предмет теории информации. Задачи кодирования и шифрования. Источник дискретных сообщений. Дискретная вероятностная модель.

Тема 1.2. Функционал энтропии и его свойства. Энтропия источника дискретных сообщений и ее свойства: непрерывность; симметричность; неотрицательность; условие обращения энтропии в нуль; максимальное значение энтропии, энтропия Хартли; свойство выпуклости; свойство аддитивности функционала энтропии; изменение энтропии при расширения алфавита.

Тема 1.3. Условная энтропия и ее свойства. Условная энтропия источника дискретных сообщений. Свойство иерархической аддитивности, верхние границы для условной энтропии.

Тема 1.4. Условная энтропия и ее изменение при дискретном функциональном преобразовании. Изменение энтропии при дискретном функциональном преобразовании. Режим простой замены.

Тема 1.5. Удельная энтропия стационарной символьной последовательности. Удельная энтропия. Свойство существования удельной энтропии стационарной символьной последовательности.

Тема 1.6. Энтропийные характеристики марковских символьных последовательностей. Удельная энтропия стационарной марковской символьной последовательности 1-го и высокого порядков.

Тема 1.7. Источники непрерывных сообщений и их энтропийные свойства. Источник непрерывных сообщений. Абсолютно непрерывная вероятностная модель. Энтропия источника непрерывных сообщений и ее свойства. Условная энтропия и ее свойства. Изменение энтропии при функциональных преобразованиях. Удельная энтропия стационарной гауссовской символьной последовательности.

Тема 1.8. 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

Тема 2.1. Асимптотические свойства стационарного источника дискретных сообщений. Асимптотические свойства стационарного источника дискретных сообщений. Теорема о высоковероятном подмножестве.

Тема 2.2. Теорема о мощности высоковероятного подмножества. Теорема о мощности высоковероятного подмножества.

Тема 2.3. Энтропийная устойчивость случайных символьных последовательностей. Энтропийная устойчивость случайных последовательностей.

Тема 2.4. Обобщенная теорема Стратоновича. Обобщенная теорема Стратоновича.

Тема 2.5. Количество информации по Шеннону и его свойства. Количество информации по Шеннону и ее свойства: эквивалентные выражения; свойство симметричности; нижние и верхние границы количества информации; обращение в нуль;

Тема 2.6. Изменение количества информации при отображениях. Изменение количества информации при отображениях, свойство аддитивности для независимых случайных величин.

Тема 2.7. Шенноновские модели криптосистем. Шенноновские модели криптосистем. Элементарные криптосистемы: подстановка, перестановка, шифр Виженера, шифр Цезаря, шифр Бофора, криптопреобразование Вернама, биграммная подстановка.

Тема 2.8. Теоретико-информационные оценки стойкости симметричных криптосистем. Совершенная криптостойкость. Теоремы Шеннона о необходимых и достаточных условиях совершенной криптостойкости.

Тема 2.9. Совершенная криптостойкость шифра Вернама. Совершенная криптостойкость шифра Вернама.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

№п/п	Название раздела, темы	Количество часов				Количество часов УСР	Форма контроля знаний
		Аудиторные					
		Лекции	Практ. и сем. занятия	Лаб. занятия	Иное		
1	**Вероятностно-статистические модели сообщений и их энтропийные свойства**	**16**	**10**	**8**		**4**	
1.1	Введение. Источники дискретных сообщений и их вероятностные модели	2					
1.2	Функционал энтропии и его свойства	2	2	2			Опрос, проверка самостоятельной работы
1.3	Условная энтропия и ее свойства	2	2	2			Опрос, проверка самостоятельной работы
1.4	Условная энтропия и ее изменение при дискретном функциональном преобразовании	2					
1.5	Удельная энтропия стационарной символьной последовательности.	2	2	2			Опрос, проверка самостоятельной работы
1.6	Энтропийные характеристики марковских символьных последовательностей	2	2			2	Контрольная работа №1
1.7	Источники непрерывных сообщений и их энтропийные свойства	2	2	2			Опрос, проверка самостоятельной работы
1.8	Оптимизация функционала энтропии на классе вероятностных распределений	2				2	Контрольная работа №2
2	**Методы теории информации в криптологии**	**18**	**4**	**4**		**4**	
2.1	Асимптотические свойства стационарного источника дискретных сообщений	2					

2.2	Теорема о мощности высоковероятного подмножества	2	2			2	Тест
2.3	Энтропийная устойчивость случайных символьных последовательностей	2					
2.4	Обобщенная теорема Стратоновича	2					
2.5	Количество информации по Шеннону и его свойства	2	2	2			Опрос, проверка самостоятельной работы
2.6	Изменение количества информации при отображениях	2					
2.7	Шенноновские модели криптосистем	2		2			Опрос, проверка самостоятельной работы
2.8	Теоретико-информационные оценки стойкости симметричных криптосистем	2					
2.9	Совершенная криптостойкость шифра Вернама	2				2	Тест
ИТОГО		**34**	**14**	**12**		**8**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Рекомендуемая литература

Основная

1. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии / Минск: БГУ, 1999.
2. Духин А.А. Теория информации: учеб. пос. для спец. “Компьютерная безопасность” / М.: Гелиос АРВ, 2007. – 248 с.
3. Стратонович Р.Л. Теория информации / Москва: Наука, 1975.
4. Кульбак С. Теория информации и статистика / Москва: Наука, 1963.
5. Орлов В.А., Филлипов Л.И. Теория информации в упражнениях и задачах / Москва: Ввысшая школа, 1976.

Дополнительная

1. Колесник В.Д., Полтырев Г.Ш. Курс теории информации / Москва: Наука, 1982.
2. Шэннон К. Работы по теории информации / Москва: ИЛ, 1963.
3. Тарасенко Ф.П. Введение в курс теории информации / Томск: ТГУ, 1973.

Организация управляемой самостоятельной работы студентов

Управляемая самостоятельная работа (УСР) студентов – это самостоятельная работа, выполняемая по заданию и при методическом руководстве преподавателя, а также контролируемая преподавателем на определенном этапе обучения. Целью УСР является целенаправленное обучение студентов основным навыкам и умению индивидуальной самостоятельной работы.

На освоение учебного материала в рамках УСР для дисциплины «Теория информации» отводится 8 аудиторных часов.

Для самостоятельного изучения в рамках УСР дисциплины «Теория информации» выносятся следующие темы:

1. Энтропийные характеристики марковских символьных последовательностей.
2. Оптимизация функционала энтропии на классе вероятностных распределений.
3. Теорема о мощности высоковероятного подмножества.
4. Совершенная криптостойкость шифра Вернама

По первой и четвертой предложенным темам контроль осуществляется в виде контрольной работы, по второй и третьей темам – в виде тестирования.

Результативность самостоятельной работы студентов во многом определяется наличием активных методов ее контроля:

– входной контроль знаний и умений студентов в начале изучения очередной дисциплины;

– текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических и лабораторных занятиях;

– промежуточный контроль по окончании изучения раздела или модуля курса;

– самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;

– итоговый контроль по дисциплине в виде зачета или экзамена;

– контроль остаточных знаний и умений спустя определенное время после завершения изучения дисциплины.

Рекомендации по контролю качества усвоения знаний и проведению аттестации

На лекционных занятиях по учебной дисциплине «Комбинаторный анализ» рекомендуется использовать элементы проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным и конечным требованиям образовательной программы создаются фонды оценочных средств, включающие типовые задания, контрольные работы и тесты. Оценочными средствами предусматривается оценка способности обучающихся к творческой деятельности, их готовность вести поиск решения новых задач, связанных с недостаточностью конкретных специальных знаний и отсутствием общепринятых алгоритмов.

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

– устная форма: собеседования, устные промежуточные и итоговый зачеты.

– письменная форма: тесты, контрольные опросы, контрольная работа.

– устно-письменная форма: отчеты по домашним практическим упражнениям с их устной защитой.

Контрольные мероприятия проводятся в соответствии с учебно-методической картой дисциплины. В случае неявки на контрольное мероприятие по уважительной причине студент вправе по согласованию с преподавателем выполнить его в дополнительное время. Для студентов, получивших неудовлетворительные оценки за контрольные мероприятия, либо не явившихся по неуважительной причине, по согласованию с преподавателем и с разрешения заведующего кафедрой мероприятие может быть проведено повторно.

Оценка текущей успеваемости рассчитывается как среднее оценок за каждую из письменных контрольных работ, оценки за отчеты по домашним практическим упражнениям и оценки за итоговый тест.

Итоговая аттестация предусматривает проведение экзамена. При этом рекомендуется использовать оценивание успеваемости на основе модульно-рейтинговой системы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Математический анализ	Кафедра дискретной математики и алгоритмики	нет	Оставить содержание учебной дисциплины без изменения, протокол № 8 от 01 декабря 2015 г.
Дискретные функции	Кафедра дискретной математики и алгоритмики	нет	Оставить содержание учебной дисциплины без изменения, протокол № 8 от 01 декабря 2015 г.
Теория вероятностей и математическая статистика	Кафедра математического моделирования и анализа данных	нет	Оставить содержание учебной дисциплины без изменения, протокол № 8 от 01 декабря 2015 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ

на _____/_____ учебный год

№№ Пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры дискретной математики и алгоритмики (протокол № ____ от _____ 201_ г.)

Заведующий кафедрой

_____ _____ _____

(ученая степень, звание) (подпись) (И.О. Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____

(ученая степень, звание) (подпись) (И.О.Фамилия)