Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям

_____ О.Г. Прохоренко

«08» июля 2022 г.

Регистрационный № УД – 11768/уч.

ТЕОРИЯ ИНФОРМАЦИИ

**Учебная программа учреждения высшего образования
по учебной дисциплине для специальности:**

1-98 01 01 Компьютерная безопасность (по направлениям)
Направление специальности:
1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)

2022 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-98 01 01-2013, учебного плана: № Р 98-138/уч. от 30.05.2013 г.

СОСТАВИТЕЛЬ:
В. Ю. Палуха, доцент кафедры математического моделирования и анализа данных Белорусского государственного университета, кандидат физико-математических наук, доцент.

РЕЦЕНЗЕНТ:
В.И. Берник, главный научный сотрудник отдела теории чисел и дискретной математики ГНУ «Институт математики НАН Беларуси», доктор физико-математических наук, профессор.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой математического моделирования и анализа данных
факультета прикладной математики и информатики БГУ
(протокол № 10 от 26 апреля 2022 г.)

Научно-методическим Советом БГУ
(протокол № 6 от 29.06.2022)

Заведующий кафедрой _____ И.А. Бодягин

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. Стратонович, 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» для специальности 1-98 01 01 Компьютерная безопасность (по направлениям) предполагает изучение *теории информации в* предположении, что данные имеют *вероятностную* (*стохастическую*) природу, а для их описания и анализа используются *вероятностно-статистические* модели и методы.

Цели и задачи учебной дисциплины

Целью дисциплины «Теория информации» является изучение математических моделей, методов, алгоритмов и программного обеспечения теории информации.

Задачи дисциплины «Теория информации»:

– определение и установление свойств энтропии источника дискретных и непрерывных сообщений;

– оптимизация энтропии на классе вероятностных распределений;

– определение и установление свойств функционала количества информации по Шеннону;

– установление свойства энтропийной устойчивости символьных последовательностей;

– установление свойств энтропии для марковских источников;

– изучение Шенноновских моделей криптосистем.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина «Теория информации» относится к **циклу** специальных дисциплин компонента учреждения высшего образования.

Связи с другими учебными дисциплинами.

Учебная дисциплина «Теория информации» взаимосвязана с учебными дисциплинами «Математический анализ», «Теория вероятностей и математическая статистика», «Криптографические методы».

Знания, полученные в рамках данной дисциплины, будут использованы при изучении дисциплины специальности 1-98 01 01 Компьютерная безопасность (по направлениям) «Системы связи и сети передачи информации».

Требования к компетенциям

Освоение учебной дисциплины «Теория информации» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций.

Академические компетенции:

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным вырабатывать новые идеи (креативность).

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

АК-8. Иметь лингвистические навыки (устная и письменная коммуникация).

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

Социально-личностные компетенции:

СЛК-6. Уметь работать в команде.

Профессиональные компетенции:

ПК-1. Работать с научно-технической, нормативно-справочной и специальной литературой с целью получения последних сведений о новых методах защиты информации, о стойкости существующих систем защиты информации.

ПК-2. Формулировать задачи, возникающие при организации защиты информации.

ПК-3. Разрабатывать модели процессов, явлений или систем при организации защиты информации.

ПК-4. Выбирать необходимые методы исследования, модифицировать существующие, разрабатывать новые методы и применять их для решения поставленных задач при организации защиты информации.

ПК-5. Выполнять оценку эффективности методов защиты информации.

В результате изучения дисциплины студент должен

***знать*:**

– определение и свойства энтропии, условной энтропии;

– определение и свойства удельной энтропии стационарной символьной последовательности;

– определение и свойства количества информации по Шеннону;

– теоретико-информационные оценки стойкости симметричных криптосистем;

– элементы теории кодирования;

уметь:

– вычислять энтропию и условную энтропию;

– вычислять удельную энтропию стационарной символьной последовательности;

– вычислять количество информации по Шеннону;

владеть

– методами вычисления энтропии и количества информации;

– навыками по подготовке отчётов с результатами статистического анализа данных, включающих содержательную интерпретацию результатов анализа, комментарии, выводы и рекомендации.

Структура учебной дисциплины

Дисциплина изучается в 6 семестре. Всего на изучение учебной дисциплины «Теория информации» отведено:

– для очной формы получения высшего образования – 148 часов, в том числе 68 аудиторных часов, из них: лекции – 34 часа, практические занятия – 12 часов, лабораторные занятия – 18 часов, управляемая самостоятельная работа – 4 часа.

Трудоёмкость учебной дисциплины составляет 4 зачётные единицы.

Форма текущей аттестации – 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 расширении алфавита.

Тема 1.3. Условная энтропия и её свойства. Условная энтропия источника дискретных сообщений. Свойство иерархической аддитивности, верхние границы для условной энтропии. Изменение энтропии при дискретном функциональном преобразовании. Информационная дивергенция.

Тема 1.4. Аксиоматическое определение энтропии. Системы аксиом Хинчина, Фаддева, Чечёты.

Тема 1.5. Энтропия Реньи и Тсаллиса. Применение энтропии к статистическому тестированию генераторов. Обобщённый функционал энтропии. Равномерно распределённая случайная последовательность. Статистическое оценивание энтропии Шеннона, Реньи и Тсаллиса. Статистическое тестирование генераторов случайных и псевдослучайных последовательностей с помощью оценок энтропии.

Тема 1.6. 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 1.7. 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.

Тема 1.8. Количество информации по Шеннону и его свойства. Количество информации по Шеннону и его свойства: эквивалентные выражения; свойство симметричности; нижние и верхние границы количества ин-

формации; обращение в нуль. Изменение количества информации при отображениях, свойство аддитивности для независимых случайных величин. Взаимная информация трёх и более случайных величин, условное количество информации.

Раздел II. Методы теории информации в криптологии

Тема 2.1. Удельная энтропия стационарной символьной последовательности. Удельная энтропия. Свойство существования удельной энтропии стационарной символьной последовательности.

Тема 2.2. Асимптотические свойства стационарного источника дискретных сообщений. Асимптотические свойства стационарного источника дискретных сообщений. Теорема о высоковероятном подмножестве. Теорема о мощности высоковероятного подмножества.

Тема 2.3. Энтропийная устойчивость случайных символьных последовательностей. Энтропийная устойчивость случайных последовательностей. Обобщенная теорема Стратоновича.

Тема 2.4. Энтропийные характеристики марковских символьных последовательностей. Удельная энтропия стационарной марковской символьной последовательности 1-го и высокого порядков. Статистическое оценивание $(s + \tau)$-мерной энтропии цепи Маркова s-го порядка, $(s + \tau)$-мерной энтропии сбалансированной цепи Маркова порядка s с r частичными связями.

Тема 2.5. Теорема Мак-Миллана для дискретного эргодического источника. Аппроксимация l-мерных распределений. Теорема Мак-Миллана.

Тема 2.6. Шенноновские модели криптосистем. Шенноновские модели криптосистем. Элементарные криптосистемы: подстановка, перестановка, шифр Виженера, шифр Цезаря, шифр Бофора, криптопреобразование Вернама, биграммная подстановка.

Тема 2.7. Теоретико-информационные оценки стойкости симметричных криптосистем. Совершенная криптостойкость. Теоремы Шеннона о необходимых и достаточных условиях совершенной криптостойкости. Совершенная криптостойкость шифра Вернама.

Тема 2.8. Элементы теории кодирования. Алфавитное кодирование. Кодовые деревья. Средняя длина оптимального кода.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования с применением электронных средств обучения (ДО)

№п/п	Название раздела, темы	Количество часов				Количество часов УСР	Форма контроля знаний
		Аудиторные					
		Лекции	Практические занятия	Лабораторные занятия	Иное		
1	**Вероятностно-статистические модели сообщений и их энтропийные свойства**	**16**	**8**	**8**		**2**	
1.1	Введение. Источники дискретных сообщений и их вероятностные модели	2					Опрос
1.2	Функционал энтропии и его свойства	2	2	2			Отчёт по лабораторной работе с устной защитой
1.3	Условная энтропия и её свойства	2	2	2			Отчёт по домашним практическим упражнениям с устной защитой
1.4	Аксиоматическое определение энтропии	2				2	Опрос
1.5	Энтропия Реньи и Тсаллиса. Применение энтропии к статистическому тестированию генераторов	2					Опрос
1.6	Источники непрерывных сообщений и их энтропийные свойства	2	2	2			Отчёт по домашним практическим упражнениям с устной защитой
1.7	Оптимизация функционала энтропии на клас-	2					Опрос

	се вероятностных распределений						
1.8	Количество информации по Шеннону и его свойства	2	2	2			Коллоквиум
2	**Методы теории информации в криптологии**	**18**	**4**	**10**		**2**	
2.1	Удельная энтропия стационарной символьной последовательности.	2		2			Отчёт по домашним практическим упражнениям с устной защитой
2.2	Асимптотические свойства стационарного источника дискретных сообщений	2	2	2			Опрос
2.3	Энтропийная устойчивость случайных символьных последовательностей	2					Опрос
2.4	Энтропийные характеристики марковских символьных последовательностей	4	2	2			Контрольная работа
2.5	Теорема Мак-Миллана для дискретного эргодического источника	2					Опрос
2.6	Шенноновские модели криптосистем	2					Опрос
2.7	Теоретико-информационные оценки стойкости симметричных криптосистем	2		2			Отчёт по домашним практическим упражнениям с устной защитой
2.8	Элементы теории кодирования	2		2		2	Опрос
ИТОГО		**34**	**12**	**18**		**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Харин, Ю. С. Математические основы теории информации: учебное пособие с грифом Министерства образования / Ю.С. Харин, И. А. Бодягин, Е. В. Вечёрко. – Минск: БГУ, 2018. – 302 с.

Перечень дополнительной литературы

2. Духин, А. А. Теория информации: учебное пособие / А. А. Духин. – Москва: Гелиос АРВ, 2007. – 248 с.
3. Стратонович, Р. Л. Теория информации / Р. Л. Стратонович. – Москва: Советское радио, 1975. – 424 с.
4. Кульбак, С. Теория информации и статистика / С. Кульбак. – Москва: Наука, 1967. – 408 с.
5. Орлов, В. А. Теория информации в упражнениях и задачах / В. А. Орлов, Л. И. Филиппов. – Москва: Высшая школа, 1976. – 136 с.
6. Криптология: учебник с грифом Министерства образования / Ю. С. Харин [и др.] / Минск: БГУ, 2013. – 512 с.
7. Палуха, В. Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности / В. Ю. Палуха // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. – 2017. – № 1. – С. 79–88.
8. Палуха, В. Ю. Об оценивании энтропии дискретных временных рядов с Марковской зависимостью / В. Ю. Палуха, Ю. С. Харин // Теория вероятностей, случайные процессы, математическая статистика и их приложения: сборник научных статей / под редакцией Н. Н. Труша, Г. А. Медведева, Ю. С. Харина. – Минск: РИВШ, 2014. – С. 183–188.

Информационно-методическое обеспечение дисциплины доступно студентам в виде онлайн-курса на образовательном портале https://edufpmi.bsu.by/course/view.php?id=153.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

На лекционных занятиях по дисциплине «Теория информации» рекомендуется особое внимание обращать внимание на установлении связей между теоретическим темами курса и использованием, изучаемых методов и алгоритмов для решения практических задач анализа данных.

Контрольные мероприятия проводятся в соответствии с учебно-методической картой дисциплины.

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

– устная форма: устные опросы по текущим темам;

– письменная форма: контрольная работа, коллоквиум по нескольким теоретическим темам дисциплины;

– устно-письменная форма: отчёты по домашним практическим упражнениям и лабораторным работам с их устной защитой.

Отчёты загружаются для проверки в специально организованный онлайн-курс на портале https://edufpmi.bsu.by/course/view.php?id=153.

Формой текущей аттестации по дисциплине «Теория информации» учебным планом предусмотрен **экзамен.**

При формировании итоговой отметки используется рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Отметка текущей успеваемости рассчитывается как среднеарифметическая величина отметок по всем формам текущего контроля знаний по учебной дисциплине, т.е. отметки за письменную контрольную работу, отметки за коллоквиум, отметок за отчёты по домашним практическим упражнениям и лабораторным работам.

Итоговая отметка по дисциплине рассчитывается на основе отметки текущей успеваемости (рейтинговой системы оценки знаний) и экзаменационной отметки с учётом их весовых коэффициентов. Вес отметки по текущей успеваемости составляет 40 %, экзаменационной отметки – 60 %.

Примерный перечень заданий для 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 4 аудиторных часа по двум следующим темам в соответствии с учебно-методической картой дисциплины.

Тема 1.4. Аксиоматическое определение энтропии. (2 ч)

*Перечень вопросов для углубленного самостоятельного изучения***:**

- система аксиом Хинчина;
- система аксиом Фаддеева.

Рекомендуемая литература: [2].

Форма контроля – устный опрос.

Тема 2.8. Элементы теории кодирования. (2 ч)

Перечень вопросов для углубленного самостоятельного изучения:

- неравенства Крафта и Мак-Миллана;
- средняя длина оптимального кода.

Рекомендуемая литература: [1, 2].

Форма контроля **–** устный опрос.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется практико-ориентированный подход.

Практико-ориентированный подход предполагает:

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

Методические рекомендации по организации самостоятельной работы обучающихся

Студенты самостоятельно выполняют следующую работу:

– осуществляют углубленное изучение тем 1.4 и 2.8 с использованием рекомендуемой литературы;

– выполняют лабораторные задания с использованием различных языков программирования;

– готовят отчёт с результатами проведённых исследований в соответствии с установленными требования;

– работают над устранением указанных при проверке отчётов недостатков.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и бумажных) курсов лекций, учебно-методических материалов по основным темам дисциплины на портале https://edufpmi.bsu.by/course/view.php?id=153.

Примерный перечень вопросов к экзамену

1. Источники дискретных сообщений и их вероятностные модели.
2. Функционал энтропии и его свойства.
3. Условная энтропия и её свойства.

4. Информационная дивергенция.
5. Аксиоматическое определение энтропии.
6. Обобщённый функционал энтропии. Функционалы энтропии Реньи и Тсаллиса.
7. Применение энтропии к статистическому тестированию генераторов.
8. Источники непрерывных сообщений и их энтропийные свойства.
9. Оптимизация функционала энтропии на классе вероятностных распределений.
10. Количество информации по Шеннону и его свойства.
11. Взаимная информация трёх и более случайных величин.
12. Удельная энтропия стационарной символьной последовательности.
13. Асимптотические энтропийные свойства источника дискретных сообщений без памяти.
14. Энтропийная устойчивость случайных символьных последовательностей.
15. Энтропийные характеристики марковских последовательностей.
16. Энтропия цепи Маркова высокого порядка.
17. Теорема Мак-Миллана для дискретного эргодического источника.
18. Шенноновские модели криптосистем.
19. Теоретико-информационные оценки стойкости симметричных криптосистем.
20. Алфавитное кодирование. Кодовые деревья.
21. Неравенства Крафта и Мак-Миллана.
22. Средняя длина оптимального кода.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

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)
Криптографические методы	Кафедра математического моделирования и анализа данных	нет	Оставить содержание учебной дисциплины без изменения (протокол № 10 от 26 апреля 2022 г.)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ

на _____/_____ учебный год

№№ Пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры математического моделирования и анализа данных (протокол № __ от 20___ г.).

Заведующий кафедрой
канд. физ.-мат. наук, доцент _____ И.А.Бодягин
(ученая степень, звание) (подпись) (И.О. Фамилия)

УТВЕРЖДАЮ
Декан факультета
доктор техн. наук, доцент _____ А.М.Недзьведь
(ученая степень, звание) (подпись) (И.О. Фамилия)